Suites arythmiques.

Compositions.

Approche purement syntaxique.

Transparents des compositions.

Three classes of notes.

Courbes et points entiers.

Traverser un carré.

Essai : graphe de produits.

Hyperboles et mots.

Hyperboles et mots.

Essai de formalisation de l'approche proposée pour représenter la primalité à l'aide de mots de Christoffel associés à des hyperboles.

Un programme si surprenant pour connaître la primalité des entiers.

Un programme à mots plus courts pour connaître la primalité des entiers.

Mots de nombres premiers.

transparents : Mots de Christoffel d'hyperboles et primalité.

Codage de mots booléens.

Etude d'une fonction particulière.

Sens des inégalités.

Découle des mots de Christoffel sous hyperboles.

Redondire.

Polygones modulaires.

A la recherche d'une formule récurrente.

Parité.

Voir la primalité dans le triangle de Pascal.

Espace des nombres premiers et pavage apériodique du plan par des triminos colorés ou bicolores.

Malte.

Trouver un passage vers un lieu que quelqu'un connaît.

Les points de l'espace Goldbach commutent-ils ?.

Refaire ses gammes.

Arc tangente.

Très constante.

Note de Riemann.

Proposer une autre formule de calcul du nombre de nombres premiers inférieurs à un nombre donné.

Suite des calculs des formules de Riemann.

Emerveillement.

Petit memo.

Ma fonction somme de sommes de cosinus.

Valuations p-adiques dans les factorisations des factorielles.

Hasard de date dans fraction.

Plaisante.

Interpréter géométriquement l'hypothèse de Riemann.

Transcription textes de Galois du wikisource.

Géométrie modulaire et quantique.

Valuations p-adiques des nombres dans les factorielles.

Sommes de résidus modulaires.

Sommes de résidus modulaires.

Moyenne des résidus quadratiques et moitié des nombres.

Différence entre les fonctions f et F de l'article de Riemann concernant le nombre des nombres premiers inférieurs à une grandeur donnée.

Drôle de manière de caractériser les premiers.

Où est 3 ? puis cercle par transparence.

Pile la moitié.

Espace et mon opérateur.

Matrices pour la somme des diviseurs d'Euler, version simplifiée.

Spirale et ζ.

Refaire ses gammes.

Nombre de solutions de l'équation $xy = -1$ dans les corps premiers.

Causer ou ne pas causer.

Suites de relations "est résidu quadratique de" en miroir.

Rappels sur le nombre de racines de -1 dans les corps premiers.

Motifs rythmiques.

Tautologies.

Diagramme de produits.

Carrés points fixes des nombres composés.

Nombre de solutions de l'équation $x^2 \equiv x \ (mod\ n)$ pour n impair.

Nombre de solutions de l'équation $x^2 \equiv 1 \ (mod\ n)$ pour n impair.

Nombre de solutions de l'équation $x^2 \equiv 1 \ (mod\ n)$ pour n impair.

Nombre de solutions de l'équation $x^4 \equiv 1 \ (mod\ n)$ pour n impair.

Nombre de solutions de l'équation $x^5 \equiv 1 \ (mod\ n)$.

Nombre de solutions de l'équation $x^{10} \equiv 1 \ (mod\ n)$ en fonction du dernier chiffre de n.

Suites arythmiques (Denise Vella-Chemla, 2.1.2017)

On cherche des symétries au sein de l'ensemble des nombres premiers.

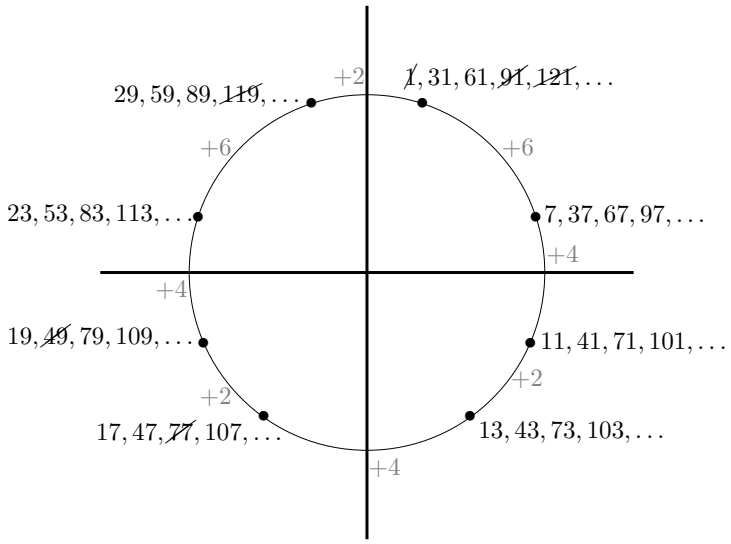
Gauss, dans les Recherches arithmétiques, distinguait les nombres de la forme $4k+1$ de ceux de la forme $4k+3$. On passe des uns aux autres en ajoutant systématiquement 2 et rien ne permet de se situer dans cette suite d'additions successives. D'autres, considérant la divisibilité par 2 et par 3, s'intéressent aux nombres des formes $6k-1$ et $6k+1$, le fait de passer des uns aux autres selon la suite d'additions successives $+2, +4, +2, +4, +2, \ldots$ introduit une petite dissymétrie qui permet de se repérer davantage.

On va s'intéresser ici aux huit suites arithmétiques $30k+1, 30k+7, 30k+11, 30k+13, 30k+17, 30k+19, 30k+23, 30k+29$ auxquelles appartiennent nécessairement les nombres premiers supérieurs à 5. On rappelle la symétrie du groupe des unités à 30 : les $30k+29$ sont des $30k-1$, les $30k+23$ sont des $30k-7$, etc. Si on avait choisi une raison de 60 au lieu de 30, on aurait 16 suites arithmétiques à considérer : $\varphi(30) = 8, \varphi(60) = 16$.

On passe d'un nombre au suivant en répétant indéfiniment la suite de 8 additions :

$$+6,\ +4,\ +2,\ +4,\ +2,\ +4,\ +6,\ +2,$$

C'est ce changement constant de rythme qui justifie l'emploi du terme *arythmiques* dans le titre. Pour visualiser la cyclicité des additions successives, on positionne les nombres sur un cercle ; on voit la symétrie verticale entre les additions en regard.



On obtient les nombres successifs de la suite par multiplication matricielle ainsi :

$$\begin{pmatrix} u_{n+8} \\ u_{n+7} \\ u_{n+6} \\ u_{n+5} \\ u_{n+4} \\ u_{n+3} \\ u_{n+2} \\ u_{n+1} \\ u_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 4 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} u_{n+7} \\ u_{n+6} \\ u_{n+5} \\ u_{n+4} \\ u_{n+3} \\ u_{n+2} \\ u_{n+1} \\ u_n \\ u_0 \end{pmatrix}$$

On aimerait cumuler à ce dispositif un autre dispositif qui tirerait à pile ou face (ou plus) les probabilités qu'a chaque nombre d'être premier ou pas mais on ne sait pas le faire (il faudrait pouvoir modéliser que tout nombre à une chance sur p d'être divisible par p premier et $\frac{p-1}{p}$ chances de ne pas l'être (pour tout p premier) par des matrices de la forme $\begin{pmatrix} \frac{1}{p} & 0 \\ 0 & \frac{p-1}{p} \end{pmatrix}$ mais on ne voit pas comment agglomérer ces probabilités aux suites arythmiques présentées ci-dessus).

Par la magie des produits tensoriels utilisés en mécanique quantique, cela permettrait peut-être, selon la formule, d'envisager "tous les possibles" et la résolution de l'incertitude permettrait d'un coup d'un seul de savoir quel nombre est premier et quel nombre ne l'est pas.

Notes :
Premiers à 6 : 1,5,7,11,13,17,19,23,25,29,31,35,...,121
(+4,+2)

Premiers à 7 : 1,2,3,4,5,6,8,9,10,11,12,13,15,16,17,...,121
(+1,+1,+1,+1,+1,+2)

Premiers à 15 : 1,2,4,7,8,11,13,14,16,17,19,22,29,...,121
(+1,+2,+3,+1,+3,+2,+1,+2)

Premiers à 21 : 1,2,4,5,8,10,11,13,16,17,19,20,...,121
(+1,+2,+1,+3,+2,+1,+2,+3,+1,+2,+1,+2)

Premiers à 35 : 1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34,...,121
(+1,+1,+1,+2,+2,+1,+2,+1,+1,+3,+1,+1,+1,+3,+1,+1,+2,+1,+2,+2,+1,+1,+1,+2)

Intersection : *Premiers à 6=2.3 et premiers à 35=5.7 :* 11,13,17,19,23,29,31,...,121

Chaque nombre x coupe l'ensemble des nombres en 2, les nombres premiers à x et les nombres non-premiers à x.

Les nombres premiers sont premiers à tous les nombres qu'ils ne divisent pas.

Pour aller vers la topologie, voir les graphes étiquetés par des éléments de partitions (compositions) de nombres et voir l'article sur les diagrammes de Venn dessinables.
wikipedia : compositions d'un nombre
Venn symmetry and prime numbers : a seductive proof revisited, S. Wagon, P. Webb, 2008
The search for symmetric Venn diagrams, B. Grünbaum, 1999
Venn Diagrams and Symmetric Chain Decompositions in the Boolean Lattice, J. Briggs, C.E. Killian, C.D. Savage, 2004

Compositions (Denise Vella-Chemla, 7.1.2017)

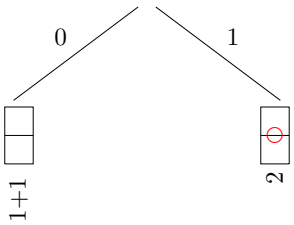
On cherche ce que les nombres premiers symétrisent.

On sait par exemple qu'un nombre premier p a exactement $\frac{p-1}{2}$ résidus quadratiques, tandis que ce n'est pas le cas d'un nombre composé. Si on considère x et $p-x$ inférieurs à p, soit tous 2 sont résidus quadratiques de p simultanément, soit si l'un l'est, l'autre ne l'est pas et inversement. On peut voir dans ces faits une forme de symétrie.

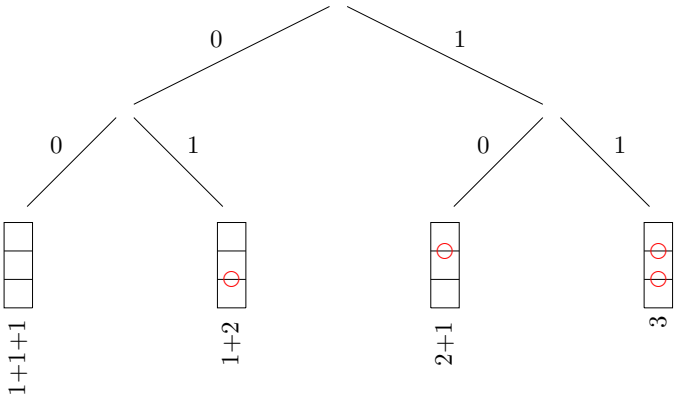
Cherchons d'autres formes de symétrie en étudiant les compositions des nombres. On prend comme référence l'article de wikipedia https://fr.wikipedia.org/wiki/Composition_(*combinatoire*).

Un nombre n a 2^{n-1} compositions différentes. On peut voir les compositions de n comme feuilles d'un arbre binaire de hauteur $n-1$. On voit que l'ordre des sommants importe, $1+1+2+2$ et $1+2+1+2$ sont des compositions différentes de 6 (alors qu'elles correspondent à la même partition).

Arbre binaire des compositions de 2



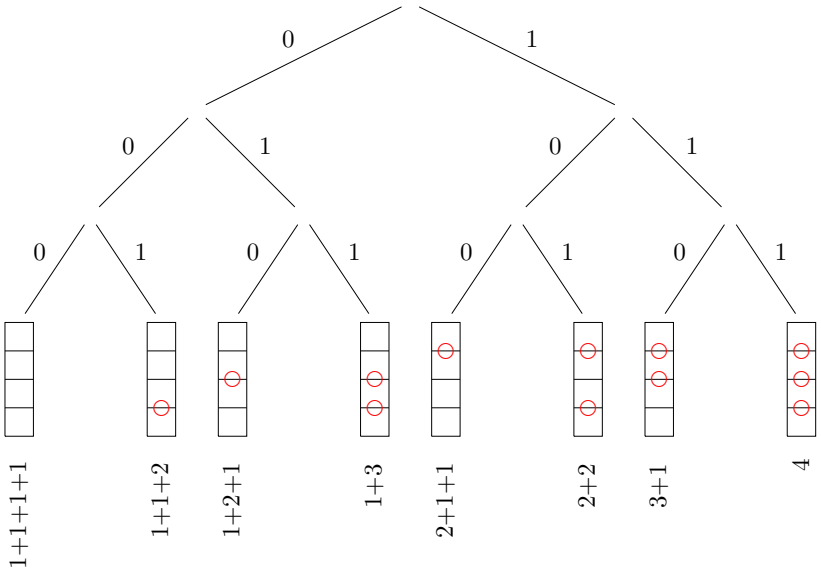
Arbre binaire des compositions de 3 (lire les dessins de haut en bas)



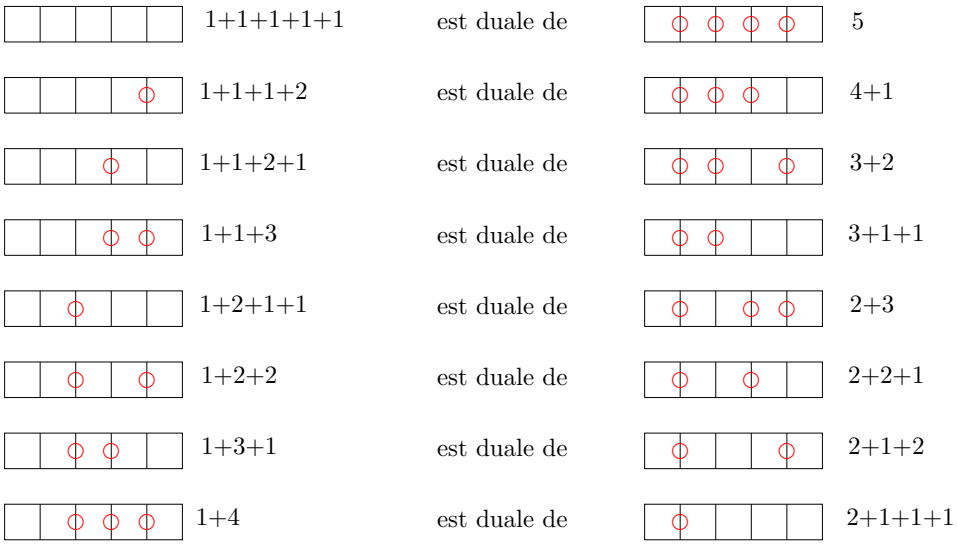
Pour obtenir une composition de $n+1$ à partir d'une composition de n, il suffit soit d'ajouter un sommant $1+$ au début de la composition de n, soit de remplacer le premier sommant de la composition de n par son successeur, en obtenant à partir de la composition $n = s_0 + A$ la composition $n+1 = (1+s_0) + A$, le calcul entre parenthèses devant être effectivement effectué.

Voyons cela pour le passage des compositions de 3 à celles de 4 : de l'ensemble $\{1+1+1, 1+2, 2+1, 3\}$ des compositions de 3, on peut concaténer $1+$ au début de chaque somme, ce qui permet d'obtenir l'ensemble de compositions de 4 $\{1+1+1+1, 1+1+2, 1+2+1, 1+3\}$; ou bien dans chaque composition de 3, on remplace le premier sommant par son successeur, ce qui permet d'obtenir l'ensemble de compositions de 4 $\{2+1+1, 2+2, 3+1, 4\}$. On réitère le processus pour passer de l'ensemble des compositions de 4 $\{1+1+1+1, 1+1+2, 1+2+1, 1+3, 2+1+1, 2+2, 3+1, 4\}$ à l'ensemble de compositions de 5 constitué de l'union des deux ensembles $\{1+1+1+1+1, 1+1+1+2, 1+1+2+1, 1+1+3, 1+2+1+1, 1+2+2, 1+3+1, 1+4\}$ et $\{2+1+1+1, 2+1+2, 2+2+1, 2+3, 3+1+1, 3+2, 4+1, 5\}$.

Arbre binaire des compositions de 4



On appelle *duales*[1] deux compositions d'un nombre dont les mots binaires ont des lettres inversées (0 à la place de 1 et 1 à la place de 0). Voyons les compositions duales pour le nombre 5.

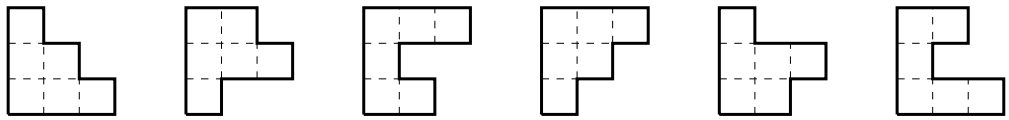


Un nombre composé est notamment caractérisé par le fait que l'une de ses compositions au moins, différente de la composition triviale composée uniquement de 1 de la forme 1+1+...+1, est telle que, quelle que soit la permutation qu'on pourrait effectuer entre 2 de ses sommants, cette composition reste identique à elle-même. Il en est ainsi de la composition 2+2+2 de 6, ou 5+5+5+5+5 de 25.

Précisons cela : il y a une correspondance bijective entre les mots booléens de $n-1$ caractères et les compositions de n. Par exemple, le mot de 5 lettres 10010 correspond à la décomposition $2+1+2+1$ de 6. Il faudrait trouver la manière dont la condition énoncée au paragraphe précédent (d'invariance syntaxique par toute permutation de deux sommants d'une composition au moins) se transfère aux mots booléens.

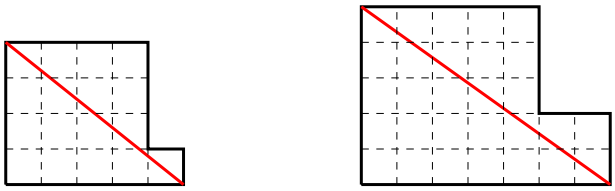
[1] On ne sait pas encore si cette définition présente une utilité.

On associe à chaque composition une surface à base de carrés qui la représente et on calcule le périmètre de cette surface. Ci-dessous les surfaces associées aux compositions à 3 sommants de 6 et leur périmètre.



$3+2+1$ $P=12$ | $1+3+2$ $P=12$ | $2+1+3$ $P=14$ | $1+2+3$ $P=12$ | $2+3+1$ $P=12$ | $3+1+2$ $P=14$

Les compositions dont les sommants sont ordonnés minimisent le périmètre (on les appelle partitions, on les représente par des diagrammes de Young). On peut calculer leur périmètre en utilisant la distance de Manhattan (ou distance associée à la norme 1). Pour les nombres composés, le périmètre minimum d'une composition vaut $2(Max(Sommants) + Nombre\_de\_Sommants)$.



17=16+1
P=18

29=25+4
P=24

Annexe 1 : les 32 compositions de 6 et leur mot booléen correspondant

$1+1+1+1+1+1$ (00000)	$2+1+1+1+1$ (10000)
$1+1+1+1+2$ (00001)	$2+1+1+2$ (10001)
$1+1+1+2+1$ (00010)	$2+1+2+1$ (10010)
$1+1+1+3$ (00011)	$2+1+3$ (10011)
$1+1+2+1+1$ (00100)	$2+2+1+1$ (10100)
$1+1+2+2$ (00101)	$2+2+2$ (10101)
$1+1+3+1$ (00110)	$2+3+1$ (10110)
$1+1+4$ (00111)	$2+4$ (10111)
$1+2+1+1+1$ (01000)	$3+1+1+1$ (11000)
$1+2+1+2$ (01001)	$3+1+2$ (11001)
$1+2+2+1$ (01010)	$3+2+1$ (11010)
$1+2+3$ (01011)	$3+3$ (11011)
$1+3+1+1$ (01100)	$4+1+1$ (11100)
$1+3+2$ (01101)	$4+2$ (11101)
$1+4+1$ (01110)	$5+1$ (11110)
$1+5$ (01111)	6 (11111)

Annexe 2 : Valeurs des majorants des périmètres minima de surface d'aire n pour n impair inférieur à 100

P(1)= 0 ( )	P(21)=20 (-)	P(41)=84 (+)	P(61)=124 (+)	P(81)=60 (-)
P(3)= 8 (+)	P(23)=48 (+)	P(43)=88 (+)	P(63)=48 (-)	P(83)=168 (+)
P(5)=12 (+)	P(25)=20 (-)	P(45)=36 (-)	P(65)=36 (-)	P(85)=44 (-)
P(7)=16 (+)	P(27)=24 (-)	P(47)=96 (+)	P(67)=136 (+)	P(87)=64 (-)
P(9)=12 (-)	P(29)=60 (+)	P(49)=28 (-)	P(69)=52 (-)	P(89)=180 (+)
P(11)=24 (+)	P(31)=64 (+)	P(51)=40 (-)	P(71)=144 (+)	P(91)=40 (-)
P(13)=28 (+)	P(33)=28 (-)	P(53)=108 (+)	P(73)=148 (+)	P(93)=68 (-)
P(15)=16 (-)	P(35)=24 (-)	P(55)=32 (-)	P(75)=56 (-)	P(95)=48 (-)
P(17)=36 (+)	P(37)=76 (+)	P(57)=44 (-)	P(77)=36 (-)	P(97)=196 (+)
P(19)=40 (+)	P(39)=32 (-)	P(59)=120 (+)	P(79)=160 (+)	P(99)=72 (-)

Approche purement syntaxique (Denise Vella-Chemla, 12.1.2017)

1) Modéliser

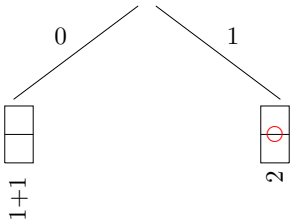
On cherche ce que les nombres premiers symétrisent.

On sait par exemple qu'un nombre premier p a exactement $\frac{p-1}{2}$ résidus quadratiques, tandis que ce n'est pas le cas d'un nombre composé. Si on considère x et $p-x$ inférieurs à p, soit tous 2 sont résidus quadratiques de p simultanément, soit si l'un l'est, l'autre ne l'est pas et inversement. On peut voir dans ces faits une forme de symétrie.

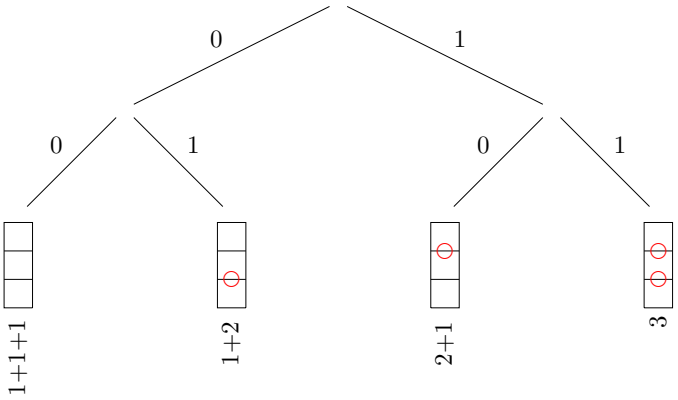
Cherchons d'autres formes de symétrie en étudiant les compositions des nombres. On prend comme référence l'article de wikipedia https://fr.wikipedia.org/wiki/Composition_(*combinatoire*).

Un nombre n a 2^{n-1} compositions différentes. On peut voir les compositions de n comme feuilles d'un arbre binaire de hauteur $n-1$. On voit que l'ordre des sommants importe, 1+1+2+2 et 1+2+1+2 sont des compositions différentes de 6 (alors qu'elles correspondent à la même partition). Il y a une correspondance bijective entre les mots booléens de $n-1$ caractères et les compositions de n. Par exemple, le mot de 5 lettres 10010 correspond à la décomposition $2+1+2+1$ de 6.

Arbre binaire des compositions de 2



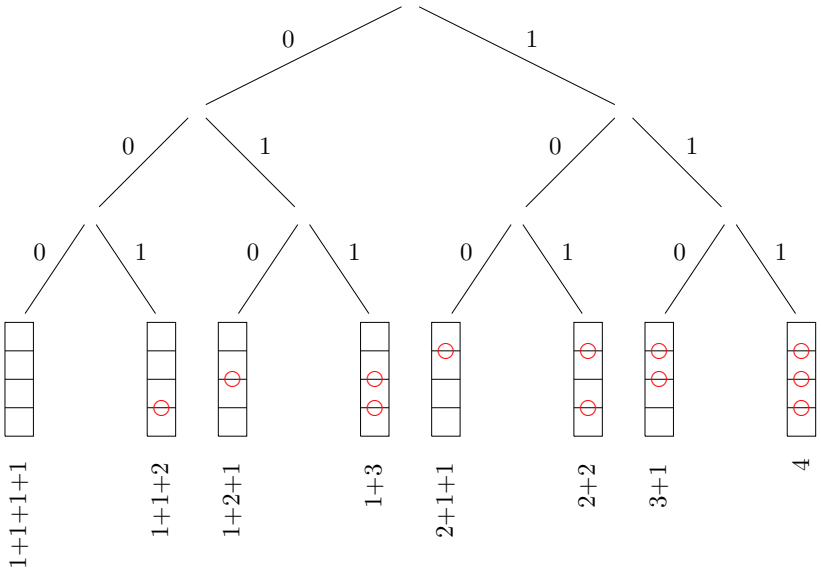
Arbre binaire des compositions de 3 (lire les dessins de haut en bas)



Pour obtenir une composition de $n+1$ à partir d'une composition de n, il suffit soit d'ajouter un sommant 1+ au début de la composition de n, soit de remplacer le premier sommant de la composition de n par son successeur, en obtenant à partir de la composition $n = s_0 + A$ la composition $n+1 = (1+s_0) + A$, le calcul entre parenthèses devant être effectivement effectué.

Voyons cela pour le passage des compositions de 3 à celles de 4 : de l'ensemble $\{1+1+1, 1+2, 2+1, 3\}$ des compositions de 3, on peut concaténer 1+ au début de chaque somme, ce qui permet d'obtenir l'ensemble de compositions de 4 $\{1+1+1+1, 1+1+2, 1+2+1, 1+3\}$; ou bien dans chaque composition de 3, on remplace le premier sommant par son successeur, ce qui permet d'obtenir l'ensemble de compositions de 4 $\{2+1+1, 2+2, 3+1, 4\}$. On réitère le processus pour passer de l'ensemble des compositions de 4 $\{1+1+1+1, 1+1+2, 1+2+1, 1+3, 2+1+1, 2+2, 3+1, 4\}$ à l'ensemble de compositions de 5 constitué de l'union des deux ensembles $\{1+1+1+1+1, 1+1+1+2, 1+1+2+1, 1+1+3, 1+2+1+1, 1+2+2, 1+3+1, 1+4\}$ et $\{2+1+1+1, 2+1+2, 2+2+1, 2+3, 3+1+1, 3+2, 4+1, 5\}$.

Arbre binaire des compositions de 4



On appelle compositions triviales les deux compositions constituées l'une uniquement de n caractères 1 séparés par des signes "+", de la forme $1+1+\ldots+1$, et l'autre de n seul. Un nombre composé est notamment caractérisé par le fait que l'une de ses compositions au moins, différente des deux compositions triviales, est telle que quelle que soit la permutation qu'on pourrait effectuer entre 2 de ses sommants, cette composition reste identique à elle-même. Il en est ainsi de la composition 2+2+2 de 6, ou 5+5+5+5+5 de 25. Un nombre premier n'a aucune de ses compositions qui est ainsi invariante par toute permutation de ses sommants. Cette caractérisation de la primalité est exclusivement syntaxique.

2) Essayer de formaliser

A chaque entier est associé un ensemble de parties de $\mathbb{N}$. Chaque partie de $\mathbb{N}$ est une application de $\mathbb{N}$ dans $\{0,1\}$ et on code par un booléen le fait qu'une partie soit image d'un entier ou pas.

Une partie de $\mathbb{N}$ étant codée par un mot infini, on complète chaque mot booléen de la section précédente par une infinité de 0 ; cette infinité de zéros à droite n'ajoute pas de sommant à l'écriture additive.

$$\begin{array}{l}\mathbb{N} \longrightarrow \{0,1\}^{\{0,1\}^{\mathbb{N}}} \\ n \longmapsto \{s \in \{0,1\}^{\mathbb{N}} / \forall i \geqslant n, s[i] = 0\} \subset \mathcal{P}(\mathbb{N})\end{array}$$

Voyons en quoi consiste le passage d'un entier au suivant selon cette formalisation (informatiquement, c'est trivial, ça consiste à concaténer une lettre 0 ou 1 à gauche des mots de n).

On a le diagramme suivant :

$$\begin{array}{ccc}\mathbb{N} & \xrightarrow{d_n} & \{0,1\}^{\{0,1\}^{\mathbb{N}}} \\ \downarrow{\scriptstyle +1} & & \downarrow{\scriptstyle d_{n+1}} \\ \mathbb{N} & \xrightarrow{d_n} & \{0,1\}^{\{0,1\}^{\mathbb{N}}}\end{array}$$

avec $d_n : \mathbb{N} \longrightarrow \{0,1\}$ et

$$\begin{array}{rccl} d_{n+1} : & k & \longmapsto & d_n(k-1), \forall k \geqslant 1 \\ & 0 & \longmapsto & 0 \\ & & \longmapsto & 1 \end{array}$$

La condition correspondant au fait d'être composé pour un nombre entier qui consiste à avoir une composition (différente des deux compositions triviales) de la forme $x+x+\ldots+x+x$ se traduit très simplement sur les mots booléens : elle consiste en l'apparition dans le mot d'une puissance au moins carrée d'un sous-mot non-nul (le sous-mot en question est appelé période en théorie des langages rationnels) ; par

exemple, la composition $2+2+2$ de 6, codée par le mot $1010100000\ldots$ contient le sous-mot 10 répété trois fois, elle s'écrit $(10)^3 0^\infty$.

Annexe 1 : les 32 compositions de 6 et leur mot booléen correspondant

$1+1+1+1+1+1$ (00000)	$2+1+1+1+1$ (10000)
$1+1+1+1+2$ (00001)	$2+1+1+2$ (10001)
$1+1+1+2+1$ (00010)	$2+1+2+1$ (10010)
$1+1+1+3$ (00011)	$2+1+3$ (10011)
$1+1+2+1+1$ (00100)	$2+2+1+1$ (10100)
$1+1+2+2$ (00101)	$2+2+2$ (10101)
$1+1+3+1$ (00110)	$2+3+1$ (10110)
$1+1+4$ (00111)	$2+4$ (10111)
$1+2+1+1+1$ (01000)	$3+1+1+1$ (11000)
$1+2+1+2$ (01001)	$3+1+2$ (11001)
$1+2+2+1$ (01010)	$3+2+1$ (11010)
$1+2+3$ (01011)	$3+3$ (11011)
$1+3+1+1$ (01100)	$4+1+1$ (11100)
$1+3+2$ (01101)	$4+2$ (11101)
$1+4+1$ (01110)	$5+1$ (11110)
$1+5$ (01111)	6 (11111)

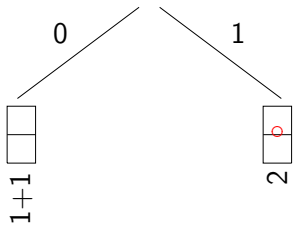
Annexe 2 : Programme de passage des mots booléens aux compositions

```
#include <cstdlib>
#include <iostream>
#include <vector>

using std::cout;
using std::endl;
using std::atoi;

typedef std::vector<bool> bitset;

void print_bits(bitset &bits) {
    for (int i = 0; i < bits.size(); ++i)
        cout << (int) bits[i];
}

void print_deco(bitset &bits) {
    int s = 1;
    for (int i = 0; i < bits.size(); ++i) {
        if (bits[i]) {
            ++s;
        } else {
            cout << s << "+";
            s = 1;
        }
    }
    cout << s;
}
```

```
void generate(int n, bitset &bits) {
    if (n-- > 0) {
        bits[n] = 0; generate(n, bits);
        bits[n] = 1; generate(n, bits);
    } else {
        print_bits(bits);
        cout << " : ";
        print_deco(bits);
        cout << endl;
    }
}

int main(int argc, char* argv[]) {
    int n_max = 0;
    if (argc > 1) n_max = atoi(argv[1]);
    for (int n = 0; n < n_max; ++n) {
        cout << "n = " << n + 1 << " :" << endl;
        bitset bits(n);
        generate(n, bits);
        cout << endl;
    }
}
```

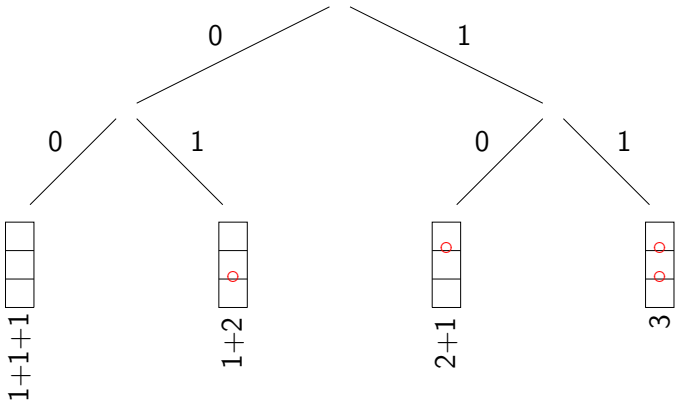
Compositions et mots booléens

- A chaque entier n, on associe ses 2^{n-1} compositions additives.
- *exemple* : arbre binaire des compositions de 2



Exemple

- *exemple* : arbre binaire des compositions de 3



- Noter que la composition $1+2$ est différente de la composition $2+1$.

Obtention des compositions de $n+1$ à partir de celles de n

- On concatène 0 ou 1 au début de chaque mot booléen de n.
- Cela correspond à deux actions syntaxiques : concaténer "1+" en début de composition ou bien remplacer le premier sommant par son successeur.

Nombre composé / nombre premier

- On appelle compositions triviales la composition correspondant au mot booléen ne contenant que des 0 (composition de la forme $1+1+\ldots+1$) ou bien la composition correspondant au mot booléen contenant $n-1$ lettres 1 (composition de la forme n).
- Un nombre composé admet au moins une décomposition non triviale de la forme $x+x+x+\ldots+x$ contenant 2 occurrences de x au moins.
- A chaque entier est associé un ensemble de mots booléens, i.e. un ensemble de parties de $\mathbb{N}$.

$$\mathbb{N} \longrightarrow \{0,1\}^{\{0,1\}^{\mathbb{N}}}$$
$$n \longmapsto \{s \in \{0,1\}^{\mathbb{N}} / \forall i \geqslant n, s[i] = 0\} \subset \mathcal{P}(\mathbb{N})$$

Formalisation

- Le passage de n à $n+1$ est codé par le diagramme suivant :

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{d_n} & \{0,1\}^{\{0,1\}^{\mathbb{N}}} \\ {\scriptstyle +1}\downarrow & & \downarrow{\scriptstyle d_{n+1}} \\ \mathbb{N} & \xrightarrow[d_n]{} & \{0,1\}^{\{0,1\}^{\mathbb{N}}} \end{array}$$

avec $\quad d_n : \mathbb{N} \longrightarrow \{0,1\}$

et

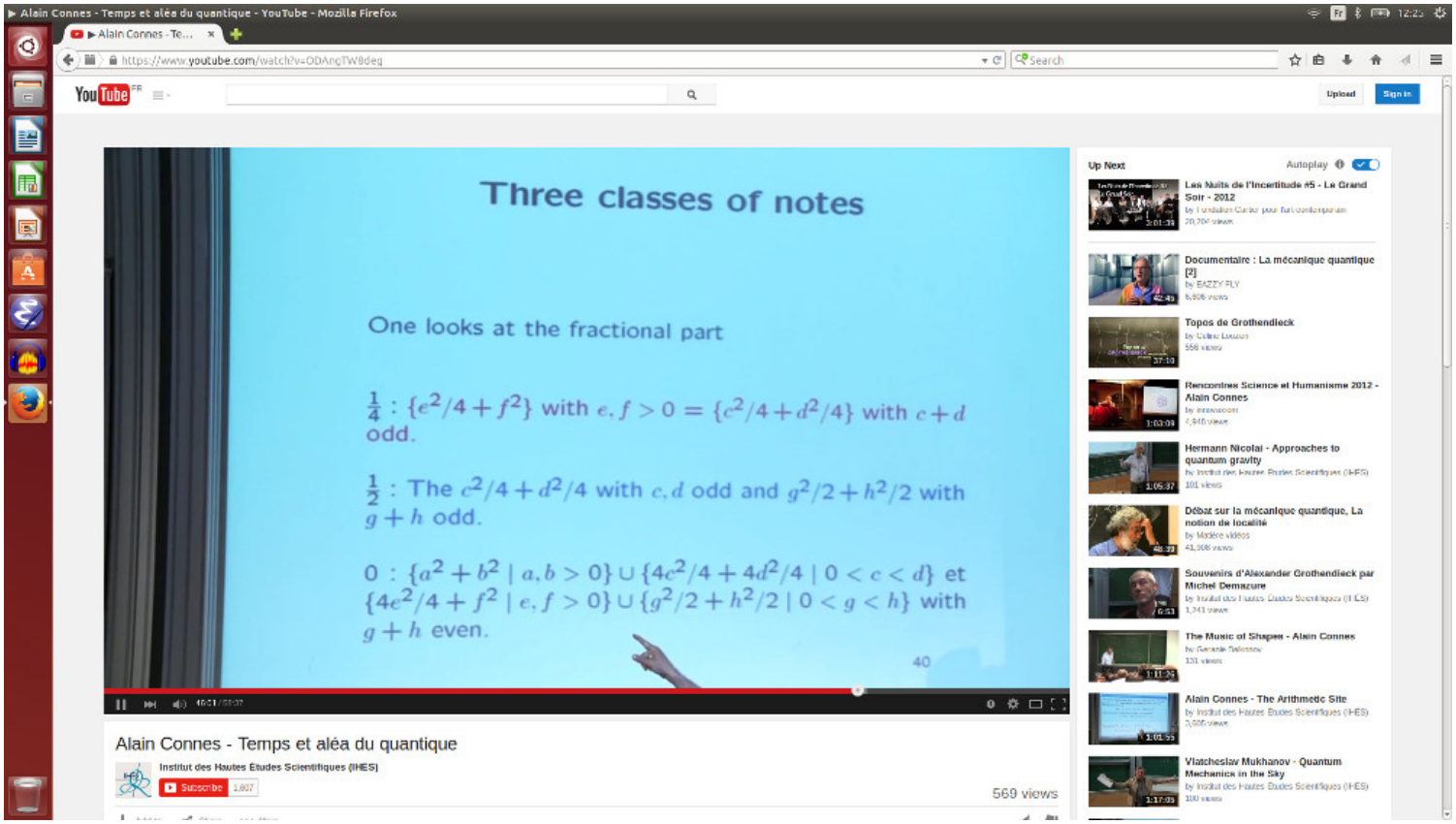
$$d_{n+1} : \begin{array}{ccc} k & \longmapsto & d_n(k-1), \forall k \geqslant 1 \\ 0 & \longmapsto & 0 \end{array}$$

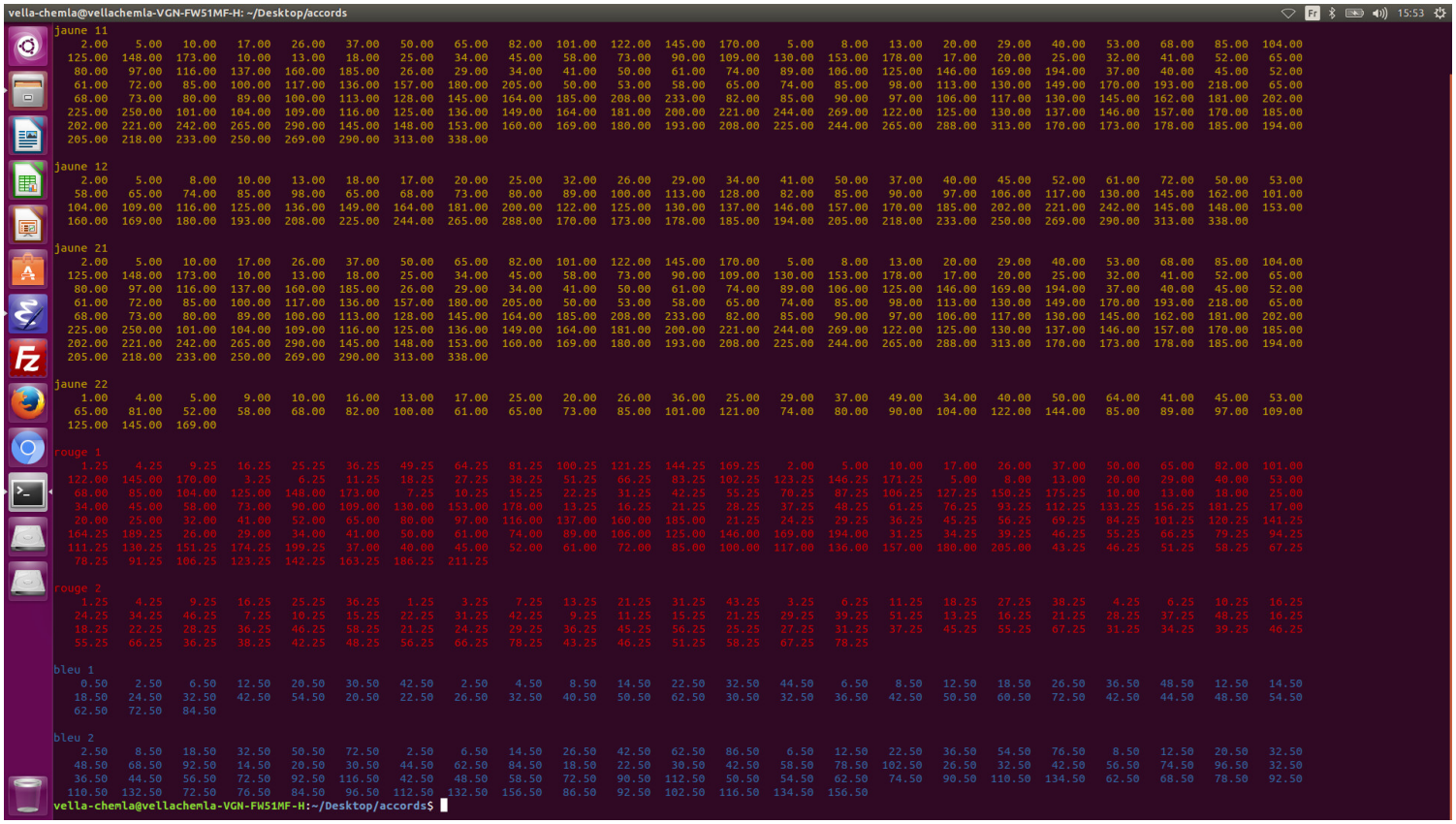
- faire l'union de cet ensemble de fonctions avec l'ensemble des fonctions d_{n+1} qui associent l'image 1 (plutôt que 0) à 0.

Nombre composé / nombre premier

- Un nombre est composé n si l'un de ces mots non triviaux (dont on considère les $n-1$ premières lettres, i.e. la partie des mots avant l'infinité de zéros) admet une période (c'est un motif qui se répète, en théorie des langages).

- Un nombre est premier si tous ses mots sont apériodiques.


Alain Connes - Temps et aléa du quantique - YouTube - Mozilla Firefox
https://www.youtube.com/watch?v=ODAngTW8deg
Three classes of notes
One looks at the fractional part
$\frac{1}{4}$: $\{e^2/4+f^2\}$ with $e,f>0 = \{c^2/4+d^2/4\}$ with $c+d$ odd.
$\frac{1}{2}$: The $c^2/4+d^2/4$ with c,d odd and $g^2/2+h^2/2$ with $g+h$ odd.
0 : $\{a^2+b^2 \mid a,b>0\} \cup \{4c^2/4+4d^2/4 \mid 0<c<d\}$ et $\{4e^2/4+f^2 \mid e,f>0\} \cup \{g^2/2+h^2/2 \mid 0<g<h\}$ with $g+h$ even.
40
Alain Connes - Temps et aléa du quantique
Institut des Hautes Études Scientifiques (IHES)
Subscribe
569 views
Up Next
Autoplay
Les Nuits de l'Incertitude #5 - Le Grand Soir - 2012
Documentaire : La mécanique quantique [2]
Topos de Grothendieck
Rencontres Science et Humanisme 2012 - Alain Connes
Hermann Nicolai - Approaches to quantum gravity
Débat sur la mécanique quantique, La notion de localité
Souvenirs d'Alexander Grothendieck par Michel Demazure
The Music of Shapes - Alain Connes
Alain Connes - The Arithmetic Site
Vlatcheslav Mukhanov - Quantum Mechanics in the Sky


vella-chemla@vellachemla-VGN-FW51MF-H: ~/Desktop/accords
15:53
jaune 11
2.00 5.00 10.00 17.00 26.00 37.00 50.00 65.00 82.00 101.00 122.00 145.00 170.00 5.00 8.00 13.00 20.00 29.00 40.00 53.00 68.00 85.00 104.00
125.00 148.00 173.00 10.00 13.00 18.00 25.00 34.00 45.00 58.00 73.00 90.00 109.00 130.00 153.00 178.00 17.00 20.00 25.00 32.00 41.00 52.00 65.00
80.00 97.00 116.00 137.00 160.00 185.00 26.00 29.00 34.00 41.00 50.00 61.00 74.00 89.00 106.00 125.00 146.00 169.00 194.00 37.00 40.00 45.00 52.00
61.00 72.00 85.00 100.00 117.00 136.00 157.00 180.00 205.00 50.00 53.00 58.00 65.00 74.00 85.00 98.00 113.00 130.00 149.00 170.00 193.00 218.00 65.00
68.00 73.00 80.00 89.00 100.00 113.00 128.00 145.00 164.00 185.00 208.00 233.00 82.00 85.00 90.00 97.00 106.00 117.00 130.00 145.00 162.00 181.00 202.00
225.00 250.00 101.00 104.00 109.00 116.00 125.00 136.00 149.00 164.00 181.00 200.00 221.00 244.00 269.00 122.00 125.00 130.00 137.00 146.00 157.00 170.00 185.00
202.00 221.00 242.00 265.00 290.00 145.00 148.00 153.00 160.00 169.00 180.00 193.00 208.00 225.00 244.00 265.00 288.00 313.00 170.00 173.00 178.00 185.00 194.00
205.00 218.00 233.00 250.00 269.00 290.00 313.00 338.00
jaune 12
2.00 5.00 8.00 10.00 13.00 18.00 17.00 20.00 25.00 32.00 26.00 29.00 34.00 41.00 50.00 37.00 40.00 45.00 52.00 61.00 72.00 50.00 53.00
58.00 65.00 74.00 85.00 98.00 65.00 68.00 73.00 80.00 89.00 100.00 113.00 128.00 82.00 85.00 90.00 97.00 106.00 117.00 130.00 145.00 162.00 101.00
104.00 109.00 116.00 125.00 136.00 149.00 164.00 181.00 200.00 122.00 125.00 130.00 137.00 146.00 157.00 170.00 185.00 202.00 221.00 242.00 145.00 148.00 153.00
160.00 169.00 180.00 193.00 208.00 225.00 244.00 265.00 288.00 170.00 173.00 178.00 185.00 194.00 205.00 218.00 233.00 250.00 269.00 290.00 313.00 338.00
jaune 21
2.00 5.00 10.00 17.00 26.00 37.00 50.00 65.00 82.00 101.00 122.00 145.00 170.00 5.00 8.00 13.00 20.00 29.00 40.00 53.00 68.00 85.00 104.00
125.00 148.00 173.00 10.00 13.00 18.00 25.00 34.00 45.00 58.00 73.00 90.00 109.00 130.00 153.00 178.00 17.00 20.00 25.00 32.00 41.00 52.00 65.00
80.00 97.00 116.00 137.00 160.00 185.00 26.00 29.00 34.00 41.00 50.00 61.00 74.00 89.00 106.00 125.00 146.00 169.00 194.00 37.00 40.00 45.00 52.00
61.00 72.00 85.00 100.00 117.00 136.00 157.00 180.00 205.00 50.00 53.00 58.00 65.00 74.00 85.00 98.00 113.00 130.00 149.00 170.00 193.00 218.00 65.00
68.00 73.00 80.00 89.00 100.00 113.00 128.00 145.00 164.00 185.00 208.00 233.00 82.00 85.00 90.00 97.00 106.00 117.00 130.00 145.00 162.00 181.00 202.00
225.00 250.00 101.00 104.00 109.00 116.00 125.00 136.00 149.00 164.00 181.00 200.00 221.00 244.00 269.00 122.00 125.00 130.00 137.00 146.00 157.00 170.00 185.00
202.00 221.00 242.00 265.00 290.00 145.00 148.00 153.00 160.00 169.00 180.00 193.00 208.00 225.00 244.00 265.00 288.00 313.00 170.00 173.00 178.00 185.00 194.00
205.00 218.00 233.00 250.00 269.00 290.00 313.00 338.00
jaune 22
1.00 4.00 5.00 9.00 10.00 16.00 13.00 17.00 25.00 20.00 26.00 36.00 25.00 29.00 37.00 49.00 34.00 40.00 50.00 64.00 41.00 45.00 53.00
65.00 81.00 52.00 58.00 68.00 82.00 100.00 61.00 65.00 73.00 85.00 101.00 121.00 74.00 80.00 90.00 104.00 122.00 144.00 85.00 89.00 97.00 109.00
125.00 145.00 169.00
rouge 1
1.25 4.25 9.25 16.25 25.25 36.25 49.25 64.25 81.25 100.25 121.25 144.25 169.25 2.00 5.00 10.00 17.00 26.00 37.00 50.00 65.00 82.00 101.00
122.00 145.00 170.00 3.25 6.25 11.25 18.25 27.25 38.25 51.25 66.25 83.25 102.25 123.25 146.25 171.25 5.00 8.00 13.00 20.00 29.00 40.00 53.00
68.00 85.00 104.00 125.00 148.00 173.00 7.25 10.25 15.25 22.25 31.25 42.25 55.25 70.25 87.25 106.25 127.25 150.25 175.25 10.00 13.00 18.00 25.00
34.00 45.00 58.00 73.00 90.00 109.00 130.00 153.00 178.00 13.25 16.25 21.25 28.25 37.25 48.25 61.25 76.25 93.25 112.25 133.25 156.25 181.25 17.00
20.00 25.00 32.00 41.00 52.00 65.00 80.00 97.00 116.00 137.00 160.00 185.00 21.25 24.25 29.25 36.25 45.25 56.25 69.25 84.25 101.25 120.25 141.25
164.25 189.25 26.00 29.00 34.00 41.00 50.00 61.00 74.00 89.00 106.00 125.00 146.00 169.00 194.00 31.25 34.25 39.25 46.25 55.25 66.25 79.25 94.25
111.25 130.25 151.25 174.25 199.25 37.00 40.00 45.00 52.00 61.00 72.00 85.00 100.00 117.00 136.00 157.00 180.00 205.00 43.25 46.25 51.25 58.25 67.25
78.25 91.25 106.25 123.25 142.25 163.25 186.25 211.25
rouge 2
1.25 4.25 9.25 16.25 25.25 36.25 1.25 3.25 7.25 13.25 21.25 31.25 43.25 3.25 6.25 11.25 18.25 27.25 38.25 4.25 6.25 10.25 16.25
24.25 34.25 46.25 7.25 10.25 15.25 22.25 31.25 42.25 9.25 11.25 15.25 21.25 29.25 39.25 51.25 13.25 16.25 21.25 28.25 37.25 48.25 16.25
18.25 22.25 28.25 36.25 46.25 58.25 21.25 24.25 29.25 36.25 45.25 56.25 25.25 27.25 31.25 37.25 45.25 55.25 67.25 31.25 34.25 39.25 46.25
55.25 66.25 36.25 38.25 42.25 48.25 56.25 66.25 78.25 43.25 46.25 51.25 58.25 67.25 78.25
bleu 1
0.50 2.50 6.50 12.50 20.50 30.50 42.50 2.50 4.50 8.50 14.50 22.50 32.50 44.50 6.50 8.50 12.50 18.50 26.50 36.50 48.50 12.50 14.50
18.50 24.50 32.50 42.50 54.50 20.50 22.50 26.50 32.50 40.50 50.50 62.50 30.50 32.50 36.50 42.50 50.50 60.50 72.50 42.50 44.50 48.50 54.50
62.50 72.50 84.50
bleu 2
2.50 8.50 18.50 32.50 50.50 72.50 2.50 6.50 14.50 26.50 42.50 62.50 86.50 6.50 12.50 22.50 36.50 54.50 76.50 8.50 12.50 20.50 32.50
48.50 68.50 92.50 14.50 20.50 30.50 44.50 62.50 84.50 18.50 22.50 30.50 42.50 58.50 78.50 102.50 26.50 32.50 42.50 56.50 74.50 96.50 32.50
36.50 44.50 56.50 72.50 92.50 116.50 42.50 48.50 58.50 72.50 90.50 112.50 50.50 54.50 62.50 74.50 90.50 110.50 134.50 62.50 68.50 78.50 92.50
110.50 132.50 72.50 76.50 84.50 96.50 112.50 132.50 156.50 86.50 92.50 102.50 116.50 134.50 156.50
vella-chemla@vellachemla-VGN-FW51MF-H:~/Desktop/accords$

```
#include <cstdlib>
#include <iostream>
#include <vector>
#include <math.h>
#include <stdio.h>
#include <stdlib.h>

#define BLACK    "\033[0;30m"
#define RED      "\033[0;31m"
#define GREEN    "\033[0;32m"
#define YELLOW   "\033[0;33m"
#define BLUE     "\033[0;34m"
#define PURPLE   "\033[0;35m"
#define CYAN     "\033[0;36m"
#define GREY     "\033[0;37m"

int main(int argc, char* argv[]) {
  int a, b, c, d, e, f, g, h ;
  int vaalaligne ;

  vaalaligne = -1 ;
  // jaune 11
  std::cout << "\033[0;33m" ;
  std::cout << "\n\njaune 11\n" ;
  for (a = 1 ; a <= 13 ; ++a)
    for (b = 1 ; b <= 13 ; ++b) {
      if (vaalaligne == 22) {std::cout << "\n" ; vaalaligne = 0 ;}
      else vaalaligne = vaalaligne+1 ;
      printf("%8.2f", (float) a*a+b*b) ;
    }

  vaalaligne = -1 ;
  // jaune 12
  std::cout << "\n\njaune 12\n" ;
  for (d = 1 ; d <= 13 ; ++d)
    for (c = 1 ; c <= d ; ++c) {
      if (vaalaligne == 22) {std::cout << "\n" ; vaalaligne = 0 ;}
      else vaalaligne = vaalaligne+1 ;
      printf("%8.2f", 4.0*(float)c*(float)c/4.0+4.0*(float)d*(float)d/4.0) ;
    }

  vaalaligne = -1 ;
  // jaune 21
  std::cout << "\n\njaune 21\n" ;
  for (e = 1 ; e <= 13 ; ++e)
    for (f = 1 ; f <= 13 ; ++f) {
      if (vaalaligne == 22) {std::cout << "\n" ; vaalaligne = 0 ;}
      else vaalaligne = vaalaligne+1 ;
      printf("%8.2f", 4.0*(float)e*(float)e/4.0+(float)f*(float)f) ;
    }

  vaalaligne = -1 ;
  // jaune 22
  std::cout << "\n\njaune 22\n" ;
  for (h = 1 ; h <= 13 ; ++h)
    for (g = 1 ; g <= h ; ++g)
      if (((g+h)%2) == 0) {
        if (vaalaligne == 22) {std::cout << "\n" ; vaalaligne = 0 ;}
        else vaalaligne = vaalaligne+1 ;
        printf("%8.2f", (float)g*(float)g/2.0+(float)h*(float)h/2.0) ;
      }

  vaalaligne = -1 ;
  std::cout << "\033[0;31m" ;
```

```
        //rouge 1
        std::cout << "\n\nrouge 1\n" ;
        for (e = 1 ; e <= 13 ; ++e)
          for (f = 1 ; f <= 13 ; ++f) {
            if (vaalaligne == 22) {std::cout << "\n" ; vaalaligne = 0 ;}
            else vaalaligne = vaalaligne+1 ;
            printf("%8.2f", (float)e*(float)e/4.0+(float)f*(float)f) ;
          }

        vaalaligne = -1 ;
        //rouge 2
        std::cout << "\n\nrouge 2\n" ;
        for (c = 1 ; c <= 13 ; ++c)
          for (d = 1 ; d <= 13 ; ++d)
            if (((c+d)%2) == 1) {
              if (vaalaligne == 22) {std::cout << "\n" ; vaalaligne = 0 ;}
              else vaalaligne = vaalaligne+1 ;
              printf("%8.2f", (float)c*(float)c/4.0+(float)d*(float)d/4.0) ;
            }

        vaalaligne = -1 ;
        std::cout << "\033[0;34m" ;
        // bleu 1
        std::cout << "\n\nbleu 1\n" ;
        for (c = 1 ; c <= 13 ; ++c)
          for (d = 1 ; d <= 13 ; ++d)
            if (((c % 2) == 1) && ((d % 2) == 1)) {
              if (vaalaligne == 22) {std::cout << "\n" ; vaalaligne = 0 ;}
              else vaalaligne = vaalaligne+1 ;
              printf("%8.2f", (float)c*(float)c/4.0+(float)d*(float)d/4.0) ;
            }

        vaalaligne = -1 ;
        // bleu 2
        std::cout << "\n\nbleu 2\n" ;
        for (g = 1 ; g <= 13 ; ++g)
          for (h = 1 ; h <= 13 ; ++h)
            if (((g+h)%2) == 1) {
              if (vaalaligne == 22) {std::cout << "\n" ; vaalaligne = 0 ;}
              else vaalaligne = vaalaligne+1 ;
              printf("%8.2f", (float)g*(float)g/2.0+(float)h*(float)h/2.0) ;
            }

        std::cout << "\n" ;
}
```

Courbes et points entiers (Denise Vella-Chemla, 18.1.2017)

On avait proposé la définition suivante pour les nombres premiers : un nombre p est premier si et seulement si toute fraction rationnelle de la forme $\frac{p-x}{x}$ avec x entier compris strictement entre 1 et p n'est pas égale à un nombre entier.

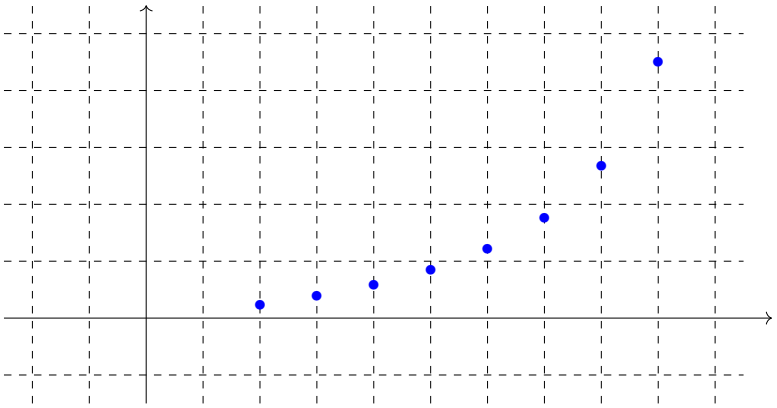
En mettant les nombres en regard à la manière dont Gauss l'a fait pour trouver, enfant, à la demande de son professeur, que la somme des 100 premiers entiers vaut 5050, on comprend aisément la raison d'une telle possibilité de définition.

7 est premier car aucune des fractions de l'ensemble $\left\{\frac{5}{2}, \frac{4}{3}, \frac{3}{4}, \frac{2}{5}\right\}$ n'est entière.

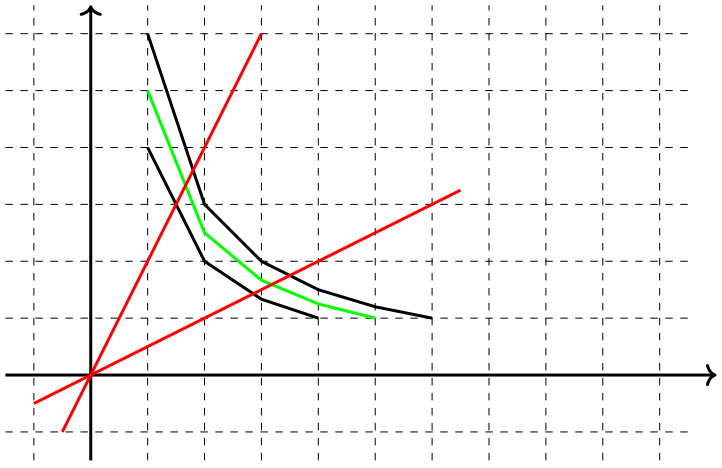
De même, 11, à qui est associé l'ensemble de fractions $\left\{\frac{9}{2}, \frac{8}{3}, \frac{7}{4}, \frac{6}{5}, \frac{5}{6}, \frac{4}{7}, \frac{3}{8}, \frac{2}{9}\right\}$, est premier.

Par contre, 6 est composé car l'ensemble qui lui est associé, $\left\{\frac{4}{2}, \frac{3}{3}, \frac{2}{4}\right\}$, contient une fraction entière au moins, $\frac{4}{2}$ par exemple.

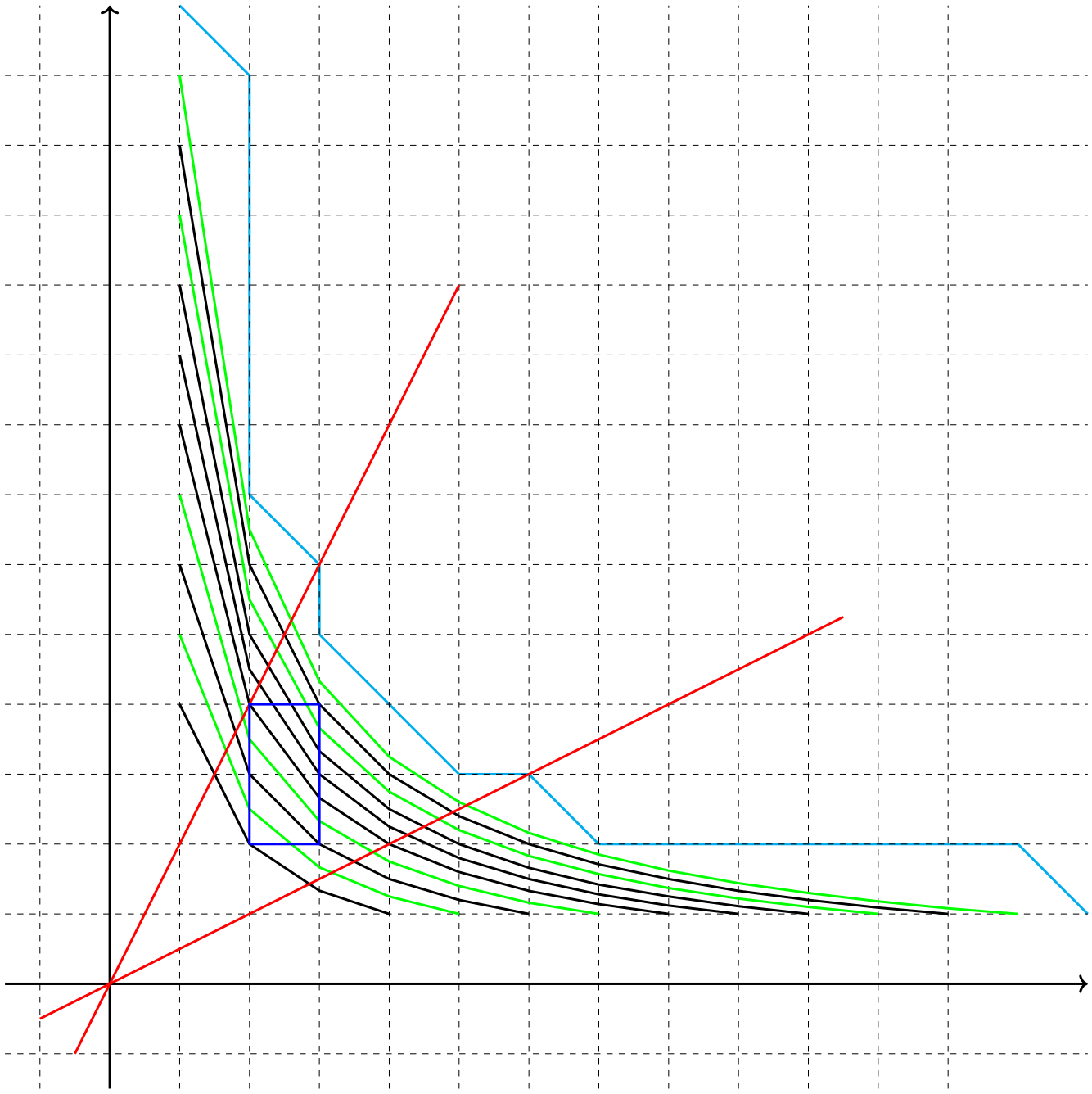
Si l'on représente chaque fraction de la forme $\frac{a}{b}$ par le point du plan de coordonnées $\left(a, \frac{a}{b}\right)$, voyons ci-dessous, les points d'ordonnées non entières, appartenant à une hyperbole, associés au nombre pemier 11.



Il est plus judicieux de représenter les hyperboles de la forme $xy = n$ et de considérer la définition littérale de la primalité qui définit un nombre premier comme étant le seul produit d'1 et de lui-même. L' hyperbole verte apparaissant sur le graphique ci-dessous correspond au nombre premier 5 entre celles des nombres composés 4 et 6. Elle ne contient aucun point entier entre les droites $y = 2x$ et $y = x/2$.

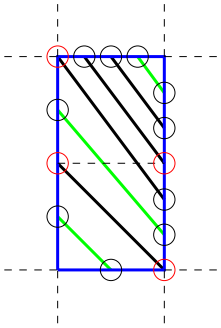


Courbe complétée jusqu'à $n = 13$ (5, 7, 11 et 13, premiers, en vert).



Imaginerait-on une méthode géométrique qui permettrait de dénombrer exactement le nombre de nombres premiers compris entre 2 nombres ?

Focalisons-nous sur la portion du plan encadrée en bleu sur le graphique précédent et agrandissons-la.



Puisque les coins bas-gauche et haut-droit ont pour coordonnées (2,2) et (3,4), on sait que passent dans la portion encadrée $12-4-1=7$ hyperboles, ce qui correspond à 14 points d'entrée/sortie dans la zone. Or il reste 4 "coins" par lesquels peuvent passer des hyperboles (on les a entourés en rouge) qui soustraient 8 entrées ou sorties (un seul point entier suffit à éliminer toute l'hyperbole). Il reste 6 entrées ou sorties ne passant pas par des "coins", ce qui divisé par 2 amène le nombre de 3 nombres premiers entre 4 et 12 (ces nombres premiers sont 5, 7 et 11).

Les hyperboles successives n'ont aucun point commun. Cette méthode de comptage semble également fonctionner pour une zone avec points entiers intérieurs (ne serait-ce qu'un seul). Prenons la zone carrée de 2×2 entre les points bas-gauche $(3,5)$ et haut-droit $(5,7)$. 19 hyperboles (correspondant à $5\times 7-3\times 5-1$ passent dans la zone (soient 38 entrées/sorties). Les 7 "coins" éliminent 14 entrées ou sorties, ce qui correspondrait à 12 $(=(38-14)/2)$ nombres compris entre 15 et 35 qui ne sont divisibles ni par 3, ni par 4, ni par 5.

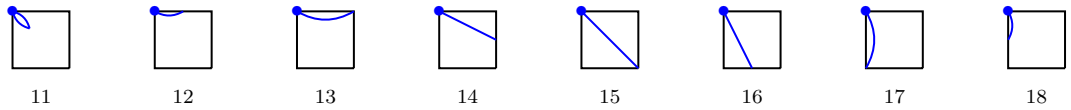
Ce qui est surprenant, c'est qu'on peut compter de la même manière, sous prétexte qu'il s'agit dans tous les cas d'étudier les divisibilités par 2 et 3 de nombres assez petits, le nombre de nombres premiers compris entre 4 et 12 (zone bleue déjà délimitée) ou bien le nombre de nombres premiers compris entre 8 et 18 (en utilisant la zone de même forme qui a pour coin bas-gauche (2,4) et coin haut-droit (3,6)), ou encore le nombre de nombres premiers compris entre 6 et 16 (zone de coin bas gauche (3,2) et de coin haut-droit (4,4)). Les 3 nombres premiers sont 5, 7 et 11 dans le premier cas, 11, 13 et 17 dans le second et 7, 11 et 13 dans le troisième.

Pistes : en terme d'invariants de comptage, on doit peut-être tenir compte du fait que ce qui sort par le bas d'une maille entre par le haut dans la maille qui est au-dessous ou bien que ce qui sort par la droite d'une maille entre par la gauche dans la maille qui en est à droite, etc. Il faut aussi peut-être avoir trois autres choses à l'esprit :
- le théorème de Pick d'une part (qui permet de relier le nombre de points entiers à l'intérieur d'un polygone, le nombre de points entiers qui sont sur sa bordure et l'aire de ce polygone) ;
- le fait de conserver l'aire mais de jouer sur un principe de "vases communicants" entre ensemble des points intérieurs et ensemble des points de la bordure lorsqu'on effectue des découpages-collages de petits triangles moitiés de mailles en les accolant à leur symétrique (ces petits triangles moitié de mailles sont en miroir de part et d'autre de la diagonale principale) ;
- le fait d"'enrober au plus juste" les hyperboles successives dans des polygones de périmètre minimum (on a dessiné en turquoise un tel polygone) selon des règles simples déterministes et fonction de la manière dont la dernière hyperbole traverse ses mailles.

Traverser un carré (Denise Vella-Chemla, 21.1.2017)

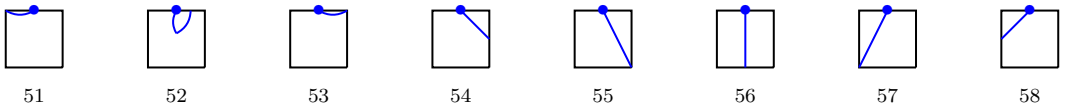
On étudie les différentes possibilités pour les points d'hyperboles d'équations de la forme $xy = n$ de traverser une maille-unité du plan. Le carré a 4 sommets, 4 côtés. On voit quels sont les seuls cas conservés parmi les $64 = 8 \times 8$ cas possibles.

1) l'hyperbole entre dans la maille (au point bleu) par le coin haut-gauche. Seuls 3 cas sur 8 sont conservés, les cas $14, 15$ et 16.



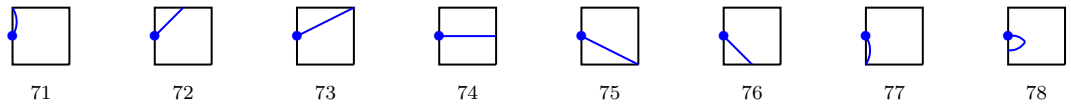
2) 3) et 4) Si l'hyperbole entre dans la maille par l'un des 3 autres coins, on se ramène au cas 1) ci-dessus.

5) L'hyperbole entre dans la maille par le côté haut : seuls 3 cas sur 8 sont conservés, les cas $54, 55$ et 56.



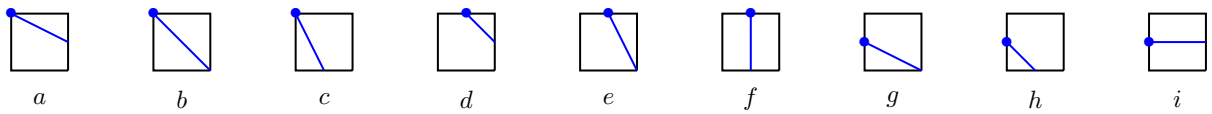
6) L'hyperbole ne peut entrer dans la maille par le côté bas.

7) L'hyperbole entre dans la maille par le côté gauche : seuls 3 cas sur 8 sont conservés, les cas $74, 75$ et 76.



8) Si l'hyperbole entre dans la maille par le côté droit, on se ramène au cas 7).

Revoyons les 9 possibilités :



Remarque : la possibilité b) correspond aux points proches de la diagonale (qui minimisent la différence $y - x$ lorsque n est de la forme $n(n + 1)$).

On doit étudier si les contraintes de placement de 2 hyperboles successives $xy = n$ et $x'y' = n + 1$ limiteraient le nombre de cas à envisager qui s'élève au départ à $81 = 9 \times 9$.

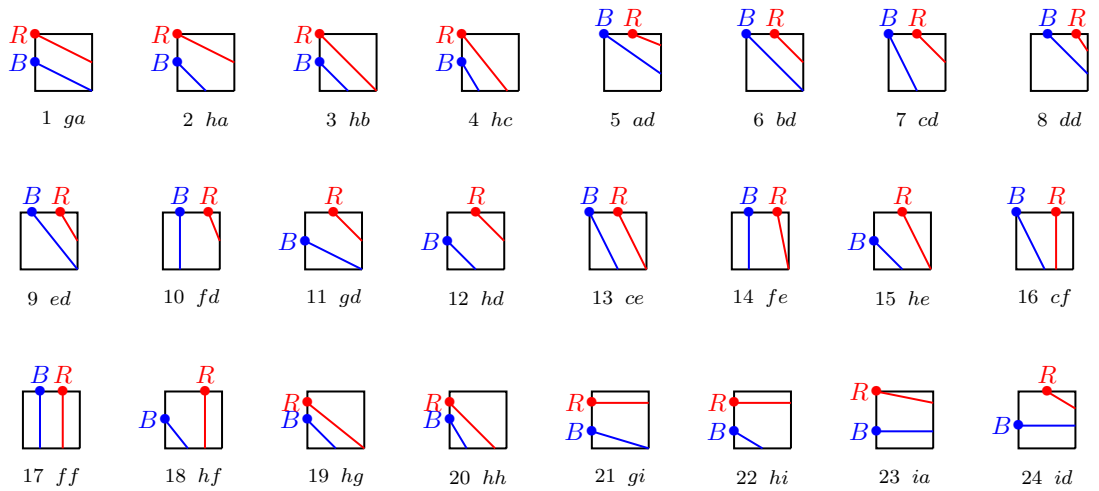
De visu en plaçant les configurations dans une maille, on arrive d'ores et déjà à réduire le nombre de cas possibles à 24 sur 81.

En effet, un certain nombre d'impossibilités provient du fait que deux hyperboles associées à deux entiers successifs partageraient un coin de maille, ce qui est impossible. C'est le cas pour les configurations : aa, ba, ca, ab, bb, cb, gb, ac, bc, cc, be, ee, ge et gg.

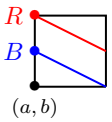
Un autre type d'impossibilités provient du fait que deux hyperboles associées à deux entiers successifs se croisent dans la maille, ce qui est impossible. C'est le cas pour les configurations : gc, ae, de, af, bf, df, ef, gf, gh, ai, bi, ci, ei, fi, ib, ic, ie, if, ig et ih.

Un troisième type d'impossibilités provient du fait qu'il est impossible que l'entrée dans la maille de la seconde hyperbole (d'équation $xy = n = 1$) s'effectue à gauche ou au-dessous de l'entrée de la première hyperbole dans la maille (d'équation $x'y' = n$). C'est le cas pour les configurations : da, ea, fa, db, eb, fb, dc, ec, fc, ag, bg, cg, dg, eg, fg, ah, bh, ch, dh, eh, fh et di.

Les 24 cas restant sont dessinés ci-dessous, l'hyperbole associée à n est bleue, celle associée à $n+1$ est rouge :



Pour réduire le nombre de variables qu'on va essayer de lier par des invariants, on utilise le fait que lorsque deux points sont soit sur le côté gauche du carré, soit sur son côté droit, ils ont même abscisse et que lorsque deux points sont soit sur le côté haut du carré, soit sur son côté bas, ils ont même ordonnée pour étudier chacune des 24 possibilités afin d'en éliminer certaines. Voyons un exemple : trouvons une contradiction sur la possibilité (1) qu'on a répertoriée (le coin bas-gauche de la maille a pour coordonnées (a, b)).

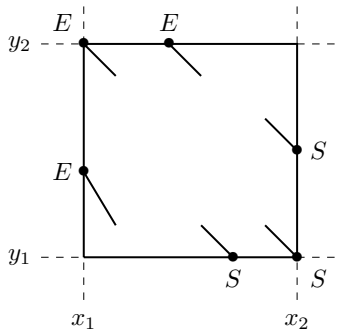


Les égalités ou inégalités sur les points d'entrée-sortie sont :

$$\begin{cases} (a+1)b = n \\ a(b+\varepsilon) = n \\ a(b+1) = n+1 \\ (a+1)(b+\delta) = n+1 \\ 0 < \varepsilon < 1 \\ 0 < \delta < 1 \end{cases}$$

De la première et la troisième égalité réécrites $ab + b = n$ et $ab + a = n + 1$, on obtient $a = b + 1$. De la seconde égalité, on obtient $\varepsilon = \frac{n-ab}{a} = \frac{n-a(a-1)}{a}$. On remplace ε par cette valeur dans l'inégalité $0 < \varepsilon < 1$, on obtient $0 < \frac{n-a(a-1)}{a} < 1$, soit $0 < n-a(a-1) < a$ en multipliant par a puis $a(a-1) < n < a+a(a-1)$, i.e. $a(a-1) < n < a^2$ qui est une impossibilité dans la mesure où $a|n$ (voir le point B de l'hyperbole d'équation $xy = n$) et où il n'y a pas de nombre divisible par a qui soit strictement compris entre $a(a-1)$ et a^2.

Pour calculer par programme les valeurs des variables correspondant aux différents cas possibles (pour les nombres n inférieurs à 100 par exemple) à la recherche d'invariants qui lieraient localement les variables associées à deux hyperboles successives, on étudie les différentes manières qu'a une courbe de traverser une maille ; les 3 possibilités différentes d'entrer dans la maille ci-dessous sont symbolisées par des E pour entrée et les 3 possibilités de sortie par des S.



Si $f(x_1)$ est strictement compris entre y_1 et y_2 alors la courbe entre dans la maille par le côté gauche. Elle y entre par le coin haut-gauche si $f(x_1) = y_2$.

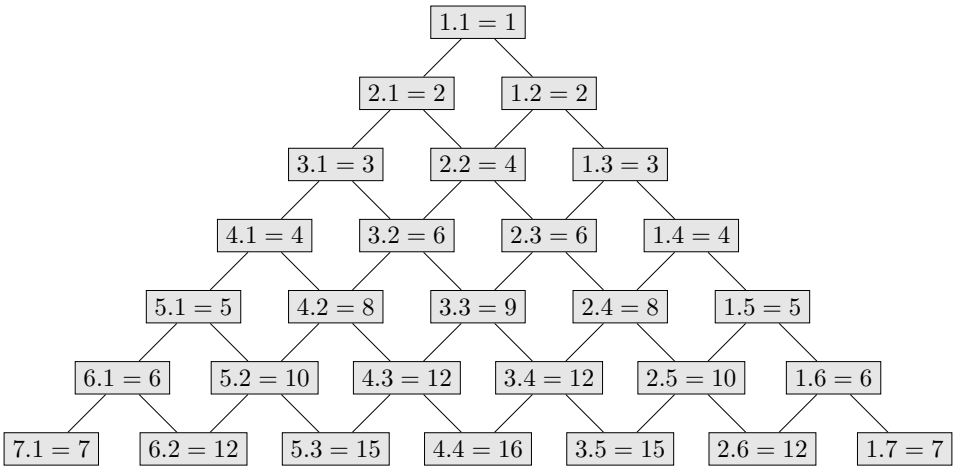
(Sinon) Si $f^{-1}(y_2)$ est compris strictement entre x_1 et x_2 alors la courbe entre dans la maille par le côté haut. Elle y entre aussi par le coin haut-gauche si $f^{-1}(y_2) = x_1$.

Si $f(x_2)$ est strictement compris entre y_1 et y_2 alors la courbe sort de la maille par le côté droit. Elle en sort par le coin bas-droit si $f(x_2) = y_1$.

(Sinon) Si $f^{-1}(y_1)$ est compris strictement entre x_1 et x_2 alors la courbe sort de la maille par le côté bas. Elle en sort aussi par le coin bas-droit si $f^{-1}(y_1) = x_2$.

Essai (Denise Vella-Chemla, 5.2.2017)

Graphe des produits de 2 entiers : un noeud (x, y) a 2 fils $(x+1, y)$ et $(x, y+1)$.



C'est une table de Pythagore, autrement représentée. Sur chaque chemin du graphe ci-dessus, les nombres sont strictement ordonnés. Le problème est qu'on n'arrive pas à situer les nombres d'un chemin par rapport à ceux d'un autre chemin et de ce fait, à identifier certains sommets du graphe.

L'opération qui fait passer d'un point $\begin{pmatrix} x_1 \\ \\ y_1 \end{pmatrix}$ d'une hyperbole à un autre point de la même hyperbole $\begin{pmatrix} x_2 \\ \\ y_2 \end{pmatrix}$ consiste par exemple à multiplier la première coordonnée par un scalaire et à diviser la deuxième coordonnée par le scalaire en question, pour conserver le produit. On transforme $\begin{pmatrix} x_1 \\ \\ y_1 \end{pmatrix}$ en $\begin{pmatrix} \lambda x_1 \\ \\ \frac{y_1}{\lambda} \end{pmatrix}$. Cette transformation peut être représentée par une matrice de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix}$.

On pourrait peut-être trouver exactement le nombre de nombres premiers inférieurs à un nombre donné si on savait quotienter l'ensemble des points du plan par cette transformation, tous les produits égaux à un même nombre étant identifiés.

On a par ce cheminement identifié une méthode qui compte le nombre de nombres premiers inférieurs strictement à un nombre donné et qui est conditionnée par le fait qu'on sache quotienter par la relation d'équivalence qui lient deux points dont les produits des coordonnées sont égaux.

Illustrons cette méthode sur deux exemples. Le premier point est $A = \begin{pmatrix} 4 \\ 4 \end{pmatrix}$. On cherche le nombre de points entiers sous l'hyperbole d'équation $xy = 16$, à gauche de A et d'abscisse plus grande que 1. C'est l'ensemble des points

$$\begin{aligned} & \left\{ \begin{pmatrix} x' \\ y' \end{pmatrix} \text{ avec x}' < \text{x et} x'\text{y}' < \text{xy} \right\} \cup \left\{ \begin{pmatrix} x' \\ y' \end{pmatrix} \text{ avec y}' < \text{y et x}'\text{y}' < \text{xy} \right\} . \\ = \quad & \{3.2, 3.3, 3.4, 3.5, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 4.3, 4.2\} \end{aligned}$$

La relation d'équivalence identifie 2.3 et 3.2 ainsi que 2.6, 3.4 et 4.3 ou 2.4 et 4.2. Il reste 8 produits, ce qui permet de trouver 5 $(= 16 - 3 - 8)$ nombres premiers strictement inférieurs à 16.

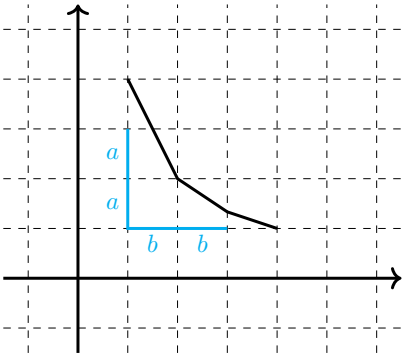
Le second point est $B = \begin{pmatrix} 5 \\ 6 \end{pmatrix}$. On cherche le nombre de points entiers sous l'hyperbole d'équation $xy = 30$, à gauche de B et d'abscisse plus grande que 1. On trouve l'ensemble de points

$$\begin{aligned} & \{5.2, 5.3, 5.4, 5.5, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, \\ & 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11, 2.12, 2.13, 2.14\} \end{aligned} .$$

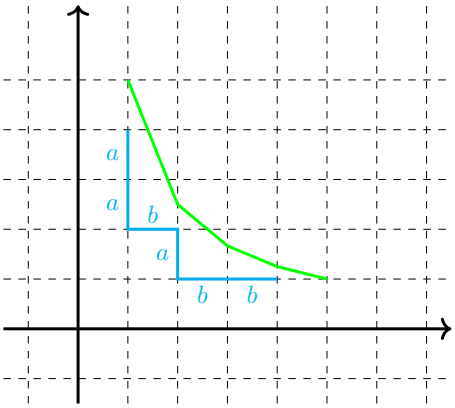
Les identifications de points permettent d'aboutir à 18 classes de points différentes et ainsi à 30-3-18=9 nombres premiers de 3 à 29.

Hyperboles et mots (Denise Vella-Chemla, 14.2.2017)

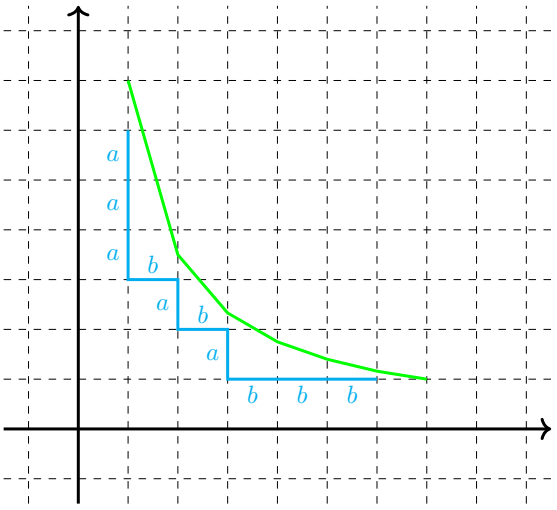
Hier, dans une note dans laquelle il était également question de mots de billard, était fournie la définition d'un mot de Christoffel. C'est un mot sur un alphabet de deux lettres qui "colle au plus près" à une courbe (par le dessus ou par le dessous). Voyons des exemples :
- *mot de l'hyperbole discrétisée associé à* $n = 4$ *: aabb.*



- *mot de l'hyperbole discrétisée associé à* $n = 5$ *: aababb.*



- *mot de l'hyperbole discrétisée associé à* $n = 7$ *: aaababbbb.*



Du fait de la symétrie des hyperboles, qui se traduit en mot par le fait que les mots sont de longueur paire et ont leur fin symétrique de leur début à inversion des lettres près, on ne conserve comme mot associé à un nombre que le début des mots présentés ici (un mot de $n-2$ lettres pour caractériser n ; on montre cette symétrie sur le dernier graphique ci-dessous par la diagonale rouge et la fin du mot en pointillé).

- *mot de l'hyperbole discrétisée associé à* $n = 13$ *: aaaaaabaaba.*

On calcule par programme les mots des 100 premiers entiers naturels, à la recherche de régularités.

3	a
4	aa
5	aab
6	$aaab$
7	$aaaba$
8	$aaaaba$
9	$aaaabaa$
10	$aaaaabab$
11	$aaaaabaab$
12	$aaaaaabaab$
13	$aaaaaabaaba$
14	$aaaaaaabaaba$
15	$aaaaaaabaaaba$
16	$aaaaaaaabaabaa$
17	$aaaaaaaabaaabab$
18	$aaaaaaaaabaaabab$
19	$aaaaaaaaabaaabaab$
20	$aaaaaaaaaabaaabaab$
21	$aaaaaaaaaabaaaababa$
22	$aaaaaaaaaaabaaabaaba$
23	$aaaaaaaaaaabaaaabaaba$
24	$aaaaaaaaaaaabaaaabaaba$
25	$aaaaaaaaaaaabaaaabaabaa$
26	$aaaaaaaaaaaaabaaaabaabab$
27	$aaaaaaaaaaaaabaaaaabaabab$
28	$aaaaaaaaaaaaaabaaaabaaabab$
29	$aaaaaaaaaaaaaabaaaaabaabaab$
30	$aaaaaaaaaaaaaaabaaaaabaabaab$
31	$aaaaaaaaaaaaaaabaaaaabaaababa$
32	$aaaaaaaaaaaaaaaabaaaaabaaababa$
33	$aaaaaaaaaaaaaaaabaaaaaabaabaaba$
34	$aaaaaaaaaaaaaaaaabaaaaabaaabaaba$
35	$aaaaaaaaaaaaaaaaabaaaaaabaaabaaba$
36	$aaaaaaaaaaaaaaaaaabaaaaaabaaababaa$
37	$aaaaaaaaaaaaaaaaaabaaaaaabaaabaabab$
38	$aaaaaaaaaaaaaaaaaabaaaaaabaaabaabab$
39	$aaaaaaaaaaaaaaaaaabaaaaaabaaabaabab$
40	$aaaaaaaaaaaaaaaaaaabaaaaaabaaaabaabab$
41	$aaaaaaaaaaaaaaaaaaabaaaaaaabaaabaabaab$
42	$aaaaaaaaaaaaaaaaaaaabaaaaaaabaaabaabaab$
43	$aaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaababa$
44	$aaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaababa$
45	$aaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaabaaababa$
46	$aaaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaabaaba$
47	$aaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaabaaba$
48	$aaaaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaabaaba$
49	$aaaaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaaababaa$
50	$aaaaaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaaababab$
51	$aaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaabaabab$
52	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaaabaabaabab$
53	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaaabaabab$
54	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaaabaabab$
55	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaaabaaabaabab$
56	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaaabaabaabaab$
57	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaaabaababa$
58	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaaabaaabaababa$
59	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaaabaaabaababa$
60	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaaabaaabaababa$

61	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaaba*
62	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaaba*
63	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaaba*
64	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabababaa*
65	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaababab*
66	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaaababab*
67	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaabab*
68	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaabab*
69	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaabab*
70	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaabab*
71	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaaabababaab*
72	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaaababaab*
73	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaababa*
74	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaababa*
75	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaababa*
76	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaababa*
77	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaababa*
78	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabababaa*
79	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaabaa*
80	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaabaa*
81	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaabaa*
82	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabababab*
83	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabababab*
84	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabababab*
85	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabababab*
86	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaabab*
87	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaabab*
88	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaabab*
89	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaabaab*
90	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabababaab*
91	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabababa*
92	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*
93	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*
94	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*
95	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*
96	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*
97	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*
98	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*
99	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*
100	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaaabaabaaba*

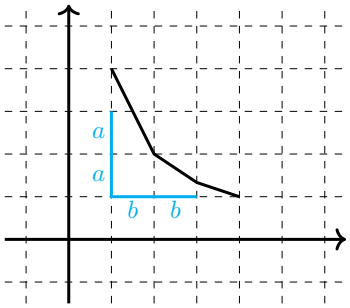
3	*a*
5	*aab*
7	*aaaba*
9	*aaaabaa*
11	*aaaaabaab*
13	*aaaaaabaaba*
15	*aaaaaaabaaaba*
17	*aaaaaaaabaaabab*
19	*aaaaaaaaabaaabaab*
21	*aaaaaaaaaabaaaababa*
23	*aaaaaaaaaaabaaaabaaba*
25	*aaaaaaaaaaaabaaaabaabaa*
27	*aaaaaaaaaaaaabaaaaabaabab*
29	*aaaaaaaaaaaaaabaaaaabaabaab*
31	*aaaaaaaaaaaaaaabaaaaabaaababa*
33	*aaaaaaaaaaaaaaaabaaaaaabaabaaba*
35	*aaaaaaaaaaaaaaaaabaaaaaabaaabaaba*
37	*aaaaaaaaaaaaaaaaaabaaaaaabaaabaabab*
39	*aaaaaaaaaaaaaaaaaaabaaaaaaabaaabaabab*
41	*aaaaaaaaaaaaaaaaaaaabaaaaaaabaaabaabaab*
43	*aaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaababa*
45	*aaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaabaaababa*
47	*aaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaabaaba*
49	*aaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaaababaa*
51	*aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaabaaaabaabaabab*
53	*aaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaabaaaabaaabaabab*
55	*aaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaabaaaaabaaababaab*
57	*aaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaabaaabaababa*
59	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaababa*
61	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaabaaaaabaaabaabaaba*
63	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaabaaaaabaaabaabaaba*
65	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaabaaaaabaaaabaababab*
67	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaabaaaaaabaaabaabaabab*
69	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaabaaaaabaaaabaabaabab*
71	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaabaaaaaabaaabaaababaab*
73	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaabaaaaaabaaaabaabaababa*
75	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaabaaaaaabaaaabaabaababa*
77	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaabaaaaaabaaaabaaabaababa*
79	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaabaaaaaaabaaaabaabaabaaba*
81	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaabaaaaaabaaaabaaabaababaa*
83	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaabaaaaaaabaaaabaaabaababab*
85	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaabaaaaaaabaaaaabaabaabaabab*
87	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaaabaaaaaaabaaaabaaabaabaabab*
89	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaaabaaaaaaabaaaaabaaabaababaab*
91	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaaabaaaaaaaabaaaabaaabaaabababa*
93	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaaaabaaaaaaabaaaaabaaabaabaababa*
95	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaaaabaaaaaaaabaaaaabaaabaabaababa*
97	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaaaabaaaaaaaabaaaaabaaabaaababaaba*
99	*aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaaaaaaaaaaabaaaaaaaabaaaaabaaabaabaabaaba*

Hyperboles et mots

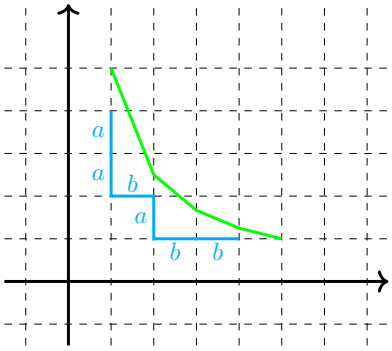
Denise Vella-Chemla

16.2.17

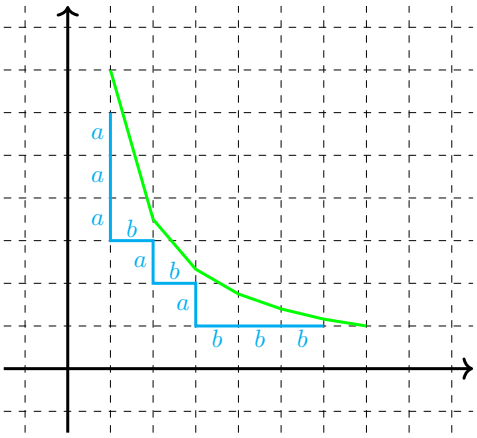
Un mot de Christoffel [1] est un mot sur un alphabet de deux lettres qui "colle au plus près" à une courbe par segments liant des points discrets (par le dessus ou par le dessous). Voyons des exemples :
- *mot de l'hyperbole discrétisée associé à* $n = 4$ *: aabb.*



- *mot de l'hyperbole discrétisée associé à* $n = 5$ *: aababb.*

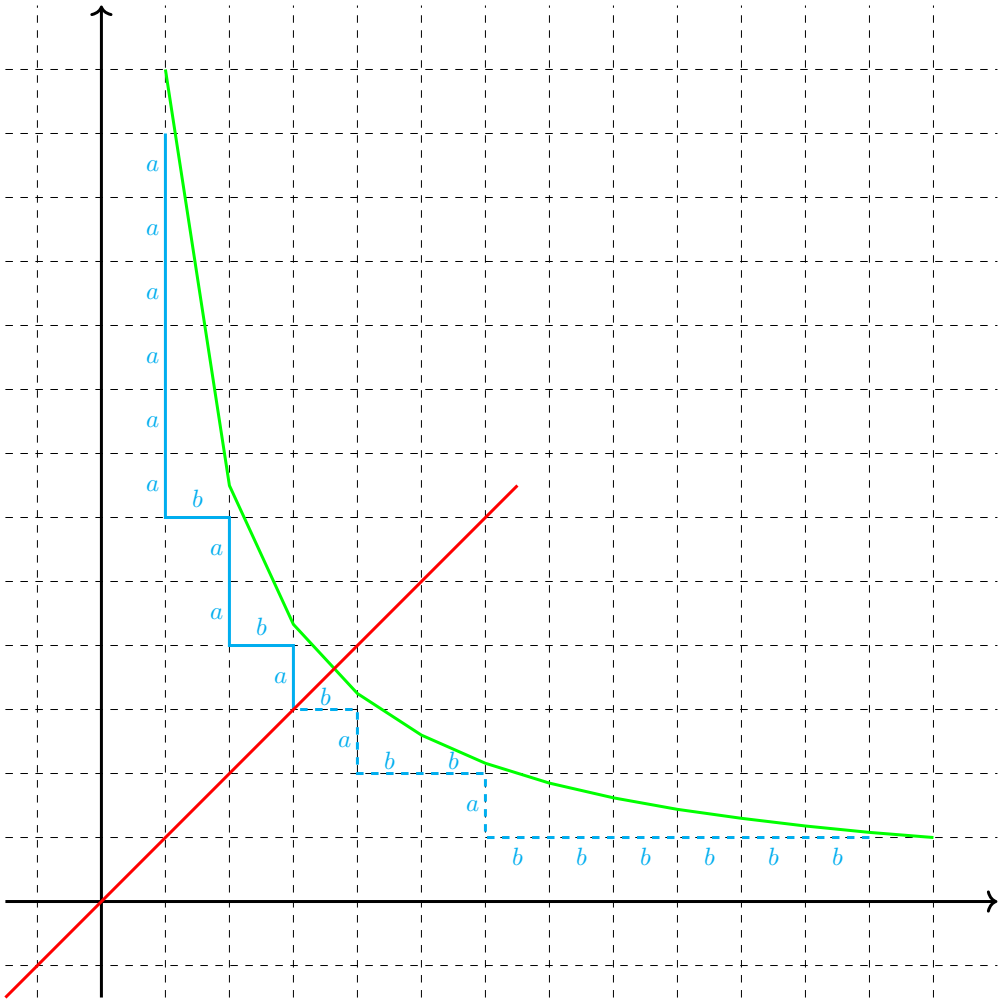


- *mot de l'hyperbole discrétisée associé à* $n = 7$ *: aaababbbb.*



Du fait de la symétrie des hyperboles, qui se traduit en mot par le fait que les mots sont de longueur paire et ont leur fin symétrique de leur début à inversion des lettres près, on ne conserve comme mot associé à un nombre que le début des mots présentés ici (un mot de $n-2$ lettres pour caractériser n ; on montre cette symétrie sur le dernier graphique ci-dessous par la diagonale rouge et la fin du mot en pointillé).

- *mot de l'hyperbole discrétisée associé à* $n = 13$ *: aaaaaabaaba.*



On calcule par programme les mots des 500 premiers entiers naturels, à la recherche de régularités. On fournit ci-dessous les mots des nombres jusqu'à 50.

3	a
4	aa
5	aab
6	$aaab$
7	$aaaba$
8	$aaaaba$
9	$aaaabaa$
10	$aaaaabab$
11	$aaaaabaab$
12	$aaaaaabaab$
13	$aaaaaabaaba$
14	$aaaaaaabaaba$
15	$aaaaaaabaaaba$
16	$aaaaaaaabaabaa$
17	$aaaaaaaabaaabab$
18	$aaaaaaaaabaaabab$
19	$aaaaaaaaabaaabaab$
20	$aaaaaaaaaabaaabaab$
21	$aaaaaaaaaabaaaababa$
22	$aaaaaaaaaaabaaabaaba$
23	$aaaaaaaaaaabaaaabaaba$
24	$aaaaaaaaaaaabaaaabaaba$
25	$aaaaaaaaaaaabaaaabaabaa$
26	$aaaaaaaaaaaaabaaaabaabab$
27	$aaaaaaaaaaaaabaaaaabaabab$
28	$aaaaaaaaaaaaaabaaaabaaabab$
29	$aaaaaaaaaaaaaabaaaaabaabaab$
30	$aaaaaaaaaaaaaaabaaaaabaabaab$
31	$aaaaaaaaaaaaaaabaaaaabaaababa$
32	$aaaaaaaaaaaaaaaabaaaaabaaababa$
33	$aaaaaaaaaaaaaaaabaaaaaabaabaaba$
34	$aaaaaaaaaaaaaaaaabaaaaabaaabaaba$
35	$aaaaaaaaaaaaaaaaabaaaaaabaaabaaba$
36	$aaaaaaaaaaaaaaaaaabaaaaaabaaababaa$
37	$aaaaaaaaaaaaaaaaaabaaaaaabaaabaabab$
38	$aaaaaaaaaaaaaaaaaaabaaaaaabaaabaabab$
39	$aaaaaaaaaaaaaaaaaaabaaaaaaabaaabaabab$
40	$aaaaaaaaaaaaaaaaaaaabaaaaaabaaaabaabab$
41	$aaaaaaaaaaaaaaaaaaaabaaaaaaabaaabaabaab$
42	$aaaaaaaaaaaaaaaaaaaaabaaaaaaabaaabaabaab$
43	$aaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaababa$
44	$aaaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaababa$
45	$aaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaabaaababa$
46	$aaaaaaaaaaaaaaaaaaaaaaabaaaaaaabaaaabaabaaba$
47	$aaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaabaaba$
48	$aaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaabaaba$
49	$aaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaaababaa$
50	$aaaaaaaaaaaaaaaaaaaaaaaaabaaaaaaaabaaaabaaababab$

Les $n/2$ premières lettres sont toutes des a. Dans la suite, les lettres b servent de séparateurs. On écrit un nouveau programme qui compte les nombres de lettres a dans les paquets de a successifs. Le résultat de ce programme est fourni pour les nombres jusqu'à 100 en annexe 2. Ci-dessous, les nombres de a pour les mots du tableau précédent (en deuxième colonne dans chaque sous-partie du tableau, p signifie premier et c composé).

			11	p	2	21	c	4 1 1	31	p	5 3 1 1	41	p	7 3 2 2
			12	c	2	22	c	3 2 1	32	c	5 3 1 1	42	c	7 3 2 2
3	p		13	p	2 1	23	p	4 2 1	33	c	6 2 2 1	43	p	7 4 2 1 1
4	c		14	c	2 1	24	c	4 2 1	34	c	5 3 2 1	44	c	7 4 2 1 1
5	p		15	c	3 1	25	c	4 2 2	35	c	6 3 2 1	45	c	8 3 3 1 1
6	c		16	c	2 2	26	c	4 2 1	36	c	6 3 1 2	46	c	7 4 2 2 1
7	p	1	17	p	3 1	27	c	5 2 1	37	p	6 3 2 1	47	p	8 4 2 2 1
8	c	1	18	c	3 1	28	c	4 3 1	38	c	6 3 2 1	48	c	8 4 2 2 1
9	c	2	19	p	3 2	29	p	5 2 2	39	c	7 3 2 1	49	c	8 4 3 1 2
10	c	1	20	c	3 2	30	c	5 2 2	40	c	6 4 2 1	50	c	8 4 3 1 1

On découvre que les nombres de a du mot d'un nombre impair premier sont tous identiques aux nombres de a du mot de son successeur, et que cela n'est pas le cas pour les nombres de a du mot d'un nombre impair composé. Cela est dû au fait que l'hyperbole d'un nombre premier ne passe que par des points non-entiers du réseau (hormis les points triviaux $(1, n)$ et $(n, 1)$). L'hyperbole du successeur d'un nombre premier, quant à elle, passe par des points entiers du réseau mais cela ne suffit pas à modifier le mot de Christoffel qui ne se voit qu'ajouter un a au tout début (dans la première partie de $n/2$ lettres qu'on a choisi de négliger). Le comptage des lettres fait sauter cela aux yeux alors qu'il est plus difficile de le constater directement sur les suites confuses de a et b du tableau en page précédente.

On est ainsi à nouveau (cf le travail effectué autour de la conjecture de Goldbach) en train de compter des nombres d'assertions logiques : ici, elles sont de la forme : $n \leqslant (x+1)y$.

Voyons ces assertions logiques sur des exemples : 7, nombre premier, a le même mot constitué d'une seule lettre a que son successeur 8 parce que $7 \leqslant (2+1).3$ est une inégalité de même sens que $8 \leqslant (2+1).3$.

De même, 11, nombre premier, a le même mot constitué de 2 lettres a que son successeur 12 parce que les inégalités $11 \leqslant (2+1).5$ et $12 \leqslant (2+1).5$ sont de même sens, de même que les inégalités $11 \leqslant (2+1).4$ et $12 \leqslant (2+1).4$.

Par contre, pour ne prendre qu'un exemple, 27 est composé car son mot est différent du mot de son successeur. Il y a passage d'une lettre a à une lettre b par exemple du fait de l'inversion de sens des 2 inégalités $27 \leqslant (2+1).9$ et $28 > (2+1).9$.

Les scans de la première et la dernière page de l'exécution du programme fourni en annexe présentent :
- la découverte de l'égalité des mots des nombres premiers inférieurs à 60 et du mot de leur successeur[1] ;
- la détection des inversions de lettres pour les nombres composés de 450 à 500[2].

La méthode proposée procède en trois étapes :
- la première consiste à calculer les assertions logiques pour un nombre donné ainsi que pour son successeur ;
- la seconde compte les assertions positives successives (les longueurs des paquets de lettres a) ;
- la troisième consiste à comparer les nombres obtenus.

La première étape est le calcul de l'application de $\mathbb{N}^3$ dans $\mathbb{B}$ qui associe à tout triplet de nombres (n, x, y) la valeur booléenne de l'inégalité $n \leqslant (x+1)y$.
La comparaison du sens des inégalités (i.e. de deux booléens) est réalisée sur l'espace entier par une application de $\mathbb{B} \times \mathbb{B}$ dans $\mathbb{B}$.
L'opération d'égalité $b1 = b2$ qui associe à 2 booléens $b1$ et $b2$ un troisième booléen b qui vaut 1 si $b1$ et $b2$ sont tous deux égaux à 1 ou bien tous deux égaux à 0 s'écrit :

$$(b1 = b2) = (\neg b1 \vee b2) \wedge (\neg b2 \vee b1).$$

Le comptage des longueurs des séquences de a de la seconde étape s'effectue classiquement (arithmétique de Peano). Aux nombres compris entre $n^2 + n + 1$ et $n^2 + 3n + 2$ (on avait remarqué que le nombre de paquets de a était augmenté de 1 selon des cycles de plus en plus longs, liés à la suite des nombres pairs successifs, d'où ces formules), sont associés $n - 1$ nombres qui sont les tailles des paquets successifs de lettres a.

La comparaison de la troisième étape est le calcul d'une application de $\mathbb{N}^2$ dans $\mathbb{B}$ qui associe à tout couple de nombres (x, y) la valeur booléenne de l'égalité $x = y$.

On pense avoir fourni ici tous les ingrédients nécessaires à une manière plutôt "syntaxique" de tester la primalité des entiers.

Bibliographie :

[1] Jean Berstel, Aaron Lauve, Christophe Reutenauer, Franco Saliola, *Combinatorics on Words : Christoffel Words and Repetitions in Words*, 2008.

[1] http://denise.vella.chemla.free.fr/2017fev15-1.jpg
[2] http://denise.vella.chemla.free.fr/2017fev15-2.jpg

Annexe 1 : programme de calcul des mots

```
1
2  #include <iostream>
3  #include <stdio.h>
4
5  int prime(int atester) {
6    bool pastrouve = true;
7    unsigned long k = 2;
8
9    if (atester == 1) return 0;
10   if (atester == 2) return 1;
11   if (atester == 3) return 1;
12   if (atester == 5) return 1;
13   if (atester == 7) return 1;
14   while (pastrouve) {
15     if ((k * k) > atester) return 1;
16     else
17       if ((atester % k) == 0) {
18         return 0 ;
19       }
20       else k++;
21   }
22 }
23
24 int main(int argc, char* argv[]) {
25   int n, i, xcourant, ycourant, xa, xb ;
26   float res ;
27
28   for (n = 3 ; n <= 500 ; ++n) {
29       printf("%5d : ", n) ;
30       if (prime(n)) std::cout << "(p) " ; else std::cout << "(c) " ;
31       xcourant = 1 ; ycourant = n-1 ;
32       xa = 0 ; xb = 0 ;
33       for (i = 1 ; i <= n-1 ; ++i) {
34          res = (float) n-(((float) xcourant + 1.0) * (float) ycourant) ;
35          if (res > 0.0) {
36            std::cout << "b" ;
37            if (i > n/2+1) std::cout << xa << " " ;
38            xcourant = xcourant+1 ;
39            xa = 0 ; xb = xb+1 ;
40          }
41          else {
42            if (i > n/2) std::cout << "a" ;
43            ycourant = ycourant-1 ;
44            xb = 0 ; xa = xa+1 ;
45          }
46       }
47       std::cout << "\n" ;
48   }
49 }
```

Annexe 2 : résultat du programme de calcul des mots

			26	c	4 2 1	51	c	9 4 2 2 1	76	c	12 7 3 3 2 1 1
			27	c	5 2 1	52	c	8 5 2 2 1	77	c	13 6 4 3 2 1 1
3	p		28	c	4 3 1	53	p	9 4 3 2 1	78	c	13 6 4 3 1 2 1
4	c		29	p	5 2 2	54	c	9 4 3 2 1	79	p	13 7 4 2 2 2 1
5	p		30	c	5 2 2	55	c	9 5 3 1 2	80	c	13 7 4 2 2 2 1
6	c		31	p	5 3 1 1	56	c	9 5 2 2 2	81	c	14 6 4 3 2 1 2
7	p	1	32	c	5 3 1 1	57	c	10 4 3 2 1 1	82	c	13 7 4 3 2 1 1
8	c	1	33	c	6 2 2 1	58	c	9 5 3 2 1 1	83	p	14 7 4 3 2 1 1
9	c	2	34	c	5 3 2 1	59	p	10 5 3 2 1 1	84	c	14 7 4 3 2 1 1
10	c	1	35	c	6 3 2 1	60	c	10 5 3 2 1 1	85	c	14 7 5 2 2 2 1
11	p	2	36	c	6 3 1 2	61	p	10 5 3 2 2 1	86	c	14 7 4 3 2 2 1
12	c	2	37	p	6 3 2 1	62	c	10 5 3 2 2 1	87	c	15 7 4 3 2 2 1
13	p	2 1	38	c	6 3 2 1	63	c	11 5 3 2 2 1	88	c	14 8 4 3 2 2 1
14	c	2 1	39	c	7 3 2 1	64	c	10 6 3 2 1 2	89	p	15 7 5 3 2 1 2
15	c	3 1	40	c	6 4 2 1	65	c	11 5 4 2 1 1	90	c	15 7 5 3 2 1 2
16	c	2 2	41	p	7 3 2 2	66	c	11 5 3 3 1 1	91	c	15 8 4 3 3 1 1 1
17	p	3 1	42	c	7 3 2 2	67	p	11 6 3 2 2 1	92	c	15 8 4 3 2 2 1 1
18	c	3 1	43	p	7 4 2 1 1	68	c	11 6 3 2 2 1	93	c	16 7 5 3 2 2 1 1
19	p	3 2	44	c	7 4 2 1 1	69	c	12 5 4 2 2 1	94	c	15 8 5 3 2 2 1 1
20	c	3 2	45	c	8 3 3 1 1	70	c	11 6 4 2 2 1	95	c	16 8 5 3 2 2 1 1
21	c	4 1 1	46	c	7 4 2 2 1	71	p	12 6 3 3 1 2	96	c	16 8 4 4 2 2 1 1
22	c	3 2 1	47	p	8 4 2 2 1	72	c	12 6 3 3 1 2	97	p	16 8 5 3 3 1 2 1
23	p	4 2 1	48	c	8 4 2 2 1	73	p	12 6 4 2 2 1 1	98	c	16 8 5 3 3 1 2 1
24	c	4 2 1	49	c	8 4 3 1 2	74	c	12 6 4 2 2 1 1	99	c	17 8 5 3 2 2 2 1
25	c	4 2 2	50	c	8 4 3 1 1	75	c	13 6 4 2 2 1 1	100	c	16 9 5 3 2 2 1 2

Essai de formalisation de l'approche proposée pour représenter la primalité à l'aide de mots de Christoffel associés à des hyperboles (Denise Vella-Chemla, 17.2.17)

Pour la définition des mots de Christoffel et l'utilisation qui en est faite ici, se reporter à [1] et [2].

On définit une application, indexée par les entiers, et qui associe elle-même un booléen à chaque entier : $f_n : \mathbb{N} \rightarrow \mathbb{B}$. On garde à l'esprit que cette fonction est le reflet d'une fonction f'_n qui à chaque point du plan associe un booléen : $f'_n : \mathbb{N}^2 \rightarrow \mathbb{B}$ et qu'on dispose d'une fonction φ_n qui passe de $\mathbb{N}^2$ à $\mathbb{N}$ et qui est définie par $\varphi_n : (x, y) \longmapsto x-y+n-1$. La fonction booléenne f_n sur les entiers (i.e. les positions successives dans les mots) a comme ensemble de départ l'ensemble d'arrivée de la fonction auxiliaire $\varphi_n(x, y)$ (l'utilisation de la fonction φ est motivé par le fait que les lignes brisées de segments faisant des zig-zags, il faut ordonner totalement les points qu'elles contiennent par leur position).

$f'_n((x, y)) = f_n(\varphi_n(x, y))$ est un booléen qui vaut 0 si $(x + 1)y \leqslant n$ et qui vaut 1 sinon (on peut se représenter cela de deux manières différentes : soit par le fait d'accoler une bande $\mathcal{B}$ de largeur horizontale 1 sur la gauche d'une hyperbole, et d'avoir tous les points dans cette bande qui sont à une altitude de 0 quand tous les autres points du plan sont à altitude 1, une sorte de ravin hyperbolique ; la deuxième représentation imagée peut être de laisser tous les points dans le plan et d'utiliser 2 couleurs, l'une pour les points de la bande et l'autre pour les points hors de la bande).

On considère la moitié supérieure de l'hyperbole d'équation $xy = n$, de pente négative. On approche cette courbe par une suite de points dont les ordonnées sont les entiers décroissants successifs à partir de $n - 1$ et dont les abscisses sont les plus grandes possibles strictement à gauche de l'hyperbole (il n'y a pas de point de contact entre les segments de la ligne brisée reliant les points et l'hyperbole). Le mot de Christoffel de n (cf [1]) est un mot fini sur l'alphabet $\{0, 1\}$ constitué de la suite de lettres associées à des segments-unités reliant des points entiers contigus verticalement (de même abscisse), ces points ayant pour image 0, ou contigus horizontalement (de même ordonnée), ces points ayant pour image 1. Les segments horizontaux sont utilisés pour "ramener la ligne brisée des segments" dans la bande $\mathcal{B}$ à chaque fois qu'elle en est sortie.

Considérons maintenant les fonctions associées à deux nombres entiers successifs f_n et f_{n+1}.

On a vu que le nombre n est premier si son mot de Christoffel se transfère à l'identique dans le mot de Christoffel de $n + 1$, à un décalage d'abscisse près. Il est composé sinon.

Cela correspond à la condition :

$$n \textit{ premier } \iff \forall k \in \mathbb{N}, \left\lfloor \frac{n+1}{2} \right\rfloor \leqslant k < n, f_n(\varphi_n^{-1}(k)) = f_{n+1}(\varphi_{n+1}^{-1}(k+1)).$$

Le signe "=" entre les images par deux fonctions booléennes (f_n et f_{n+1}) de deux positions dans deux mots est une fonction de $\mathbb{B} \times \mathbb{B}$ dans $\mathbb{B}$.

On peut aussi choisir une représentation par des opérateurs : on peut associer à la lettre a, qu'on a choisi de représenter ci-dessus par le booléen 0, l'opérateur $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ qui transforme le point $\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$ en $\begin{pmatrix} x \\ y-1 \\ 1 \end{pmatrix}$ tandis qu'on associe à la lettre b (ou booléen 1) l'opérateur $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ qui transforme le point $\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$ en $\begin{pmatrix} x+1 \\ y \\ 1 \end{pmatrix}$.

Bibliographie :

[1] Jean Berstel, Aaron Lauve, Christophe Reutenauer, Franco Saliola, *Combinatorics on Words : Christoffel Words and Repetitions in Words*, 2008.

[2] Denise Vella-Chemla, *Hyperboles et mots*, février 2017.

Un programme si surprenant pour connaître la primalité des entiers

Denise Vella-Chemla

20.02.2017

On fournit simplement ici un programme si surprenant issu de notre travail récent au sujet de mots de Christoffel sous des hyperboles.

```
#include <iostream>

int main(int argc, char* argv[]) {
  int n, i, xn, yn, xnplusun, ynplusun ;
  bool sensok, res1, res2 ;

  for (n = 3 ; n <= 99 ; n=n+2) {
    i = 1 ; sensok = true ;
    xn = 1 ; yn = n-1 ;
    xnplusun = 1 ; ynplusun = n ;
    while ((i <= n-1) && sensok) {
      res1 = (n > (xn + 1) * yn) ;
      res2 = (n+1 > ((xnplusun + 1) * (ynplusun - 1))) ;
      sensok = sensok && ((res1 && res2) || (not res1 && not res2)) ;
      if (sensok) {
        if (res1) xn = xn+1 ;
        else yn = yn-1 ;
        if (res2) xnplusun = xnplusun+1 ;
        else ynplusun = ynplusun-1 ;
        i = i+1 ;
      }
    }
    if (sensok) std::cout << n << " est premier.\n\n" ;
    else std::cout << n << " est composé.\n\n" ;
  }
}
```

Ci-dessous, le même programme en Python.

```
for n in range (3,100,2):
    xn = 1
    yn = n-1
    i = 1
    sensok = True
    xnplusun = 1
    ynplusun = n
    while ((i <= n-1) and sensok):
        res1 = (n > (xn + 1) * yn)
        res2 = (n+1 > ((xnplusun + 1) * (ynplusun - 1)))
        sensok = sensok and ((res1 and res2) or ((not res1) and (not res2)))
        if sensok:
            if res1:
                xn = xn+1
            else:
                yn = yn-1
            if res2:
                xnplusun = xnplusun+1
            else:
                ynplusun = ynplusun-1
            i = i+1
    if sensok:
        print("%d est premier." % n)
    else:
        print("%d est composé." % n)
```

Un programme à mots plus courts pour connaître la primalité des entiers

Denise Vella-Chemla

1.3.2017

On fournit simplement ici une petite adaptation d'un programme fourni précédemment et tel qu'un nombre est premier si son mot de Christoffel sous une portion d'hyperbole est égal au mot de son successeur.

```
#include <iostream>
#include <stdio.h>

int main(int argc, char* argv[]) {
  int n, i, xcourant, ycourant, xa, xb ;
  float res ;

  for (n = 3 ; n <= 100 ; ++n) {
    printf("%5d == ", n) ;
    xcourant = 1 ; if (n%2 == 0) ycourant = n/2-1 ; else ycourant = n/2 ;
    xa = 0 ; xb = 0 ;
    for (i = n/2+1 ; i <= n-2 ; ++i) {
      res = n-((xcourant + 1) * ycourant) ;
      if (res > 0) {
        if (i > n/2+1) std::cout << "b" ;
          xcourant = xcourant+1 ;
          xa = 0 ; xb = xb+1 ;
      }
      else {
        if (i > n/2+1) std::cout << "a" ;
          ycourant = ycourant-1 ;
          xb = 0 ; xa = xa+1 ;
        }
      }
      std::cout << "\n" ;
    }
}
```

Ci-dessous, les mots calculés par ce programme :

```
 7 == a
 8 == a
 9 == aa
10 == ab
11 == aab
12 == aab
13 == aaba
14 == aaba
15 == aaaba
16 == aabaa
17 == aaabab
18 == aaabab
19 == aaabaab
20 == aaabaab
21 == aaaababa
22 == aaabaaba
23 == aaaabaaba
24 == aaaabaaba
25 == aaaabaabaa
26 == aaaabaabab
27 == aaaaabaabab
28 == aaaabaaabab
29 == aaaaabaabaab
30 == aaaaabaabaab
31 == aaaaabaaababa
32 == aaaaabaaababa
33 == aaaaaabaabaaba
34 == aaaaabaaabaaba
35 == aaaaaabaaabaaba
36 == aaaaaabaaababaa
37 == aaaaaabaaabaabab
38 == aaaaaabaaabaabab
39 == aaaaaaabaaabaabab
40 == aaaaaabaaaabaabab
41 == aaaaaaabaaabaabaab
42 == aaaaaaabaaabaabaab
43 == aaaaaaabaaaabaababa
44 == aaaaaaabaaaabaababa
45 == aaaaaaaabaaabaaababa
46 == aaaaaaabaaaabaabaaba
47 == aaaaaaaabaaaabaabaaba
48 == aaaaaaaabaaaabaabaaba
49 == aaaaaaaabaaaabaaababaa
50 == aaaaaaaabaaaabaaababab
51 == aaaaaaaaabaaaabaabaabab
52 == aaaaaaaabaaaaabaabaabab
53 == aaaaaaaaabaaaabaaabaabab
54 == aaaaaaaaabaaaabaaabaabab
55 == aaaaaaaaabaaaaabaaababaab
56 == aaaaaaaaabaaaaabaabaabaab
57 == aaaaaaaaaabaaaabaaabaababa
58 == aaaaaaaaabaaaaabaaabaababa
59 == aaaaaaaaaabaaaaabaaabaababa
60 == aaaaaaaaaabaaaaabaaabaababa
61 == aaaaaaaaaabaaaaabaaabaabaaba
62 == aaaaaaaaaabaaaaabaaabaabaaba
63 == aaaaaaaaaaabaaaaabaaabaabaaba
64 == aaaaaaaaaabaaaaaabaaabaababaa
65 == aaaaaaaaaaabaaaaabaaaabaababab
66 == aaaaaaaaaaabaaaaabaaabaaababab
67 == aaaaaaaaaaabaaaaaabaaabaabaabab
68 == aaaaaaaaaaabaaaaaabaaabaabaabab
69 == aaaaaaaaaaaabaaaaabaaaabaabaabab
70 == aaaaaaaaaaabaaaaaabaaaabaabaabab
```

```
 71 == aaaaaaaaaaaabaaaaaabaaabaaababaab
 72 == aaaaaaaaaaaabaaaaaabaaabaaababaab
 73 == aaaaaaaaaaaabaaaaaabaaaabaabaababa
 74 == aaaaaaaaaaaabaaaaaabaaaabaabaababa
 75 == aaaaaaaaaaaaabaaaaaabaaaabaabaababa
 76 == aaaaaaaaaaaabaaaaaaabaaabaaabaababa
 77 == aaaaaaaaaaaaabaaaaaabaaaabaaabaababa
 78 == aaaaaaaaaaaaabaaaaaabaaaabaaabababaa
 79 == aaaaaaaaaaaaabaaaaaaabaaaabaabaababa
 80 == aaaaaaaaaaaaabaaaaaaabaaaabaabaababa
 81 == aaaaaaaaaaaaaabaaaaaabaaaabaaabaababa
 82 == aaaaaaaaaaaaabaaaaaaabaaaabaaabababab
 83 == aaaaaaaaaaaaaabaaaaaabaaaabaaabaababab
 84 == aaaaaaaaaaaaaabaaaaaabaaaabaaabaababab
 85 == aaaaaaaaaaaaaabaaaaaabaaaaabaabaababab
 86 == aaaaaaaaaaaaaabaaaaaabaaaabaaabaababab
 87 == aaaaaaaaaaaaaaabaaaaaabaaaabaaabaababab
 88 == aaaaaaaaaaaaaabaaaaaaabaaaabaaabaababab
 89 == aaaaaaaaaaaaaaabaaaaaabaaaaabaaabababaab
 90 == aaaaaaaaaaaaaaabaaaaaabaaaaabaaabababaab
 91 == aaaaaaaaaaaaaaabaaaaaaabaaaabaaabaaababa
 92 == aaaaaaaaaaaaaaabaaaaaaabaaaabaaabaababa
 93 == aaaaaaaaaaaaaaaabaaaaaabaaaaabaaabaababa
 94 == aaaaaaaaaaaaaaabaaaaaaabaaaaabaaabaababa
 95 == aaaaaaaaaaaaaaaabaaaaaaabaaaaabaaabaababa
 96 == aaaaaaaaaaaaaaaabaaaaaaabaaaabaaaabaababa
 97 == aaaaaaaaaaaaaaaabaaaaaaabaaaaabaaabaaababaa
 98 == aaaaaaaaaaaaaaaabaaaaaaabaaaaabaaabaaababaa
 99 == aaaaaaaaaaaaaaaaabaaaaaaabaaaaabaaabaababaa
100 == aaaaaaaaaaaaaaaabaaaaaaabaaaaabaaabaababaa
```

Mots de nombres premiers

Denise Vella-Chemla

4.3.17

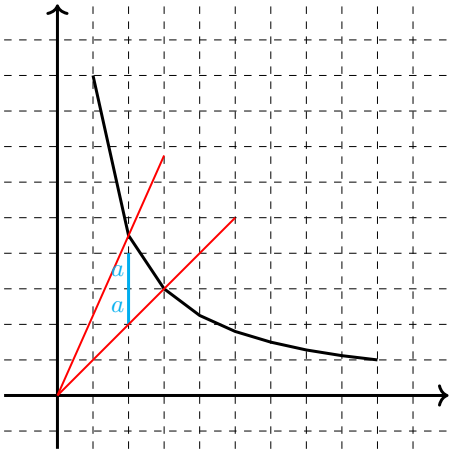
On voudrait ici présenter lentement une découverte qu'on a faite récemment qui permet de caractériser les nombres premiers en étudiant des mots sur un alphabet à 2 lettres a et b.

Cette découverte une fois effectuée est simple, elle utilise des opérations élémentaires : ajouter 1 à un nombre, multiplier deux nombres, comparer deux nombres, coder le sens d'inégalités par des lettres a ou b et comparer des mots.

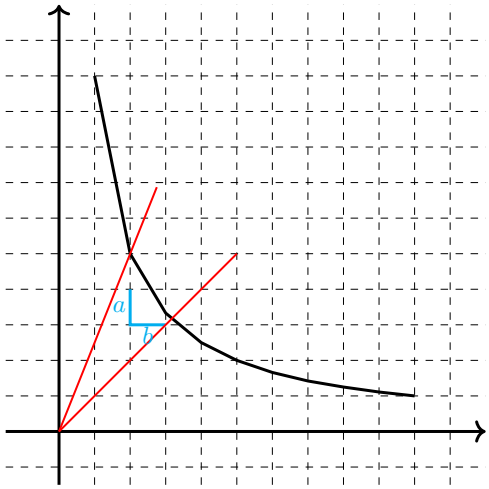
On est parti du fait que l'hyperbole d'équation $xy = n$ avec n un nombre premier ne passe que par des points à coordonnées non-entières du plan, hormis les points $(1, n)$ et $(n, 1)$. Par contre, si n est composé, l'hyperbole passe par autant de points à coordonnées entières du plan que n a de diviseurs. Par exemple, l'hyperbole d'équation $xy = 12$ passe par les points à coordonnées entières $(1, 12), (2, 6), (3, 4), (4, 3), (6, 2), (12, 1)$. Ces considérations (sur les points, dont les 2 coordonnées dans le plan peuvent être entières ou non) sont des considérations géométriques.

On a souhaité comprendre ce qui se passait lors du passage d'une hyperbole à la suivante (i.e. de l'hyperbole d'équation $xy = n$ à l'hyperbole d'équation $xy = n + 1$). Dans ce but, on a choisi d'associer à chaque hyperbole son mot de Christoffel.

Un mot de Christoffel [1] est un mot sur un alphabet de deux lettres qui "colle au plus près" à une courbe par segments liant des points discrets (par le dessus ou par le dessous). Voyons un exemple. Pour que la caractérisation des nombres premiers soit la plus simple possible, on ne conserve qu'une portion de chaque mot de Christoffel appartenant à une zone délimitée par deux droites, dans le quadrant $x > 0, y > 0$ (les droites d'équation $y = 2x$ et $y = x$).



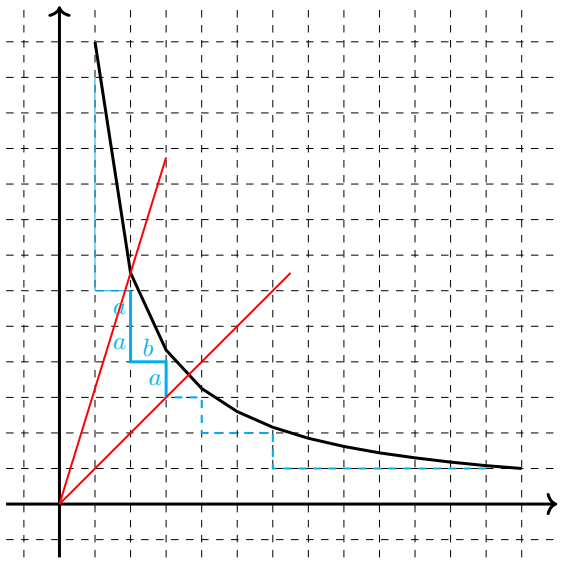
$n = 9$



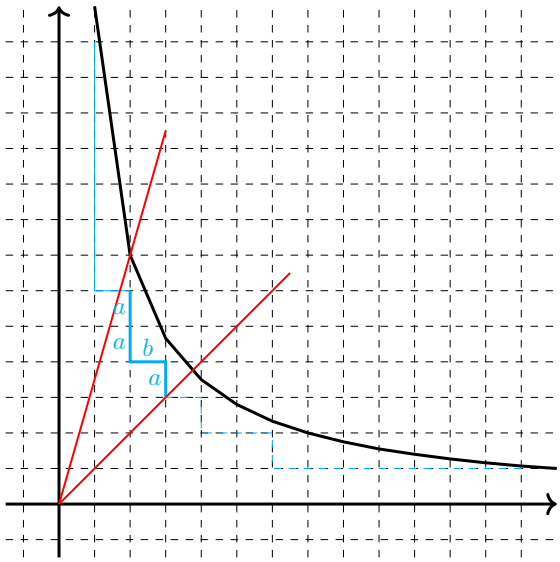
$n = 10$

On constate et c'est simple à comprendre qu'un nombre premier n a le même mot de Christoffel qu'$n + 1$ tandis qu'un nombre composé n a un mot de Christoffel différent de celui d'$n + 1$.

En choisissant la modélisation ci-dessus, on relie trois théories : la théorie des langages (qui contient les concepts d'alphabet, lettre, mot, concaténation, égalité et différence), l'arithmétique (là, les concepts sont ceux de nombre, diviseur, premier, composé) et la géométrie (et ses concepts de points, réseau de points entiers, hyperbole et équation).



$n = 13$



$n = 14$

Qu'est-ce qui se cache derrière cette modélisation informatique ?

Chaque lettre a ou b code une assertion logique, qui correspond ici à une inégalité entre deux nombres. On a un segment de longueur 1, étiqueté b, d'origine le point de coordonnées (x, y) partant horizontalement dans la direction de l'hyperbole[1] associée à n si $(x+1)y \leqslant n$. Dans le cas contraire, descend verticalement de ce point un segment étiqueté a de longueur 1.

Quand on dit qu'*un mot est égal à un autre mot*, une phrase si élémentaire que sa véracité peut être appréhendée par un élève de maternelle, on lie entre elles toute une série d'assertions logiques, les unes associées à l'hyperbole d'équation $xy = n$, les autres associées à l'hyperbole d'équation $xy = n + 1$, et on étudie si toutes les assertions sont deux à deux simultanément vérifiées ou simultanément invérifiées, ce qui est assez complexe à exprimer algébriquement.

Considérons un exemple simple, celui du passage du mot *aaaba* du nombre composé 15 au mot *aabaa* de son successeur.

Les lettres *aaaba* "de" 15 codent les inégalités :

$$\begin{cases} a : (2+1) * 7 \geqslant 15 \\ a : (2+1) * 6 \geqslant 15 \\ a : (2+1) * 5 \geqslant 15 \\ b : (2+1) * 4 < 15 \\ a : (3+1) * 4 \geqslant 15 \end{cases}$$

tandis que les lettres *aabaa* "de" 16 codent les inégalités :

$$\begin{cases} a : (2+1) * 7 \geqslant 16 \\ a : (2+1) * 6 \geqslant 16 \\ b : (2+1) * 5 < 16 \\ a : (3+1) * 5 \geqslant 16 \\ a : (3+1) * 4 \geqslant 16 \end{cases}$$

Lorsqu'on dit que ces mots sont différents, on regarde chaque doublon de lettres et on étudie si le sens des inégalités pour l'un et l'autre nombre sont égaux. En l'occurrence, on trouve une différence entre les troisièmes lettres des mots $a : (2+1) * 5 \geqslant 15$ et $b : (2+1) * 5 < 16$. A la première différence de sens entre les inégalités associées à n et celles associées à $n+1$, il y a bifurcation des chemins au niveau des mots de Christoffel.

L'interprétation qui vient d'être donnée est une interprétation algébrique. On peut se placer sur une algèbre de Boole au lieu de se placer dans la théorie des langages : la lettre a correspond à 0, la lettre b à

[1] i.e. on a "la place" pour mettre un b sans toucher à l'hyperbole.

1. Regarder si deux lettres sont identiques consiste à étudier le résultat d'une fonction qui à deux booléens en associe un troisième (une fonction de $\mathbb{B} \times \mathbb{B}$ dans $\mathbb{B}$) qui code le fait que les deux booléens sont égaux ou pas (tester l'égalité de deux booléens $b_1 = b_2$ consiste à calculer $((1 - b_1) + b_2).((1 - b_2) + b_1)$). En annexe, on rappelle les valeurs des connecteurs logiques.

D'un point de vue géométrique, à quoi cela correspond-il ?

Il faut imaginer les hyperboles d'un nombre et de son successeur ainsi que leur mot de Christoffel respectifs comme se situant dans des plans différents. Il faut aussi imaginer qu'à chaque hyperbole est associée sur la gauche une bande de largeur horizontale 1 dans laquelle se développe le mot de Christoffel. Tant que celui-ci peut se voir concaténer un a sans sortir de la bande, c'est ce qui se passe. Dès que le mot "sort de la bande hyperbolique", il faut lui concaténer une lettre b pour le ramener dans la bande (i.e. pour qu'il reste toujours à distance la plus faible possible de l'hyperbole tout en ne s'y collant pas et il s'agit d'une distance de Manhattan horizontale, je crois, ou distance de norme 1). Dès qu'on a ramené le mot dans la bande, on peut se remettre à concaténer des a, c'est pour cette raison que les lettres b n'apparaissent qu'une par une dans les mots, et jouent le rôle de séparateurs (ou ponctuations).

On peut noter qu'une fois établie la modélisation, on peut oublier son interprétation géométrique et n'en conserver que le versant algébrique (les mots de lettres codant des inégalités) en se rappelant toutefois que ce sont les images géométriques (la perception visuelle des objets géométriques) qui ont permis d'aboutir à la modélisation.

Bibliographie :

[1] Jean Berstel, Aaron Lauve, Christophe Reutenauer, Franco Saliola, *Combinatorics on Words : Christoffel Words and Repetitions in Words*, 2008.

[2] B.A. Trahtenbrot, *Algorithmes et machines à calculer*

[3] Alain Connes, *Un extrait d'un cours donné en 1998 à l'Ohio State University, à Colombus aux Etats-Unis, et dans lequel il est question d'hyperboles et points discrets ; il n'y a pas de lien avec ce qui est présenté dans cette note, on ne retiendra que l'expression utilisée à la fin de la présentation de cet exemple "c'est marrant !", qui exprime toute la jubilation que provoque l'étude et la découverte :*
http://denise.vella.chemla.free.fr/ac-hr-osu-1998-8-hyperb-9mn30.mp4

[4] Alain Connes, *Un extrait d'un Colloquium à l'ICTP de Trieste en Italie en mars 2017, dans lequel sont présentées des anagrammes exprimant la non-commutativité du langage :*
http://denise.vella.chemla.free.fr/ac-ictp-mars2017-anagrammes.mp4

Annexe : rappel des valeurs des connecteurs logiques

La notation P de la dernière colonne correspond au calcul de $(b_1 = b_2)$ aussi égal à $((1 - b_1) + b_2).((1 - b_2) + b_1)$ (en logique, on se situe dans un domaine complètement abélien ; c'est uniquement l'importance de l'ordre des lettres dans les mots (i.e. la non-commutativité de la concaténation en théorie des langages) qui rend notre modélisation non-commutative).

b_1	b_2	$1 - b_1$	$1 - b_2$	$(1 - b_1) + b_2$	$(1 - b_2) + b_1$	P
0	0	1	1	1	1	1
0	1	1	0	1	0	0
1	0	0	1	0	1	0
1	1	0	0	1	1	1

Il faut avoir à l'esprit que la formule fournie pour exprimer l'égalité entre 2 booléens fait intervenir l'addition, la soustraction et la multiplication parce que c'est pratique. En fait, on peut générer les connecteurs $\vee$ (ou $+$), $\wedge$ (ou $.$), $\neg b$ (ou $1 - b$) et $=$ (parfois noté $\odot$) à l'aide de la seule implication $\rightarrow$ comme montré dans les tables de vérité ci-dessous (pour le $=$, on extrapolera une fois l'idée comprise à cause de la lourdeur des formules à écrire).

b	$\neg b$	$b \to 0$
0	1	1
1	0	0

b_1	b_2	$b_1 \vee b_2$	$b_1 \to 0$	$(b_1 \to 0) \to b_2$
0	0	0	1	0
0	1	1	1	1
1	0	1	0	1
1	1	1	0	1

b_1	b_2	$b_1 \wedge b_2$	$b_1 \to 0$	$(b_1 \to 0) \to 0$	$b_2 \to 0$	$((b_1 \to 0) \to 0) \to (b_2 \to 0)$	$(((b_1 \to 0) \to 0) \to (b_2 \to 0)) \to 0$
0	0	0	1	0	1	1	0
0	1	0	1	0	0	1	0
1	0	0	0	1	1	1	0
1	1	1	0	1	0	0	1

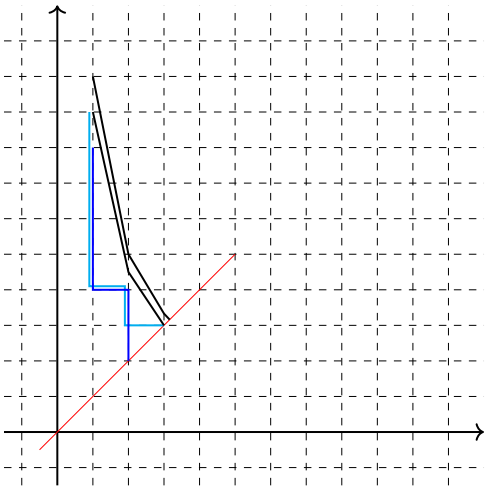
On a : $\neg b = (b \to 0)$, $b_1 \vee b_2 = (b_1 \to 0) \to b_2$ et $b_1 \wedge b_2 = (((b_1 \to 0) \to 0) \to (b_2 \to 0)) \to 0$.

Mots de Christoffel d'hyperboles et primalité

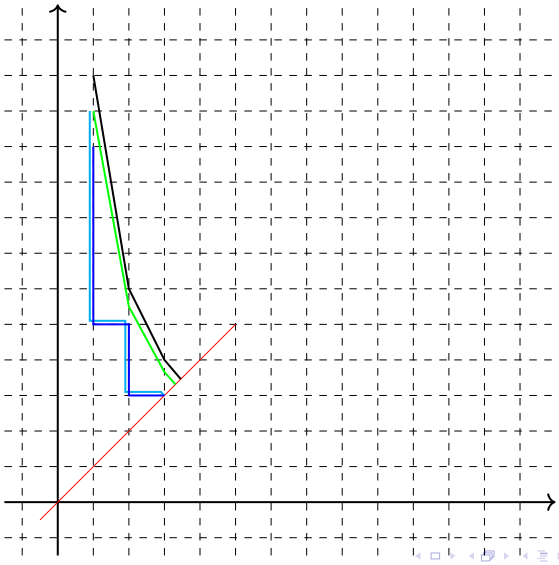
D. Vella-Chemla

17.02.2017

Mots de Christoffel des hyperboles de 9 et 10



Mots de Christoffel des hyperboles de 11 et 12



n premier $\iff$ $m_{n+1} = am_n$

3	*a*
4	*aa*
5	*aab*
6	*aaab*
7	*aaaba*
8	*aaaaba*
9	*aaaabaa*
10	*aaaaabab*
11	*aaaaabaab*
12	*aaaaaabaab*
13	*aaaaaabaaba*
14	*aaaaaaabaaba*
15	*aaaaaaabaaaba*
16	*aaaaaaaabaabaa*
17	*aaaaaaaabaaabab*
18	*aaaaaaaaabaaabab*
19	*aaaaaaaaabaaabaab*
20	*aaaaaaaaaabaaabaab*
21	*aaaaaaaaaabaaaababa*
22	*aaaaaaaaaaabaaabaaba*
23	*aaaaaaaaaaabaaaabaaba*

Changement de sens des inégalités, bifurcation des chemins

Passage du mot de 15 au mot de 16

	$a : (1+1) * 15 \geqslant 16$
$a : (1+1) * 14 \geqslant 15$	$a : (1+1) * 14 \geqslant 16$
$a : (1+1) * 13 \geqslant 15$	$a : (1+1) * 13 \geqslant 16$
$a : (1+1) * 12 \geqslant 15$	$a : (1+1) * 12 \geqslant 16$
$a : (1+1) * 11 \geqslant 15$	$a : (1+1) * 11 \geqslant 16$
$a : (1+1) * 10 \geqslant 15$	$a : (1+1) * 10 \geqslant 16$
$a : (1+1) * 9 \geqslant 15$	$a : (1+1) * 9 \geqslant 16$
$a : (1+1) * 8 \geqslant 15$	$a : (1+1) * 8 \geqslant 16$
$b : (2+1) * 8 < 15$	$b : (1+1) * 7 < 16$
$a : (2+1) * 7 \geqslant 15$	$a : (2+1) * 7 \geqslant 16$
$a : (2+1) * 6 \geqslant 15$	$a : (2+1) * 6 \geqslant 16$
$a : (2+1) * 5 \geqslant 15$ $\star$	$b : (2+1) * 5 < 16$
$b : (3+1) * 5 < 15$	$a : (3+1) * 5 \geqslant 16$
$a : (3+1) * 4 \geqslant 15$	$a : (3+1) * 4 \geqslant 16$

Essai de formalisation

- $f'_n : \mathbb{N}^2 \to \mathbb{B}$
- $f_n : \mathbb{N} \to \mathbb{B}$
- $f'_n((x, y)) = f_n(\varphi_n(x, y))$
- $\varphi_n : (x, y) \longmapsto x - y + n - 1$
- $f_n(\varphi_n(x, y)) \ = \ ((x + 1)y \leqslant n)$
- n premier
  $\iff \forall k \in \mathbb{N}, \left\lfloor \frac{n+1}{2} \right\rfloor \leqslant k < n, f_n(\varphi_n^{-1}(k)) = f_{n+1}(\varphi_{n+1}^{-1}(k+1)).$

Opérateurs associés aux deux lettres

- $a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$. a transforme $\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$ en $\begin{pmatrix} x \\ y-1 \\ 1 \end{pmatrix}$

- $b = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. b transforme $\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$ en $\begin{pmatrix} x+1 \\ y \\ 1 \end{pmatrix}$

- En partant des points de départ $(1, p-1)$ et $(1, p)$ et en appliquant les opérateurs associés aux lettres des mots de p et $p+1$, il y a identité entre les points d'arrivée (point du plan au bout du chemin de Christoffel) lorsque p est premier.

Bibliographie

- [1] B.A. Trahtenbrot, *Algorithmes et machines à calculer*
- [2] J. Berstel, A. Lauve, C. Reutenauer, F. Saliola, *Combinatorics on Words : Christoffel Words and Repetitions in Words*, 2008.

- *"On est extrêmement familiers avec la non-commutativité parce que lorsqu'on écrit, avec des lettres, lorsqu'on écrit des mots, des phrases, etc., on doit bien sûr faire attention à l'ordre des lettres."*

  (Alain Connes dans une courte interview au Collège de France, 24.04.2014)

Géométrie non-commutative 

Codage de mots booléens (Denise Vella-Chemla, 19.3.2017)

Dans une note précédente, on a vu comment associer des mots booléens aux entiers successifs (en utilisant la notion de mot de Christoffel sous une hyperbole). On a constaté également qu'un nombre n est premier si son mot booléen est identique à celui de $n+1$, et qu'il est composé sinon.

On fournit ici une première idée de fonction $f : \{a,b\}^* \rightarrow \mathbb{N}$ qui associe à un mot booléen un nombre entier. Cela permet de remplacer la condition d'égalité des mots par le fait que le rapport de 2 entiers vaille 1. Fournissons deux exemples illustrant rapidement le codage qu'on a en tête et la définition de f :

$$f(aaaababaaa) = 2^4.3.5^3$$
$$f(aaabaaaaabaa) = 2^3.3^5.5^2$$
$$f(a^{\alpha_1}ba^{\alpha_2}ba^{\alpha_3}\ldots a^{\alpha_i}) = 2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}.\ldots.p_i^{\alpha_i}$$

On fournit ici une seconde idée de fonction $g : \{a,b\}^* \rightarrow \mathbb{N}$ qui associe à un mot booléen un nombre entier. Cela permet de remplacer la condition d'égalité des mots par le fait que le rapport de 2 entiers vaille 1. Fournissons deux exemples illustrant rapidement le codage qu'on a en tête et la définition de f :

$$f(aaaababaaa) = 1111010111$$
$$f(aaabaaaaabaa) = 111011111011$$
$$f(s) = \sum_{i=1}^{i=longueur(s)} 10^i \times s_i$$

Etude d'une fonction particulière (Denise Vella-Chemla, 30.3.2017)

On va s'intéresser ici à une fonction particulière, qui opère sur des inégalités selon leur valeur de vérité et qui sera utile dans l'étude des nombres premiers.

On définit une transformation T qui opère sur une inégalité de la forme $Ineg : xy \geqslant n$.

T transforme l'inégalité $Ineg$ en l'inégalité $Ineg_a : x(y-1) \geqslant n$ si elle ($Ineg$) est vraie ou bien la transforme en $Ineg_b : (x+1)y \geqslant n$ dans le cas contraire.

A chacune des inégalités obtenues lors des applications successives de la transformation T est associée une valeur booléenne de vérité. On note entre parenthèses cette valeur de vérité par un V pour vrai et un F pour faux.

On définit une fonction *Inégalité_de_départ* par :

$$\begin{aligned} \textit{Inégalité\_de\_départ} : \quad & \mathbb{N} \to \mathbb{N} \\ & n \mapsto 3.\left\lfloor \frac{2n-1}{4} \right\rfloor \geqslant n \end{aligned}$$

On applique $\frac{n-k}{2} - 1$ (avec $k = 5$ si n est impair et $k = 6$ sinon) transformations, la première transformation étant appliquée à $\textit{Inégalité\_de\_départ}(n)$ et les transformations ultérieures étant appliquées aux résultats obtenus par les transformations successives (qui sont autant d'inégalités).

Par exemple, $\textit{Inégalité\_de\_départ}(9) : 3.4 \geqslant 9$ (V). La seule transformation appliquée à cette inégalité va la transformer en l'inégalité $3.3 \geqslant 9$ (V).

Pour $n = 10$, $\textit{Inégalité\_de\_départ}(10) : 3.4 \geqslant 10$ (V). La seule transformation appliquée à cette inégalité va la transformer en l'inégalité $3.3 \geqslant 10$ (F).

Pour $n = 13$, $\textit{Inégalité\_de\_départ}(13) : 3.6 \geqslant 13$ (V). La première transformation appliquée à cette inégalité va la transformer en l'inégalité $3.5 \geqslant 13$ (V). Une nouvelle transformation appliquée à l'inégalité obtenue permet d'obtenir l'inégalité $3.4 \geqslant 13$ (F) et une ultime transformation aboutit à $4.4 \geqslant 13$ (V).

Pour $n = 14$, $\textit{Inégalité\_de\_départ}(14) : 3.6 \geqslant 14$ (V). La première transformation appliquée à cette inégalité va la transformer en l'inégalité $3.5 \geqslant 14$ (V). Une nouvelle transformation appliquée à l'inégalité obtenue permet d'obtenir l'inégalité $3.4 \geqslant 14$ (F) et une ultime transformation aboutit à $4.4 \geqslant 14$ (V).

Pour $n = 15$, $\textit{Inégalité\_de\_départ}(15) : 3.7 \geqslant 15$ (V). La première transformation appliquée à cette inégalité va la transformer en l'inégalité $3.6 \geqslant 15$ (V). Une nouvelle transformation appliquée à l'inégalité obtenue permet d'obtenir l'inégalité $3.5 \geqslant 15$ (V), une autre transformation aboutit à $3.4 \geqslant 15$ (F) et une ultime transformation aboutit à $4.4 \geqslant 15$ (V).

Pour $n = 16$, $\textit{Inégalité\_de\_départ}(16) : 3.7 \geqslant 16$ (V). La première transformation appliquée à cette inégalité va la transformer en l'inégalité $3.6 \geqslant 16$ (V). Une nouvelle transformation appliquée à l'inégalité obtenue permet d'obtenir l'inégalité $3.5 \geqslant 16$ (F), une autre transformation aboutit à $4.5 \geqslant 16$ (V) et une ultime transformation aboutit à $4.4 \geqslant 16$ (V).

On postule qu'un nombre n est premier si et seulement si les valeurs de vérité associées aux inégalités obtenues par la chaîne de $\frac{n-5}{2} - 1$ transformations depuis son inégalité de départ sont identiques à celles associées aux inégalités obtenues par la chaîne de $\frac{n-6}{2} - 1$ transformations depuis l'inégalité de départ associée à son successeur $n+1$. Si la valeur de vérité associée à la i-ème transformation pour n diffère de celle associée à la i-ème transformation pour $n+1$ alors n est composé.

Ceci découle d'une découverte présentée dans une étude récente des mots de Christoffel associés à des hyperboles.

Sens des inégalités (Denise Vella-Chemla, 31.3.2017)

Toutes les inégalités sont deux à deux dans le même sens pour les nombres 97 et 98, 97 est premier (les inégalités fausses sont barrées).

$3.48 \geqslant 97$	$3.47 \geqslant 97$	$3.46 \geqslant 97$	$3.45 \geqslant 97$	$3.44 \geqslant 97$	$3.43 \geqslant 97$	$3.42 \geqslant 97$	$3.41 \geqslant 97$	$3.40 \geqslant 97$	$3.39 \geqslant 97$
$3.48 \geqslant 98$	$3.47 \geqslant 98$	$3.46 \geqslant 98$	$3.45 \geqslant 98$	$3.44 \geqslant 98$	$3.43 \geqslant 98$	$3.42 \geqslant 98$	$3.41 \geqslant 98$	$3.40 \geqslant 98$	$3.39 \geqslant 98$

$3.38 \geqslant 97$	$3.37 \geqslant 97$	$3.36 \geqslant 97$	$3.35 \geqslant 97$	$3.34 \geqslant 97$	$3.33 \geqslant 97$	~~$3.32 \geqslant 97$~~	$4.32 \geqslant 97$	$4.31 \geqslant 97$	$4.30 \geqslant 97$
$3.38 \geqslant 98$	$3.37 \geqslant 98$	$3.36 \geqslant 98$	$3.35 \geqslant 98$	$3.34 \geqslant 98$	$3.33 \geqslant 98$	~~$3.32 \geqslant 98$~~	$4.32 \geqslant 98$	$4.31 \geqslant 98$	$4.30 \geqslant 98$

$4.29 \geqslant 97$	$4.28 \geqslant 97$	$4.27 \geqslant 97$	$4.26 \geqslant 97$	$4.25 \geqslant 97$	~~$4.24 \geqslant 97$~~	$5.24 \geqslant 97$	$5.23 \geqslant 97$	$5.22 \geqslant 97$	$5.21 \geqslant 97$
$4.29 \geqslant 98$	$4.28 \geqslant 98$	$4.27 \geqslant 98$	$4.26 \geqslant 98$	$4.25 \geqslant 98$	~~$4.24 \geqslant 98$~~	$5.24 \geqslant 98$	$5.23 \geqslant 98$	$5.22 \geqslant 98$	$5.21 \geqslant 98$

$5.20 \geqslant 97$	~~$5.19 \geqslant 97$~~	$6.19 \geqslant 97$	$6.18 \geqslant 97$	$6.17 \geqslant 97$	~~$6.16 \geqslant 97$~~	$7.16 \geqslant 97$	$7.15 \geqslant 97$	$7.14 \geqslant 97$	~~$7.13 \geqslant 97$~~
$5.20 \geqslant 98$	~~$5.19 \geqslant 98$~~	$6.19 \geqslant 98$	$6.18 \geqslant 98$	$6.17 \geqslant 98$	~~$6.16 \geqslant 98$~~	$7.16 \geqslant 98$	$7.15 \geqslant 98$	$7.14 \geqslant 98$	~~$7.13 \geqslant 98$~~

$8.13 \geqslant 97$	~~$8.12 \geqslant 97$~~	$9.12 \geqslant 97$	$9.11 \geqslant 97$	~~$9.10 \geqslant 97$~~	$10.10 \geqslant 97$
$8.13 \geqslant 98$	~~$8.12 \geqslant 98$~~	$9.12 \geqslant 98$	$9.11 \geqslant 98$	~~$9.10 \geqslant 98$~~	$10.10 \geqslant 98$

Certaines inégalités ne sont pas deux à deux dans le même sens pour les nombres 99 et 100, 99 est composé.

$3.49 \geqslant 99$	$3.48 \geqslant 99$	$3.47 \geqslant 99$	$3.46 \geqslant 99$	$3.45 \geqslant 99$	$3.44 \geqslant 99$	$3.43 \geqslant 99$	$3.42 \geqslant 99$
$3.49 \geqslant 100$	$3.48 \geqslant 100$	$3.47 \geqslant 100$	$3.46 \geqslant 100$	$3.45 \geqslant 100$	$3.44 \geqslant 100$	$3.43 \geqslant 100$	$3.42 \geqslant 100$

$3.41 \geqslant 99$	$3.40 \geqslant 99$	$3.39 \geqslant 99$	$3.38 \geqslant 99$	$3.37 \geqslant 99$	$3.36 \geqslant 99$	$3.35 \geqslant 99$	$3.34 \geqslant 99$
$3.41 \geqslant 100$	$3.40 \geqslant 100$	$3.39 \geqslant 100$	$3.38 \geqslant 100$	$3.37 \geqslant 100$	$3.36 \geqslant 100$	$3.35 \geqslant 100$	$3.34 \geqslant 100$

$3.33 \geqslant 99$	~~$3.32 \geqslant 99$~~	$4.32 \geqslant 99$	$4.31 \geqslant 99$	$4.30 \geqslant 99$	$4.29 \geqslant 99$	$4.28 \geqslant 99$	$4.27 \geqslant 99$
~~$3.33 \geqslant 100$~~	$4.33 \geqslant 100$	$4.32 \geqslant 100$	$4.31 \geqslant 100$	$4.30 \geqslant 100$	$4.29 \geqslant 100$	$4.28 \geqslant 100$	$4.27 \geqslant 100$

$4.26 \geqslant 99$	$4.25 \geqslant 99$	~~$4.24 \geqslant 99$~~	$5.24 \geqslant 99$	$5.23 \geqslant 99$	$5.22 \geqslant 99$	$5.21 \geqslant 99$	$5.20 \geqslant 99$
$4.26 \geqslant 100$	$4.25 \geqslant 100$	~~$4.24 \geqslant 100$~~	$5.24 \geqslant 100$	$5.23 \geqslant 100$	$5.22 \geqslant 100$	$5.21 \geqslant 100$	$5.20 \geqslant 100$

~~$5.19 \geqslant 99$~~	$6.19 \geqslant 99$	$6.18 \geqslant 99$	$6.17 \geqslant 99$	~~$6.16 \geqslant 99$~~	$7.16 \geqslant 99$	$7.15 \geqslant 99$	~~$7.14 \geqslant 99$~~
~~$5.19 \geqslant 100$~~	$6.19 \geqslant 100$	$6.18 \geqslant 100$	$6.17 \geqslant 100$	~~$6.16 \geqslant 100$~~	$7.16 \geqslant 100$	$7.15 \geqslant 100$	~~$7.14 \geqslant 100$~~

$8.14 \geqslant 99$	$8.13 \geqslant 99$	~~$8.12 \geqslant 99$~~	$9.12 \geqslant 99$	$9.11 \geqslant 99$	~~$9.10 \geqslant 99$~~	$10.10 \geqslant 99$
$8.14 \geqslant 100$	$8.13 \geqslant 100$	~~$8.12 \geqslant 100$~~	$9.12 \geqslant 100$	~~$9.11 \geqslant 100$~~	$10.11 \geqslant 100$	$10.10 \geqslant 100$

Sens des inégalités (Denise Vella-Chemla, 31.3.2017)

Toutes les inégalités sont deux à deux dans le même sens pour les nombres 97 et 98, 97 est premier (les inégalités fausses sont barrées).

$3.48 \geqslant 97$	$3.47 \geqslant 97$	$3.46 \geqslant 97$	$3.45 \geqslant 97$	$3.44 \geqslant 97$	$3.43 \geqslant 97$	$3.42 \geqslant 97$	$3.41 \geqslant 97$	$3.40 \geqslant 97$	$3.39 \geqslant 97$
$3.48 \geqslant 98$	$3.47 \geqslant 98$	$3.46 \geqslant 98$	$3.45 \geqslant 98$	$3.44 \geqslant 98$	$3.43 \geqslant 98$	$3.42 \geqslant 98$	$3.41 \geqslant 98$	$3.40 \geqslant 98$	$3.39 \geqslant 98$

$3.38 \geqslant 97$	$3.37 \geqslant 97$	$3.36 \geqslant 97$	$3.35 \geqslant 97$	$3.34 \geqslant 97$	$3.33 \geqslant 97$	~~$3.32 \geqslant 97$~~	$4.32 \geqslant 97$	$4.31 \geqslant 97$	$4.30 \geqslant 97$
$3.38 \geqslant 98$	$3.37 \geqslant 98$	$3.36 \geqslant 98$	$3.35 \geqslant 98$	$3.34 \geqslant 98$	$3.33 \geqslant 98$	~~$3.32 \geqslant 98$~~	$4.32 \geqslant 98$	$4.31 \geqslant 98$	$4.30 \geqslant 98$

$4.29 \geqslant 97$	$4.28 \geqslant 97$	$4.27 \geqslant 97$	$4.26 \geqslant 97$	$4.25 \geqslant 97$	~~$4.24 \geqslant 97$~~	$5.24 \geqslant 97$	$5.23 \geqslant 97$	$5.22 \geqslant 97$	$5.21 \geqslant 97$
$4.29 \geqslant 98$	$4.28 \geqslant 98$	$4.27 \geqslant 98$	$4.26 \geqslant 98$	$4.25 \geqslant 98$	~~$4.24 \geqslant 98$~~	$5.24 \geqslant 98$	$5.23 \geqslant 98$	$5.22 \geqslant 98$	$5.21 \geqslant 98$

$5.20 \geqslant 97$	~~$5.19 \geqslant 97$~~	$6.19 \geqslant 97$	$6.18 \geqslant 97$	$6.17 \geqslant 97$	~~$6.16 \geqslant 97$~~	$7.16 \geqslant 97$	$7.15 \geqslant 97$	$7.14 \geqslant 97$	~~$7.13 \geqslant 97$~~
$5.20 \geqslant 98$	~~$5.19 \geqslant 98$~~	$6.19 \geqslant 98$	$6.18 \geqslant 98$	$6.17 \geqslant 98$	~~$6.16 \geqslant 98$~~	$7.16 \geqslant 98$	$7.15 \geqslant 98$	$7.14 \geqslant 98$	~~$7.13 \geqslant 98$~~

$8.13 \geqslant 97$	~~$8.12 \geqslant 97$~~	$9.12 \geqslant 97$	$9.11 \geqslant 97$	~~$9.10 \geqslant 97$~~	$10.10 \geqslant 97$
$8.13 \geqslant 98$	~~$8.12 \geqslant 98$~~	$9.12 \geqslant 98$	$9.11 \geqslant 98$	~~$9.10 \geqslant 98$~~	$10.10 \geqslant 98$

Certaines inégalités ne sont pas deux à deux dans le même sens pour les nombres 99 et 100, 99 est composé.

$3.49 \geqslant 99$	$3.48 \geqslant 99$	$3.47 \geqslant 99$	$3.46 \geqslant 99$	$3.45 \geqslant 99$	$3.44 \geqslant 99$	$3.43 \geqslant 99$	$3.42 \geqslant 99$
$3.49 \geqslant 100$	$3.48 \geqslant 100$	$3.47 \geqslant 100$	$3.46 \geqslant 100$	$3.45 \geqslant 100$	$3.44 \geqslant 100$	$3.43 \geqslant 100$	$3.42 \geqslant 100$

$3.41 \geqslant 99$	$3.40 \geqslant 99$	$3.39 \geqslant 99$	$3.38 \geqslant 99$	$3.37 \geqslant 99$	$3.36 \geqslant 99$	$3.35 \geqslant 99$	$3.34 \geqslant 99$
$3.41 \geqslant 100$	$3.40 \geqslant 100$	$3.39 \geqslant 100$	$3.38 \geqslant 100$	$3.37 \geqslant 100$	$3.36 \geqslant 100$	$3.35 \geqslant 100$	$3.34 \geqslant 100$

$3.33 \geqslant 99$	~~$3.32 \geqslant 99$~~	$4.32 \geqslant 99$	$4.31 \geqslant 99$	$4.30 \geqslant 99$	$4.29 \geqslant 99$	$4.28 \geqslant 99$	$4.27 \geqslant 99$
~~$3.33 \geqslant 100$~~	$4.33 \geqslant 100$	$4.32 \geqslant 100$	$4.31 \geqslant 100$	$4.30 \geqslant 100$	$4.29 \geqslant 100$	$4.28 \geqslant 100$	$4.27 \geqslant 100$

$4.26 \geqslant 99$	$4.25 \geqslant 99$	~~$4.24 \geqslant 99$~~	$5.24 \geqslant 99$	$5.23 \geqslant 99$	$5.22 \geqslant 99$	$5.21 \geqslant 99$	$5.20 \geqslant 99$
$4.26 \geqslant 100$	$4.25 \geqslant 100$	~~$4.24 \geqslant 100$~~	$5.24 \geqslant 100$	$5.23 \geqslant 100$	$5.22 \geqslant 100$	$5.21 \geqslant 100$	$5.20 \geqslant 100$

~~$5.19 \geqslant 99$~~	$6.19 \geqslant 99$	$6.18 \geqslant 99$	$6.17 \geqslant 99$	~~$6.16 \geqslant 99$~~	$7.16 \geqslant 99$	$7.15 \geqslant 99$	~~$7.14 \geqslant 99$~~
~~$5.19 \geqslant 100$~~	$6.19 \geqslant 100$	$6.18 \geqslant 100$	$6.17 \geqslant 100$	~~$6.16 \geqslant 100$~~	$7.16 \geqslant 100$	$7.15 \geqslant 100$	~~$7.14 \geqslant 100$~~

$8.14 \geqslant 99$	$8.13 \geqslant 99$	~~$8.12 \geqslant 99$~~	$9.12 \geqslant 99$	$9.11 \geqslant 99$	~~$9.10 \geqslant 99$~~	$10.10 \geqslant 99$
$8.14 \geqslant 100$	$8.13 \geqslant 100$	~~$8.12 \geqslant 100$~~	$9.12 \geqslant 100$	~~$9.11 \geqslant 100$~~	$10.11 \geqslant 100$	$10.10 \geqslant 100$

Utiliser la notion de maximum (étant donné un ensemble de variables x, trouver pour chacune d'elles le plus grand y tel que $xy < n$) allège la modélisation :

$$97 \longmapsto \{3,4,5,6,7,8,9,10\} \overset{\varphi_{97}}{\longmapsto} \{32,23,19,15,13,11,10,9\}$$

$$98 \longmapsto \{3,4,5,6,7,8,9,10\} \overset{\varphi_{98}}{\longmapsto} \{32,23,19,15,13,11,10,9\}$$

$$99 \longmapsto \{3,4,5,6,7,8,9,10\} \overset{\varphi_{99}}{\longmapsto} \{32,24,19,16,14,12,10,9\}$$

$$100 \longmapsto \{3,4,5,6,7,8,9,10\} \overset{\varphi_{100}}{\longmapsto} \{33,24,19,16,14,12,11,9\}$$

97 a pour image φ_{97}, 98 a pour image φ_{98}. Puisque $\varphi_{97} = \varphi_{98}$, i.e. puisque 97 et 98 ont même image, 97 est premier.

$\varphi_{99} \neq \varphi_{100}$, 99 et 100 n'ont pas comme images la même fonction, 99 est composé.

Le diagramme associé aux nombres premiers n est caractérisé par le fait qu'n et $n+1$ ont comme image la même fonction, ce qui est noté par la fonction Id sur la flèche descendante droite du diagramme.

$$\begin{array}{ccc} n & \xrightarrow{f_n} & \varphi_n \\ \downarrow{\scriptstyle +1} & & \downarrow{\scriptstyle Id} \\ n+1 & \xrightarrow{f_{n+1}} & \varphi_{n+1} \end{array}$$

φ_n et φ_{n+1} sont deux fonctions de $\{3,\ldots,l_n\}$ dans $\mathbb{N}$ avec $l_n = \lfloor\sqrt{n}\rfloor - 2$. L'image d'un x compris entre 3 et $\lfloor\sqrt{n}\rfloor - 2$ est le plus grand des y tel que $xy < n$.

La fonction f_n associe à n la fonction φ_n.

On préfère écrire plus simplement ce qui vient d'être vu par l'assertion logique suivante :

n $(impair) \in \mathbb{N}$ est un nombre premier $\iff \forall\, x,\ 3 \leqslant x \leqslant \lfloor\sqrt{n}\rfloor,\ max\{y \,/\, xy < n\} = max\{y' \,/\, xy' < n+1\}$.

Découle des mots de Christoffel sous hyperboles (Denise Vella-Chemla, 1/4/2017)

n (*impair*) $\in \mathbb{N}$ est un nombre premier $\iff \forall\, x,\ 2 \leqslant x \leqslant \left\lfloor \frac{2n-1}{4} \right\rfloor,\ \max\{y \,/\, xy < n\} = \max\{y' \,/\, xy' < n+1\}$.

Redondire (Denise Vella-Chemla, 15.4.2017)

On voudrait présenter ici une ébauche d'élaboration d'un comptage exact du nombre de nombres premiers inférieurs à un nombre donné. On a procédé de maière expérimentale, en programmant certains calculs. Comme dans quelques notes récentes au sujet d'hyperboles, on s'intéresse à l'écriture des nombres comme produits de deux entiers supérieurs ou égaux à 2. On a utilisé le programme suivant :

```
#include <iostream>
#include <stdio.h>
#include <math.h>
#include <vector>

int prime(int atester)
{ bool pastrouve=true; unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else if ((atester % k) == 0) return 0 ; else k++;
  }
}

int main(int argc, char* argv[]) {
  const int n=45000 ;
  int i, j, pix, compteprod, compteproddessous, nbredondances, somme, nbdivpropres ;
  std::vector<bool> dejatrouve(n) ;

  pix = 0 ; compteproddessous = 0 ; nbredondances = 0 ;
  somme = 0 ; nbdivpropres = 0 ;
  for (i = 2 ; i < n ; ++i) dejatrouve[i] = false ;
  for (i = 2 ; i < n ; ++i) if (prime(i)) pix=pix+1 ;
  for (i = 2 ; i <= n/2 ; ++i) if (n % i == 0) nbdivpropres = nbdivpropres+1 ;
  for (i = 2 ; i < n-2 ; ++i) somme = somme+((n/i)-1) ;

  for (i = 2 ; i <= n-2 ; ++i)
    for (j = 2 ; j <= n-2 ; ++j) {
      if (i*j < n) {
        compteproddessous = compteproddessous+1 ;
        //std:: cout << i << "*" << j << "=" << i*j << "\n" ;
        if (dejatrouve[i*j] == false) dejatrouve[i*j] = true ;
        else nbredondances = nbredondances+1 ;
      }
    }
  std::cout << "pi(x) = " << pix << "\n" ;
  std::cout << "somme " << somme << "\n" ;
  std::cout << "compteproddessous " << compteproddessous << "\n" ;
  std::cout << "nbdivpropres " << nbdivpropres << "\n" ;
  std::cout << "nbredondances " << nbredondances << "\n" ;
  std::cout << n-compteproddessous+nbredondances << "\n" ;
}
```

La variable *pix* compte le nombre de nombres premiers strictement inférieurs à n. La variable *compteproddessous* compte le nombre de produits de la forme xy avec x et y compris entre 2 et $n-2$ qui sont strictement inférieurs à n. La variable *nbdivpropres* compte le nombre de diviseurs propres de n (i.e. différents de 1 et n). La variable *somme* est égale à $\sum_{i=2}^{n-3} \left(\left\lfloor \frac{n}{i} \right\rfloor - 1 \right)$.

Voici les résultats des calculs effectués par le programme pour quelques nombres :

n	$\pi(x)$	$somme$	$compteproddessous$	$nbdivpropres$	$nbredondances$	$n - compteproddessous + nbredondances$
100	25	283	276	7	203	27
1000	168	5070	5056	14	4226	170
10000	1229	73669	73646	23	64877	1231
45000	4675	399133	399075	58	358752	4677

On a systématiquement :

- $nbdivpropres + compteproddessous = somme$
- ainsi que $pix = n - compteproddessous + nbredondances - 2$.

C'est normal : les nombres premiers sont ceux qui ne peuvent pas s'écrire sous la forme d'un produit de deux nombres supérieurs ou égaux à 2 quels qu'ils soient.

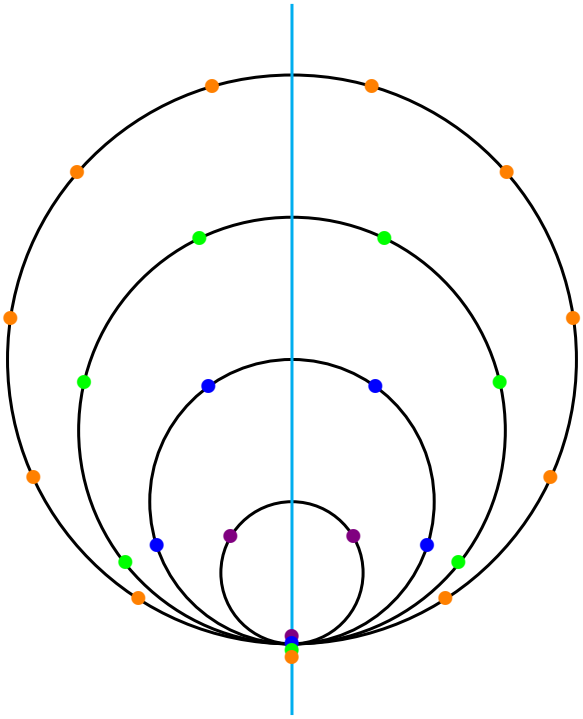
Notre problème reste entier, on n'a fait que le déplacer :

- pourrait-on trouver une formule exacte pour le nombre de produits inférieurs strictement à n ? (comptés par la variable *compteproddessous* du programme et dont on voit qu'il est égal à $-nbdivpropres(n) + \sum_{i=2}^{n-3} \left(\left\lfloor \frac{n}{i} \right\rfloor - 1 \right)$)
- comment compter exactement les redondances, i.e. le nombre d'égalités de la forme $a.b = c.d$?

Polygones modulaires (Denise Vella-Chemla, 30.4.2017)

On cherche ce que les nombres premiers symétrisent.

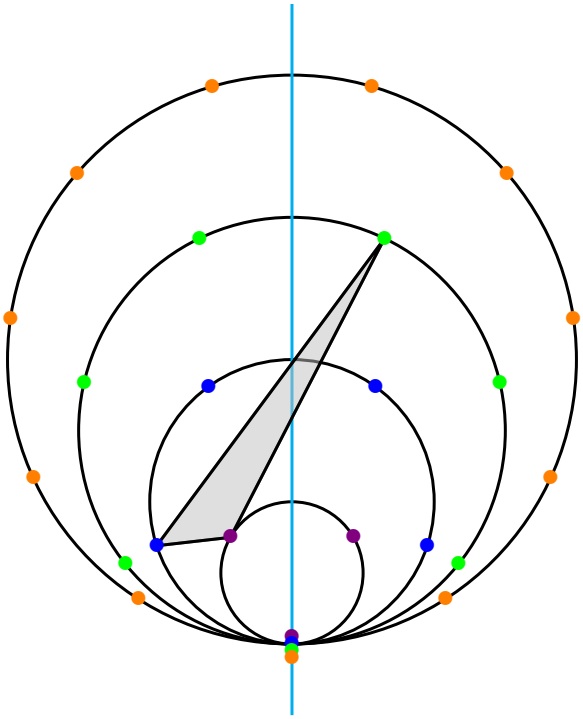
On a pris pour habitude de représenter les entiers par leurs restes modulaires selon les nombres premiers inférieurs à leur racine. Comme les nombres premiers sont tous impairs sauf 3, on va représenter les restes modulaires selon les nombres premiers 3, 5, 7 et 11 sur des cercles de rayon de plus en plus grands et partageant un point (le point tout en bas du graphique ci-dessous) ; ce point correspond dans chaque corps premier $\mathbb{Z}/p\mathbb{Z}$ au reste nul. Les restes modulo 3 correspondent aux 3 points violets du plus petit cercle, les restes modulo 5 (resp. 7, 11) aux points bleus (resp. vert, orange).



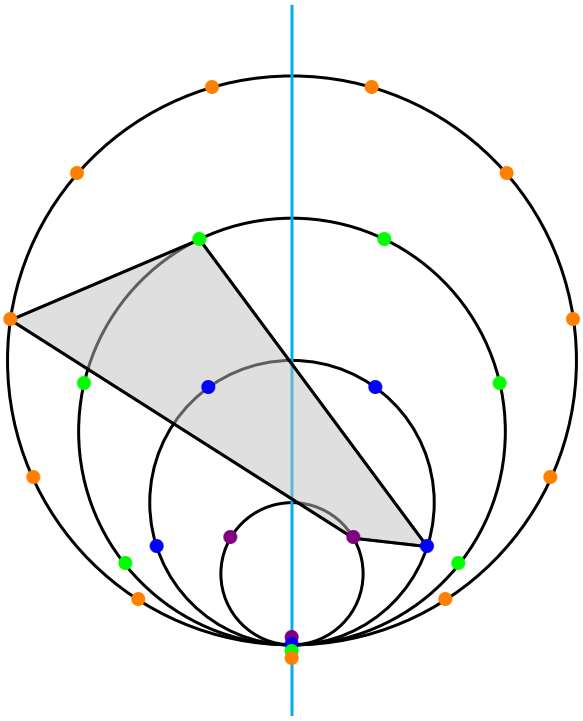
On peut ainsi associer à chaque entier un polygone dont les sommets sont les points correspondant à ses restes modulaires selon le tableau suivant :

n	3	5	7	11	n	3	5	7	11	n	3	5	7	11	n	3	5	7	11
3					47	2	2			91	1	1	0		135	0	0	2	3
5					49	1	4	0		93	0	3	2		137	2	2	4	5
7					51	0	1	2		95	2	0	4		139	1	4	6	7
9	0				53	2	3	4		97	1	2	6		141	0	1	1	9
11	2				55	1	0	6		99	0	4	1		143	2	3	3	0
13	1				57	0	2	1		101	2	1	3		145	1	0	5	2
15	0				59	2	4	3		103	1	3	5		147	0	2	0	4
17	2				61	1	1	5		105	0	0	0		149	2	4	2	6
19	1				63	0	3	0		107	2	2	2		151	1	1	4	8
21	0				65	2	0	2		109	1	4	4		153	0	3	6	10
23	2				67	1	2	4		111	0	1	6		155	2	0	1	1
25	1	0			69	0	4	6		113	2	3	1		157	1	2	3	3
27	0	2			71	2	1	1		115	1	0	3		159	0	4	5	5
29	2	4			73	1	3	3		117	0	2	5		161	2	1	0	7
31	1	1			75	0	0	5		119	2	4	0		163	1	3	2	9
33	0	3			77	2	2	0		121	1	1	2	0	165	0	0	4	0
35	2	0			79	1	4	2		123	0	3	4	2	167	2	2	6	2
37	1	2			81	0	1	4		125	2	0	6	4	169	1	4	1	4
39	0	4			83	2	3	6		127	1	2	1	6					
41	2	1			85	1	0	1		129	0	4	3	8					
43	1	3			87	0	2	3		131	2	1	5	10					
45	0	0			89	2	4	5		133	1	3	0	1					

Le polygone associé à 59 (2,4,3) est représenté ci-dessous :



Le polygone associé à 151 (1,1,4,8) est représenté ci-dessous :



Le polygone d'un nombre premier n'a aucun sommet en (0,0), le sommet origine en bas du graphique

A la recherche d'une formule récurrente (Denise Vella-Chemla, 8.5.2017)

On cherche des formules les plus simples possible pour calculer les valeurs des variables du tableau :

n	$\pi(n)$	$\Delta(n)$	$S(n)$	$C(n)$	$R(n)$		n	$\pi(n)$	$\Delta(n)$	$S(n)$	$C(n)$	$R(n)$		n	$\pi(n)$	$\Delta(n)$	$S(n)$	$C(n)$	$R(n)$
1	0	0	0	0	0		34	11	2	60	58	37		67	19	0	161	161	114
2	1	0	0	0	0		35	11	2	62	60	38		68	19	4	165	161	114
3	2	0	0	0	0		36	11	7	69	62	39		69	19	2	167	165	117
4	2	1	0	−1	0		37	12	0	69	69	45		70	19	6	173	167	118
5	3	0	1	1	0		38	12	2	71	69	45		71	20	0	173	173	123
6	3	2	3	1	0		39	12	2	73	71	46		72	20	10	183	173	123
7	4	0	3	3	1		40	12	6	79	73	47		73	21	0	183	183	132
8	4	2	5	3	1		41	13	0	79	79	52		74	21	2	185	183	132
9	4	1	6	5	2		42	13	6	85	79	52		75	21	4	189	185	133
10	4	2	8	6	2		43	14	0	85	85	57		76	21	4	193	189	136
11	5	0	8	8	3		44	14	4	89	85	57		77	21	2	195	193	139
12	5	4	12	8	3		45	14	4	93	89	60		78	21	6	201	195	140
13	6	0	12	12	6		46	14	2	95	93	63		79	22	0	201	201	145
14	6	2	14	12	6		47	15	0	95	95	64		80	22	8	209	201	145
15	6	2	16	14	7		48	15	8	103	95	64		81	22	3	212	209	152
16	6	3	19	16	18		49	15	1	104	103	71		82	22	2	214	212	154
17	7	0	19	19	10		50	15	4	108	104	71		83	23	0	214	214	155
18	7	4	23	19	10		51	15	2	110	108	74		84	23	10	224	214	155
19	8	0	23	23	13		52	15	4	114	110	75		85	23	2	226	224	164
20	8	4	27	23	13		53	16	0	114	114	78		86	23	2	228	226	165
21	8	2	29	27	16		54	16	6	120	114	78		87	23	2	230	228	166
22	8	2	31	29	17		55	16	2	122	120	83		88	23	6	236	230	167
23	9	0	31	31	18		56	16	6	128	122	84		89	24	0	236	236	172
24	9	6	37	31	18		57	16	2	130	128	89		90	24	10	246	236	172
25	9	1	38	37	23		58	16	2	132	130	90		91	24	2	248	246	181
26	9	2	40	38	23		59	17	0	132	132	91		92	24	4	252	248	182
27	9	2	42	40	24		60	17	10	142	132	91		93	24	2	254	252	185
28	9	4	46	42	25		61	18	0	142	142	100		94	24	2	258	254	186
29	10	0	46	46	28		62	18	2	144	142	100		95	24	2	258	256	187
30	10	6	52	46	28		63	18	4	148	144	101		96	24	10	268	258	188
31	11	0	52	52	33		64	18	5	153	148	104		97	25	0	268	268	197
32	11	4	56	52	33		65	18	2	155	153	108		98	25	4	272	268	197
33	11	2	58	56	36		66	18	6	161	155	109		99	25	4	276	272	200
														100	25	7	283	276	203

On a :

- $\mathrm{S(n)} = \sum_{i=2}^{n-3} \left(\left\lfloor \frac{n}{i} \right\rfloor - 1 \right)$;
- $\Delta(n) = \#\{d < n \textit{ tel que } d \mid n\}$; dans l'article A032741[1] de l'OEIS (Open Encyclopedia of Integer Sequences), il est indiqué que $\Delta(n)$ est le nombre de facteurs du nième polynôme de Fibonacci ou que $\Delta(n+1)$ est le nombre de facteurs du polynôme du nième degré $x^n + x^{n-1} + x^{n-2} + \ldots$;
- C(n) est le nombre de produits d'entiers ij strictement inférieurs à n, pour i et j variant de 2 à $n-2$, diminué de 1 ;
- on impose un ordre total lexicographique sur les produits de deux entiers : ab est avant $a'b'$ selon cet ordre si et seulement si $(a < a')$ *ou* $((a = a')$ *et* $(b < b'))$.

  $R(n)$ (pour nombre de redondances) est le nombre de produits d'entiers $i'j'$ strictement inférieurs à n, pour i' et j' variant de 2 à $n-2$ tels qu'il existe un produit de même valeur ij avec (i,j) qui est antérieur à (i',j') selon l'ordre lexicographique : on ne garde qu'un représentant par classe de produits de deux entiers de même valeur ;
- $C(n) = S(n) - \Delta(n)$;

[1] séquence à démarrer à 2.

- $\pi(n) \;=\; n - S(n) + \Delta(n) + R(n) - 2 = n - C(n) + R(n) - 2$;
- $C(n+1) = S(n)$ pour $n \geqslant 5$.

Exemple :

$C(10) = 6$ car 6 est le nombre de produits de la liste ci-dessous strictement inférieurs à 10 (on les a notés en rouge).

2×2	2×3	2×4	2×5	2×6	2×7	2×8
3×2	3×3	3×4	3×5	3×6	3×7	3×8
4×2	4×3	4×4	4×5	4×6	4×7	4×8
5×2	5×3	5×4	5×5	5×6	5×7	5×8
6×2	6×3	6×4	6×5	6×6	6×7	6×8
7×2	7×3	7×4	7×5	7×6	7×7	7×8
8×2	8×3	8×4	8×5	8×6	8×7	8×8

$R(10) = 2$ car $3 \times 2 = 2 \times 3$ et $4 \times 2 = 2 \times 4$: on dénombre 2 produits redondants. L'ordre lexicographique dont il a été question plus haut est ici l'ordre de lecture habituel, de gauche à droite puis de bas en haut.

Parité (Denise Vella-Chemla, 13.5.2017)

On cherche des formules les plus simples possible pour calculer les valeurs des variables du tableau :

n	$\pi(n)$	$\Delta(n)$	$S(n)$	$C(n)$	$R(n)$		n	$\pi(n)$	$\Delta(n)$	$S(n)$	$C(n)$	$R(n)$		n	$\pi(n)$	$\Delta(n)$	$S(n)$	$C(n)$	$R(n)$
1	0	0	0	0	0		34	11	2	60	58	37		67	19	0	161	161	114
2	1	0	0	0	0		35	11	2	62	60	38		68	19	4	165	161	114
3	2	0	0	0	0		36	11	7	69	62	39		69	19	2	167	165	117
4	2	1	0	−1	0		37	12	0	69	69	45		70	19	6	173	167	118
5	3	0	1	1	0		38	12	2	71	69	45		71	20	0	173	173	123
6	3	2	3	1	0		39	12	2	73	71	46		72	20	10	183	173	123
7	4	0	3	3	1		40	12	6	79	73	47		73	21	0	183	183	132
8	4	2	5	3	1		41	13	0	79	79	52		74	21	2	185	183	132
9	4	1	6	5	2		42	13	6	85	79	52		75	21	4	189	185	133
10	4	2	8	6	2		43	14	0	85	85	57		76	21	4	193	189	136
11	5	0	8	8	3		44	14	4	89	85	57		77	21	2	195	193	139
12	5	4	12	8	3		45	14	4	93	89	60		78	21	6	201	195	140
13	6	0	12	12	6		46	14	2	95	93	63		79	22	0	201	201	145
14	6	2	14	12	6		47	15	0	95	95	64		80	22	8	209	201	145
15	6	2	16	14	7		48	15	8	103	95	64		81	22	3	212	209	152
16	6	3	19	16	18		49	15	1	104	103	71		82	22	2	214	212	154
17	7	0	19	19	10		50	15	4	108	104	71		83	23	0	214	214	155
18	7	4	23	19	10		51	15	2	110	108	74		84	23	10	224	214	155
19	8	0	23	23	13		52	15	4	114	110	75		85	23	2	226	224	164
20	8	4	27	23	13		53	16	0	114	114	78		86	23	2	228	226	165
21	8	2	29	27	16		54	16	6	120	114	78		87	23	2	230	228	166
22	8	2	31	29	17		55	16	2	122	120	83		88	23	6	236	230	167
23	9	0	31	31	18		56	16	6	128	122	84		89	24	0	236	236	172
24	9	6	37	31	18		57	16	2	130	128	89		90	24	10	246	236	172
25	9	1	38	37	23		58	16	2	132	130	90		91	24	2	248	246	181
26	9	2	40	38	23		59	17	0	132	132	91		92	24	4	252	248	182
27	9	2	42	40	24		60	17	10	142	132	91		93	24	2	254	252	185
28	9	4	46	42	25		61	18	0	142	142	100		94	24	2	258	254	186
29	10	0	46	46	28		62	18	2	144	142	100		95	24	2	258	256	187
30	10	6	52	46	28		63	18	4	148	144	101		96	24	10	268	258	188
31	11	0	52	52	33		64	18	5	153	148	104		97	25	0	268	268	197
32	11	4	56	52	33		65	18	2	155	153	108		98	25	4	272	268	197
33	11	2	58	56	36		66	18	6	161	155	109		99	25	4	276	272	200
														100	25	7	283	276	203

On a :

- $S(n) = \sum_{i=2}^{n-3} \left(\left\lfloor \frac{n}{i} \right\rfloor - 1 \right)$;
- $\Delta(n) = \#\{d < n \textit{ tel que } d \mid n\}$; dans l'article A032741[1] de l'OEIS (Open Encyclopedia of Integer Sequences), il est indiqué que $a(n) = \Delta(n) + 1$ (pour $n \geqslant 7$) est le nombre de facteurs du nième polynôme de Fibonacci ou que $\Delta(n+1)$ est le nombre de facteurs du polynôme du nième degré $x^n + x^{n-1} + x^{n-2} + \ldots$; si $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ alors $\Delta(n) = -2 + \prod_{i=1}^{k} (\alpha_i + 1)$;
- $C(n)$ est le nombre de produits d'entiers ij strictement inférieurs à n, pour i et j variant de 2 à $n-2$;
- on impose un ordre total lexicographique sur les produits de deux entiers : ab est avant $a'b'$ selon cet ordre si et seulement si $(a < a')$ *ou* $((a = a')$ *et* $(b < b'))$.

  $R(n)$ (pour nombre de redondances) est le nombre de produits d'entiers $i'j'$ strictement inférieurs à n, pour i' et j' variant de 2 à $n-2$ tels qu'il existe un produit de même valeur ij avec (i,j) qui est antérieur à (i',j') selon l'ordre lexicographique : on ne garde qu'un représentant par classe de produits de deux entiers de même valeur ;

[1] séquence à démarrer à 2.

- $C(n) \;=\; S(n) - \Delta(n)$;
- $\pi(n) \;=\; n - S(n) + \Delta(n) + R(n) - 2 = n - C(n) + R(n) - 2$;
- $C(n+1) = S(n)$ pour $n \geqslant 5$;
- $S(n) + \Delta(n+1) = S(n+1)$ pour $n \geqslant 5$;
- $S(n) = \sum_{k=1}^{n} \Delta(k)$ et $C(n) = \sum_{k=1}^{n-1} \Delta(k)$ pour $n \geqslant 5$.

Exemple :

$C(10) = 6$ car 6 est le nombre de produits de la liste ci-dessous strictement inférieurs à 10 (on les a notés en rouge).

$$\begin{array}{ccccccc}
2\times 2 & 2\times 3 & 2\times 4 & 2\times 5 & 2\times 6 & 2\times 7 & 2\times 8 \\
3\times 2 & 3\times 3 & 3\times 4 & 3\times 5 & 3\times 6 & 3\times 7 & 3\times 8 \\
4\times 2 & 4\times 3 & 4\times 4 & 4\times 5 & 4\times 6 & 4\times 7 & 4\times 8 \\
5\times 2 & 5\times 3 & 5\times 4 & 5\times 5 & 5\times 6 & 5\times 7 & 5\times 8 \\
6\times 2 & 6\times 3 & 6\times 4 & 6\times 5 & 6\times 6 & 6\times 7 & 6\times 8 \\
7\times 2 & 7\times 3 & 7\times 4 & 7\times 5 & 7\times 6 & 7\times 7 & 7\times 8 \\
8\times 2 & 8\times 3 & 8\times 4 & 8\times 5 & 8\times 6 & 8\times 7 & 8\times 8
\end{array}$$

$R(10) = 2$ car $3 \times 2 = 2 \times 3$ et $4 \times 2 = 2 \times 4$: on dénombre 2 produits redondants. L'ordre lexicographique dont il a été question plus haut est ici l'ordre de lecture habituel, de gauche à droite puis de bas en haut.

On constate et il faudrait le démontrer que $S(n)$ et $S(n-1)$ n'ont pas même parité lorsque n est un carré d'entier (une puissance paire d'entier).

On constate et il faudrait le démontrer que $R(n)$ et $R(n+1)$ ont même parité lorsque n est un nombre premier ou un carré d'entier (une puissance paire d'entier).

On constate et il faudrait le démontrer que $S(n) = C(n)$ lorsque n est un nombre premier. C'est une condition surprenante :

$$n \;\; premier$$
$$\Longleftrightarrow$$
$$\sum_{i=2}^{n-3} \left(\left\lfloor \frac{n}{i} \right\rfloor - 1 \right) = \#\left\{ xy \;\; tels \;\; que \;\; (xy < n) \;\wedge\; (2 \leqslant x \leqslant n-2) \;\wedge\; (2 \leqslant y \leqslant n-2) \right\}$$

Cette condition d'égalité $S(n) = C(n)$ fait vraiment souhaiter voir les nombres premiers comme points fixes d'une fonction qui associerait $S(n)$ à $C(n) = S(n-1)$ (i.e. ferait passer de $S(n-1)$ à $S(n)$).

On a utilisé le programme fourni page suivante.

```
#include <iostream>
#include <stdio.h>
#include <math.h>
#include <vector>
#include <bitset>

int prime(int atester)
{ bool pastrouve=true; unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else if ((atester % k) == 0) return 0 ; else k++;
  }
}

int main(int argc, char* argv[]) {
  std::vector<bool> dejatrouve(n) ;
  int n, i, j, pix, compteprod, compteproddessous ;
  int gardenbredondances, nbredondances, gardesomme, somme, nbdiv ;
  int schangeparite, redondchangeparite, nbimpairs ;

  for (n = 1 ; n <= 1000 ; ++n)
    {
      pix = 0 ;
      compteproddessous = 0 ;
      gardenbredondances = nbredondances ;
      nbredondances = 0 ;
      gardesomme = somme ;
      somme = 0 ;
      nbdiv = 0 ;
      for (i = 2 ; i < n ; ++i) dejatrouve[i] = false ;
      for (i = 2 ; i < n ; ++i) if (prime(i)) pix=pix+1 ;
      for (i = 2 ; i <= n/2 ; ++i) if (n % i == 0) nbdiv = nbdiv+1 ;
      for (i = 2 ; i < n-2 ; ++i) somme = somme+((n/i)-1) ;
      for (i = 2 ; i <= n-2 ; ++i)
         for (j = 2 ; j <= n-2 ; ++j) {
           if (i*j < n) {
             compteproddessous = compteproddessous+1 ;
             if (dejatrouve[i*j] == false) dejatrouve[i*j] = true ;
             else nbredondances = nbredondances+1 ;
           }
         }
      std::cout << "\nn -> " << n << "\n" ;
      std::cout << "pi(x) = " << pix << "\n" ;
      std::cout << "nbdiv " << nbdiv << "\n" ;
      std::cout << "gardesomme " << gardesomme << "\n" ;
      std::cout << "somme " << somme << "\n" ;
      if (((somme % 2) == 0) != ((gardesomme % 2) == 0))
        std::cout << "Somme change de parité. \n" ;
      std::cout << "compteproddessous " << compteproddessous << "\n" ;
      std::cout << "gardenbredondances " << gardenbredondances << "\n" ;
      std::cout << "nbredondances " << nbredondances << "\n" ;
      if (((gardenbredondances % 2)==0) == ((nbredondances % 2)==0))
        std::cout << "nbredondances ne change pas de parité pour " << n-1 << "\n" ;
    }
}
```

Voir la primalité dans le triangle de Pascal (Denise Vella-Chemla, 14.5.2017)

A la recherche de formules de calcul en lien avec les nombres premiers, on a trouvé un fait surprenant, fourni par Benoit Cloitre au sujet de la séquence A032741, et qui permet de lire la primalité des nombres horizontalement, directement dans les coefficients binomiaux du triangle de Pascal.

Le nombre, noté $a(n+1)$, de diviseurs de n vérifie :

$$a(n+1) = \#\{k \; tels \; que \; 0 \leqslant k \leqslant n-1 \; et \; C_n^k \mid C_n^{k+1}\}$$

On écrit les coefficients binomiaux et on compte le nombre de relations de divisibilité entre nombres successifs d'une même ligne (relation notée par une flèche bleue). S'il n'y a qu'une telle relation de divisibilité sur la ligne de n alors $n+1$ est premier.

0	1														
1	1	→1													
2	1	→2	1												
3	1	→3	→3	1											
4	1	→4	6	4	1										
5	1	→5	→10	→10	5	1									
6	1	→6	15	20	15	6	1								
7	1	→7	→21	35	→35	21	7	1							
8	1	→8	28	→56	70	56	28	8	1						
9	1	→9	→36	84	126	→126	84	36	9	1					
10	1	→10	45	120	210	252	210	120	45	10	1				
11	1	→11	→55	→165	→330	462	→462	330	165	55	11	1			
12	1	→12	66	220	495	792	924	792	495	220	66	12	1		
13	1	→13	→78	286	715	1287	1716	→1716	1287	715	286	78	13	1	
14	1	→14	91	→364	1001	→2002	3003	3432	3003	2002	1001	364	91	14	1
15	1	→15	105	455	→1365	3003	5005	6435	→6435	5005	3003	1365	455	105	15	1

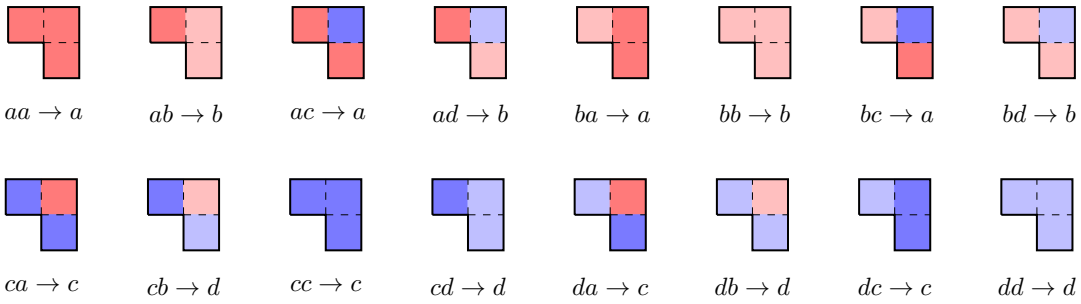
Compter les relations de divisibilité de la ligne de $n-1$ du triangle de Pascal permet de dénombrer les diviseurs de n différents de n.

$a(2) = 1$
$a(3) = 2$
$a(4) = 1$
$a(5) = 3$
$a(6) = 1$
$a(7) = 3$
$a(8) = 2$
$a(9) = 3$
$a(10) = 1$
$a(11) = 5$
$a(12) = 1$
$a(13) = 3$
$a(14) = 3$
$a(15) = 4$

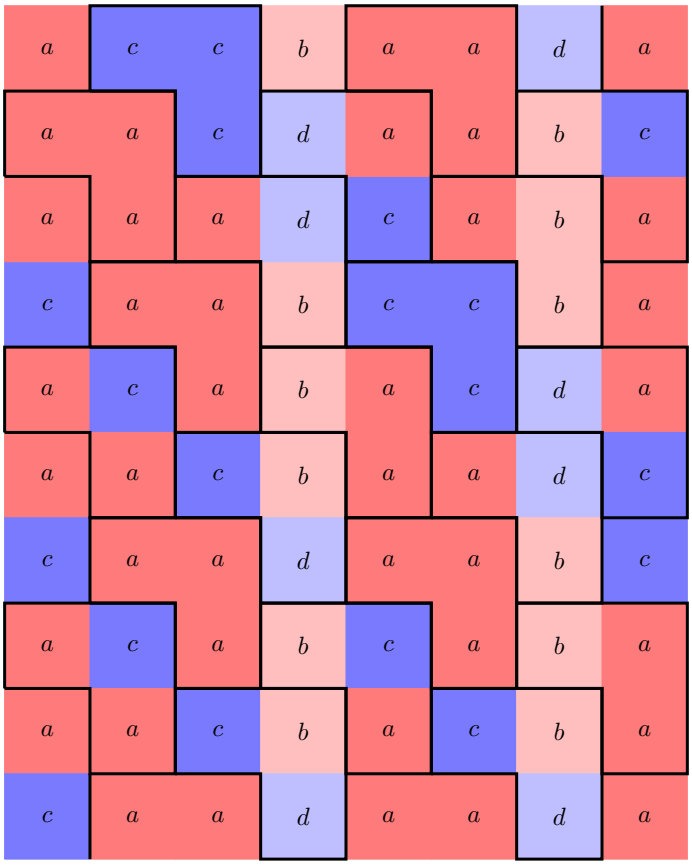
Espace des nombres premiers et pavage apériodique du plan par des triminos colorés (Denise Vella-Chemla, 21.5.2017)

On voudrait ici associer à un ensemble de règles de réécriture qu'on avait mises au jour dans le cadre de recherches d'une démonstration de la conjecture de Goldbach un pavage du plan euclidien par des triminos colorés.

Voici les triminos dont on dispose, au nombre de 16.



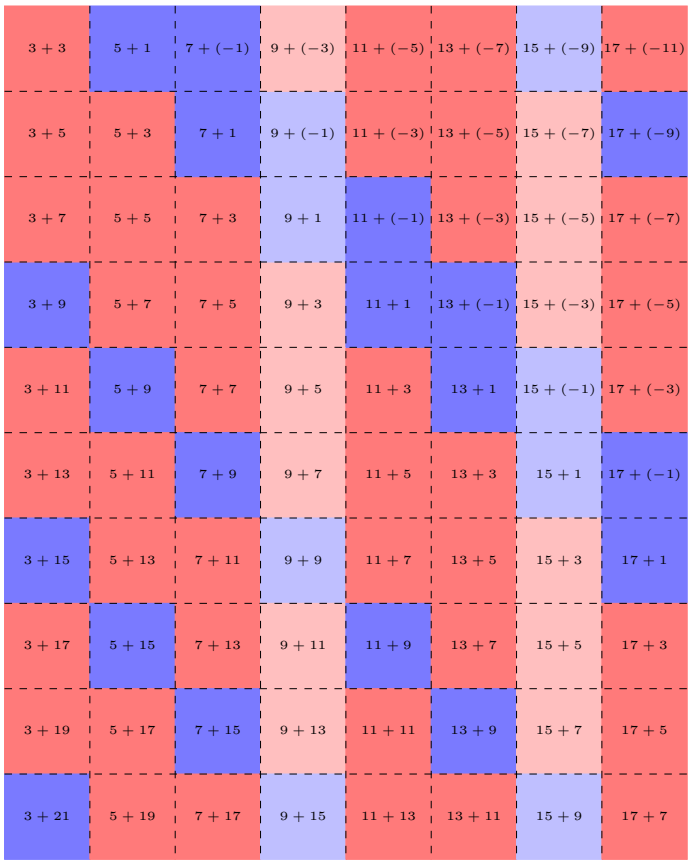
Voici un pavage du plan à l'aide de ces triminos.



Les couleurs sont à comparer aux couleurs associées aux décompositions des nombres pairs comme sommes de deux nombres impairs comme présenté sur le schéma ci-après :

- une décomposition de la forme *premier* + *premier* (lettre *a*) est colorée en rouge pâle ;
- une décomposition de la forme *composé* + *premier* (lettre *b*) est colorée en red!25 ;
- une décomposition de la forme *premier* + *composé* (lettre *c*) est colorée en gris pâle ;

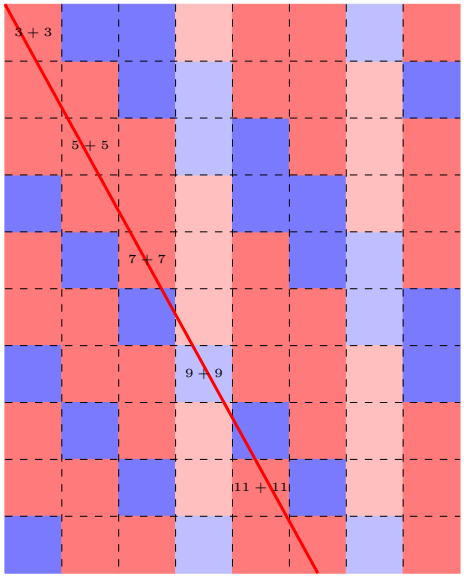
- et enfin, une décomposition de la forme *composé* + *composé* (lettre d) est colorée en vert.



Les couleurs des triminos, qu'on appelait les 16 règles, sont motivées par toutes les implications logiques qui font que si $n = x_1 + y_1 = (x_1 + 2) + (y_2 - 2)$ alors $n + 2 = (x_1 + 2) + y_1$. Cela correspond au fait que la couleur du carré en bas à droite de chaque trimino est complètement déterminée par les couleurs des deux carrés en haut du trimino[1].

On peut lire les décompositions triviales de Goldbach de la forme $2p = p + p$ sur une droite de coefficient directeur -2.

[1]Dit autrement, la couleur verte de la décomposition $9 + 15$ se déduit des couleurs grise et red!25 des décompositions $7 + 15$ et $9 + 13$ en prenant la "composante gauche" de la couleur de $9 + 13$ et la "composante droite" de la couleur de $7 + 15$.



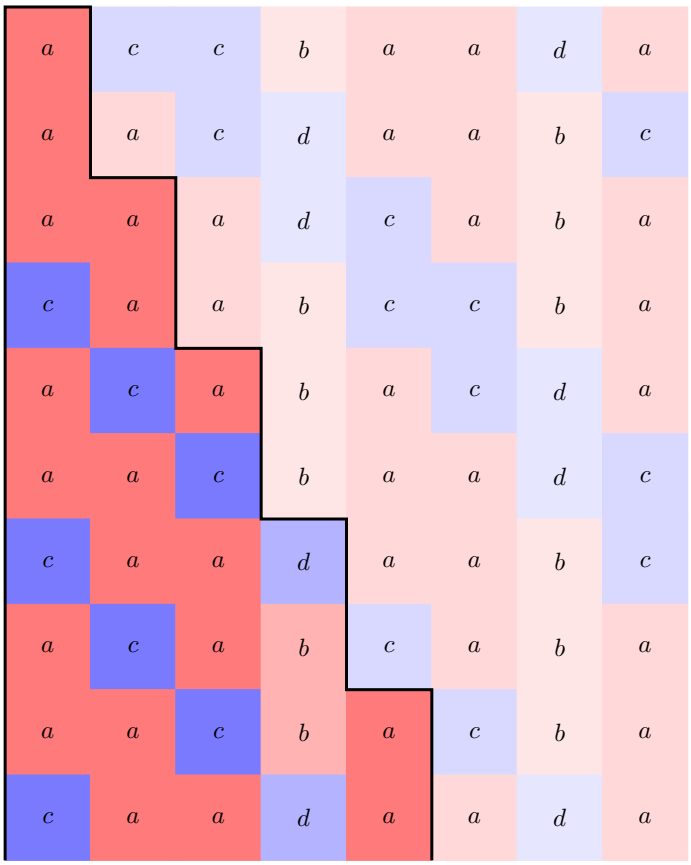
Bibliographie

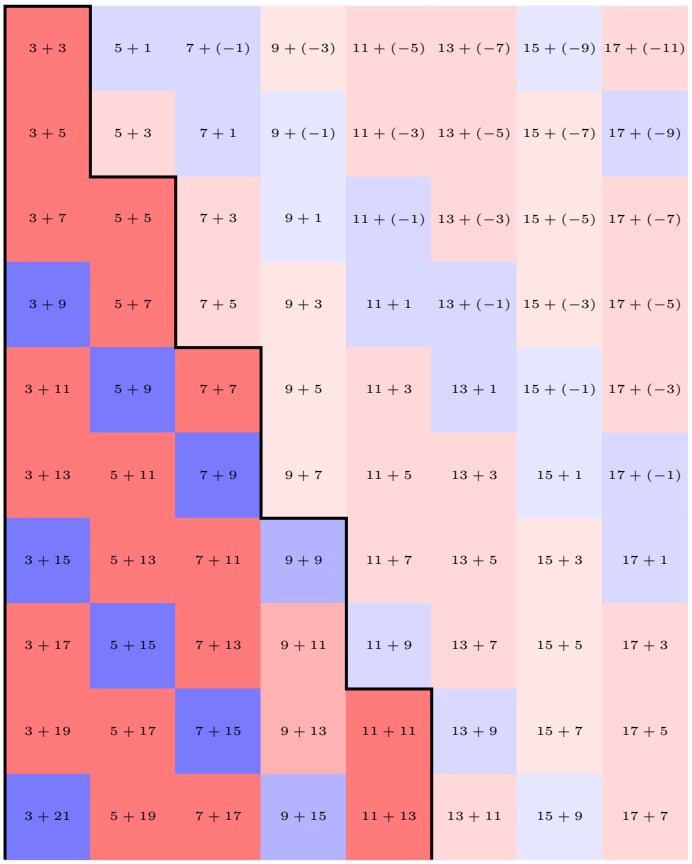
[1] D. Vella-Chemla, *Modéliser*, 31.10.2015, http://denise.vella.chemla.free.fr/champ-de-lettres.pdf.

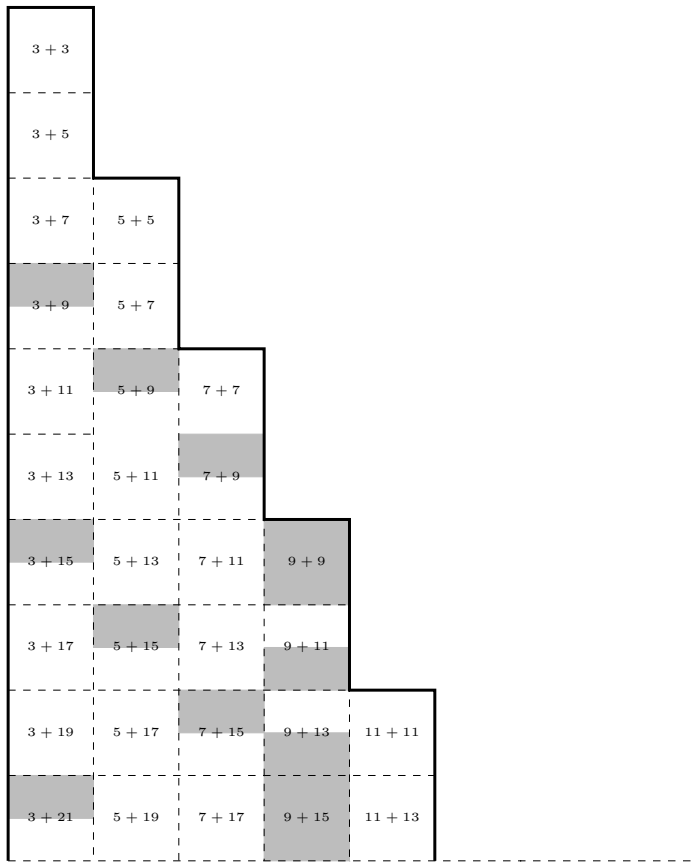
[2] A. Connes, *Géométrie non-commutative*, Dunod, 1990.

[3] B. Grünbaum, G.C. Shephard, *Tilings and patterns*, Freeman and company, New York, 1987.

Dessins colorés (Denise Vella-Chemla, 21.5.2017)



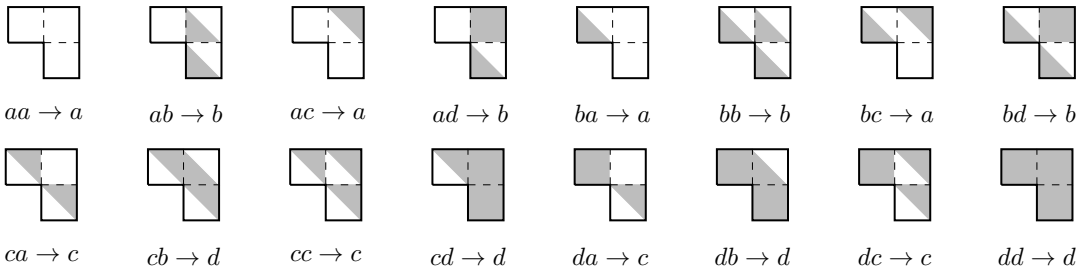

3 + 3
5 + 1
7 + (−1)
9 + (−3)
11 + (−5)
13 + (−7)
15 + (−9)
17 + (−11)
3 + 5
5 + 3
7 + 1
9 + (−1)
11 + (−3)
13 + (−5)
15 + (−7)
17 + (−9)
3 + 7
5 + 5
7 + 3
9 + 1
11 + (−1)
13 + (−3)
15 + (−5)
17 + (−7)
3 + 9
5 + 7
7 + 5
9 + 3
11 + 1
13 + (−1)
15 + (−3)
17 + (−5)
3 + 11
5 + 9
7 + 7
9 + 5
11 + 3
13 + 1
15 + (−1)
17 + (−3)
3 + 13
5 + 11
7 + 9
9 + 7
11 + 5
13 + 3
15 + 1
17 + (−1)
3 + 15
5 + 13
7 + 11
9 + 9
11 + 7
13 + 5
15 + 3
17 + 1
3 + 17
5 + 15
7 + 13
9 + 11
11 + 9
13 + 7
15 + 5
17 + 3
3 + 19
5 + 17
7 + 15
9 + 13
11 + 11
13 + 9
15 + 7
17 + 5
3 + 21
5 + 19
7 + 17
9 + 15
11 + 13
13 + 11
15 + 9
17 + 7


3 + 3
3 + 5
3 + 7
5 + 5
3 + 9
5 + 7
3 + 11
5 + 9
7 + 7
3 + 13
5 + 11
7 + 9
3 + 15
5 + 13
7 + 11
9 + 9
3 + 17
5 + 15
7 + 13
9 + 11
3 + 19
5 + 17
7 + 15
9 + 13
11 + 11
3 + 21
5 + 19
7 + 17
9 + 15
11 + 13

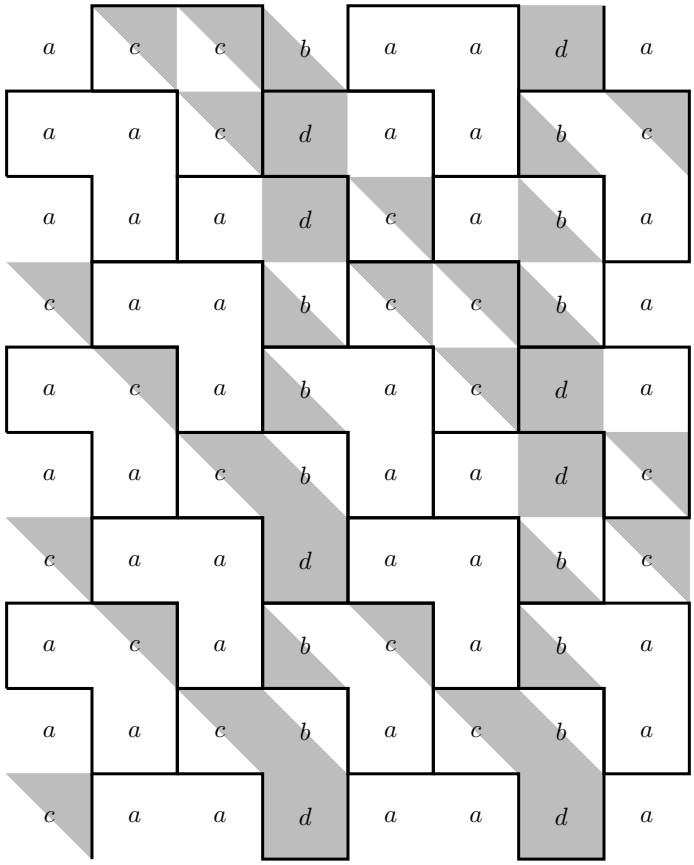
Espace des nombres premiers et pavage apériodique du plan par des triminos bicolores (Denise Vella-Chemla, 22.5.2017)

On voudrait ici associer à un ensemble de règles de réécriture qu'on avait mises au jour dans le cadre de recherches d'une démonstration de la conjecture de Goldbach un pavage du plan euclidien par des triminos bicolores.

Voici les triminos dont on dispose, au nombre de 16.



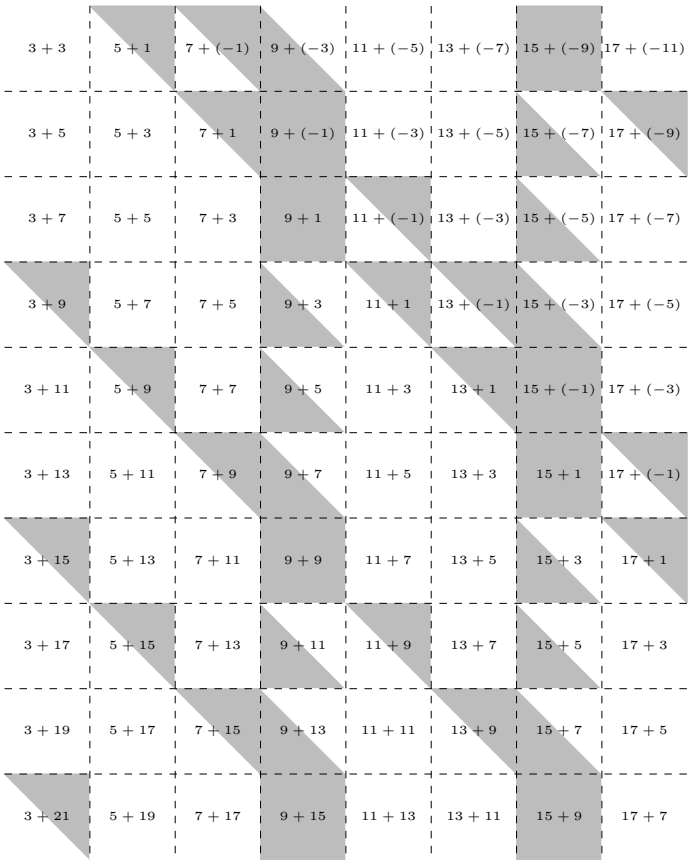
Voici un pavage du plan à l'aide de ces triminos.



Les couleurs sont à comparer aux couleurs associées aux décompositions des nombres pairs comme sommes de deux nombres impairs comme présenté sur le schéma ci-après :

- une décomposition de la forme *premier* + *premier* (lettre a) est colorée en blanc ;
- une décomposition de la forme *composé* + *premier* (lettre b) est colorée en gris au sud-ouest et blanc au nord-est ;
- une décomposition de la forme *premier* + *composé* (lettre c) est colorée en blanc au sud-ouest et gris au nord-est ;

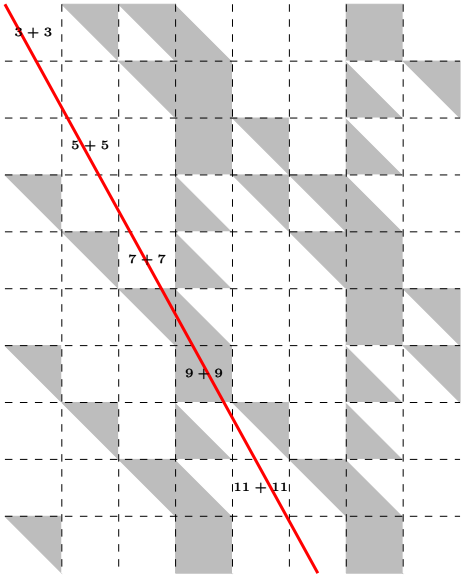
- et enfin, une décomposition de la forme *composé* + *composé* (lettre d) est colorée en gris.



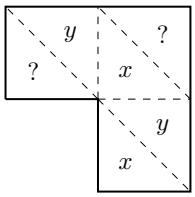
Les couleurs des triminos, qu'on appelait les 16 règles, sont motivées par toutes les implications logiques qui font que si $n = x_1 + y_1 = (x_1 + 2) + (y_2 - 2)$ alors $n + 2 = (x_1 + 2) + y_1$. Cela correspond au fait que la couleur du carré en bas à droite de chaque trimino est complètement déterminée par les couleurs des deux carrés en haut du trimino[1].

On peut lire les décompositions triviales de Goldbach de la forme $2p = p + p$ sur une droite de coefficient directeur -2.

[1]Dit autrement, la couleur d de la décomposition $9 + 15$ se déduit des couleurs c et b des décompositions $7 + 15$ et $9 + 13$ en prenant la "composante gauche" de la couleur de $9 + 13$ (le gris) et la "composante droite" de la couleur de $7 + 15$ (le gris aussi).

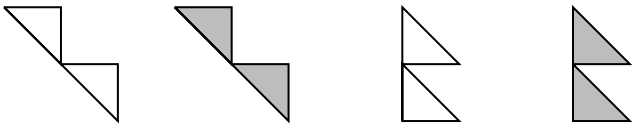


On peut ajouter que tous les triminos, abstraction faite de la bicoloration sont en fait d'une seule forme et leur bicoloration est telle que la couleur x est la même aux 2 endroits indiqués et la couleur y est la même aux deux autres endroits indiqués sur la figure ci-après. Les points d'interrogation dans les autres petits triangles du trimino indiquent que les contraintes portant sur les couleurs en question ne sont pas associées au trimino considéré. Il faut que toutes les contraintes des triminos soient respectées lorsqu'on on décale les bordures des triminos des 3 seules façons possible, la bicoloration restant fixe : prenons l'un des 3 sous-carrés des triminos, par exemple celui en haut à gauche ; selon le premier choix de bordure, il sera effectivement en haut à gauche du trimino qui le contient, selon le deuxième choix de bordure, il sera en haut à droite et selon le troisième choix de bordure, il sera en bas à droite.



Les seuls pavages qui nous intéressent sont ceux dans lesquels tous les triminos sont dans l'orientation qu'on a proposée (on ne pave pas en mettant les deux sous-carrés en bas par exemple). Cela oblige à paver "en diagonale".

Dans la mesure où on peut paver le plan avec des tuiles pouvant être constituées de plusieurs morceaux [2], le problème peut être simpifié en n'ayant à sa disposition que 4 tuiles de 2 formes différentes, chacune des deux couleurs possibles et qui contraindraient le pavage aux contraintes sur x et y vues ci-dessus. Les voici :



Bibliographie

[1] D. Vella-Chemla, *Modéliser*, 31.10.2015, http://denise.vella.chemla.free.fr/champ-de-lettres.pdf.

[2] A. Connes, *Géométrie non-commutative*, Dunod, 1990.

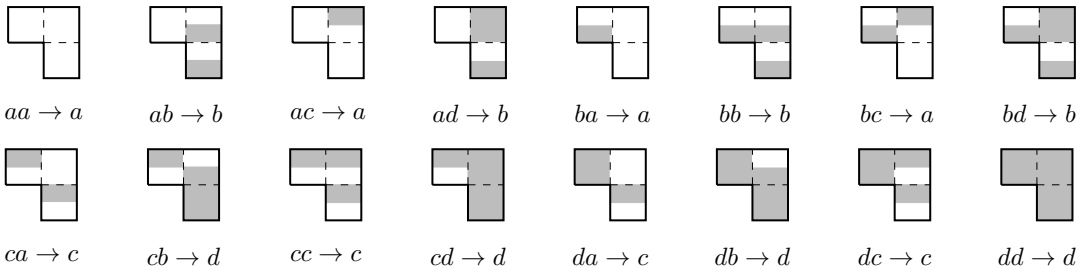
[3] B. Grünbaum, G.C. Shephard, *Tilings and patterns*, Freeman and company, New York, 1987.

[2] tuiles qui ne sont pas des disques topologiques ?

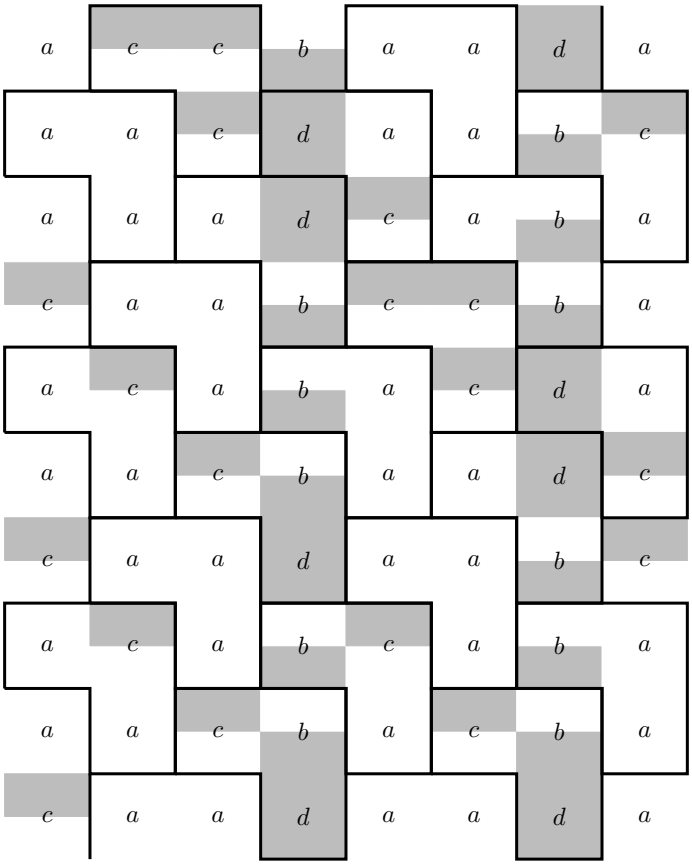
Espace des nombres premiers et pavage apériodique du plan par des triminos bicolores (Denise Vella-Chemla, 22.5.2017)

On voudrait ici associer à un ensemble de règles de réécriture qu'on avait mises au jour dans le cadre de recherches d'une démonstration de la conjecture de Goldbach un pavage du plan euclidien par des triminos bicolores.

Voici les triminos dont on dispose, au nombre de 16.



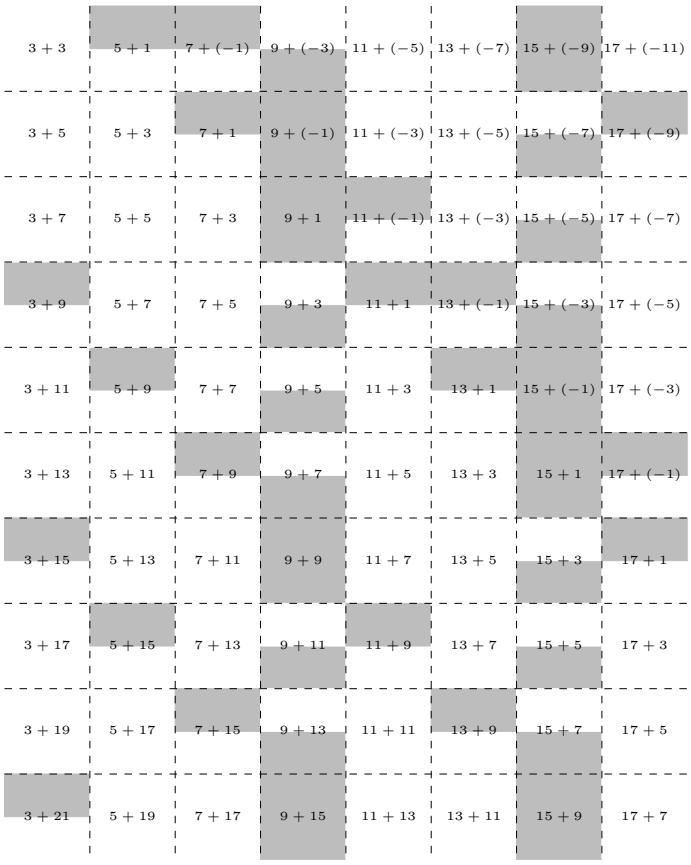
Voici un pavage du plan à l'aide de ces triminos.



Les couleurs sont à comparer aux couleurs associées aux décompositions des nombres pairs comme sommes de deux nombres impairs comme présenté sur le schéma ci-après :

- une décomposition de la forme *premier* + *premier* (lettre a) est colorée en blanc ;
- une décomposition de la forme *composé* + *premier* (lettre b) est colorée en gris dans sa partie moitié inférieure et blanc dans sa partie moitié supérieure ;
- une décomposition de la forme *premier* + *composé* (lettre c) est colorée en blanc dans sa partie moitié inférieure et gris dans sa partie moitié supérieure ;

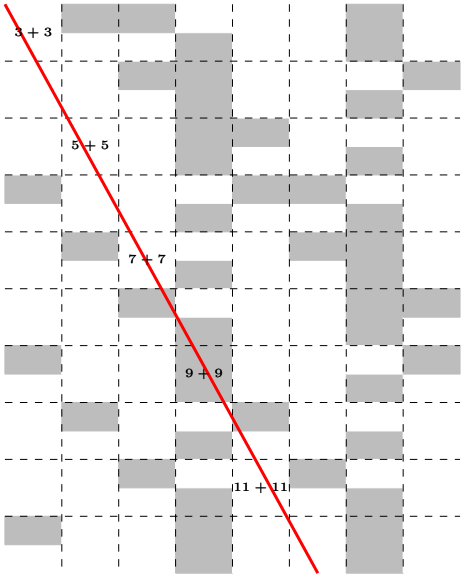
- et enfin, une décomposition de la forme *composé* + *composé* (lettre d) est colorée en gris.



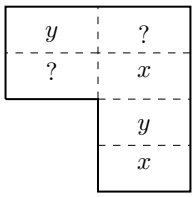
Les couleurs des triminos, qu'on appelait les 16 règles, sont motivées par toutes les implications logiques qui font que si $n = x_1 + y_1 = (x_1 + 2) + (y_2 - 2)$ alors $n + 2 = (x_1 + 2) + y_1$. Cela correspond au fait que la couleur du carré en bas à droite de chaque trimino est complètement déterminée par les couleurs des deux carrés en haut du trimino[1].

On peut lire les décompositions triviales de Goldbach de la forme $2p = p + p$ sur une droite de coefficient directeur -2.

[1]Dit autrement, la couleur d de la décomposition $9 + 15$ se déduit des couleurs c et b des décompositions $7 + 15$ et $9 + 13$ en prenant la "composante gauche" de la couleur de $9 + 13$ (le gris) et la "composante droite" de la couleur de $7 + 15$ (le gris aussi).



On peut ajouter que tous les triminos, abstraction faite de la bicoloration sont en fait d'une seule forme et leur bicoloration est telle que la couleur x est la même aux 2 endroits indiqués et la couleur y est la même aux deux autres endroits indiqués sur la figure ci-après. Les points d'interrogation dans les autres petits triangles du trimino indiquent que les contraintes portant sur les couleurs en question ne sont pas associées au trimino considéré. Il faut que toutes les contraintes des triminos soient respectées lorsqu'on on décale les bordures des triminos des 3 seules façons possible, la bicoloration restant fixe : prenons l'un des 3 sous-carrés des triminos, par exemple celui en haut à gauche ; selon le premier choix de bordure, il sera effectivement en haut à gauche du trimino qui le contient, selon le deuxième choix de bordure, il sera en haut à droite et selon le troisième choix de bordure, il sera en bas à droite.



Les seuls pavages qui nous intéressent sont ceux dans lesquels tous les triminos sont dans l'orientation qu'on a proposée (on ne pave pas en mettant les deux sous-carrés en bas par exemple). Cela oblige à paver "en diagonale".

Dans la mesure où on peut paver le plan avec des tuiles pouvant être constituées de plusieurs morceaux [2], le problème peut être simpifié en n'ayant à sa disposition que 4 tuiles de 2 formes différentes, chacune des deux couleurs possibles et qui contraindraient le pavage aux contraintes sur x et y vues ci-dessus. Les voici :

Bibliographie

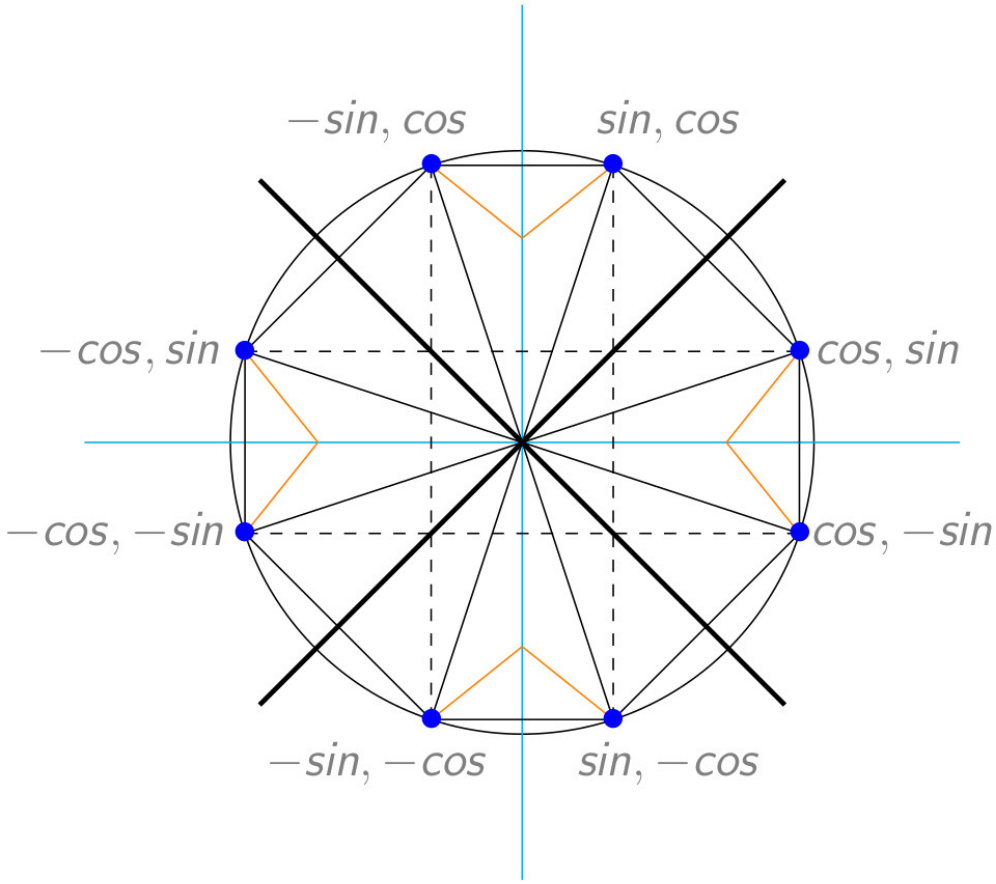
[1] D. Vella-Chemla, *Modéliser*, 31.10.2015, http://denise.vella.chemla.free.fr/champ-de-lettres.pdf.

[2] A. Connes, *Géométrie non-commutative*, Dunod, 1990.

[3] B. Grünbaum, G.C. Shephard, *Tilings and patterns*, Freeman and company, New York, 1987.

[2] tuiles qui ne sont pas des disques topologiques ?

Malte



Trouver un passage vers un lieu que quelqu'un connaît (Denise Vella-Chemla, 27.5.2017)

On a exposé dans une note récente une manière de paver le plan à l'aide de tuiles bicolores. Ce pavage permettait de représenter les décompositions des nombres pairs en sommes de deux impairs.

Pour transformer le pavage que l'on a proposé en un pavage de Penrose, on ne considère plus que des tuiles rectangulaires élémentaires. Un nombre premier est codé par une tuile rectangle blanche tandis qu'un nombre composé est codé par une tuile rectangle grise. Pour mémoire, on note les décompositions dans les tuiles, le premier sommant est codé par le rectangle du bas des carrés délimités et le second sommant est codé par le rectangle du haut.

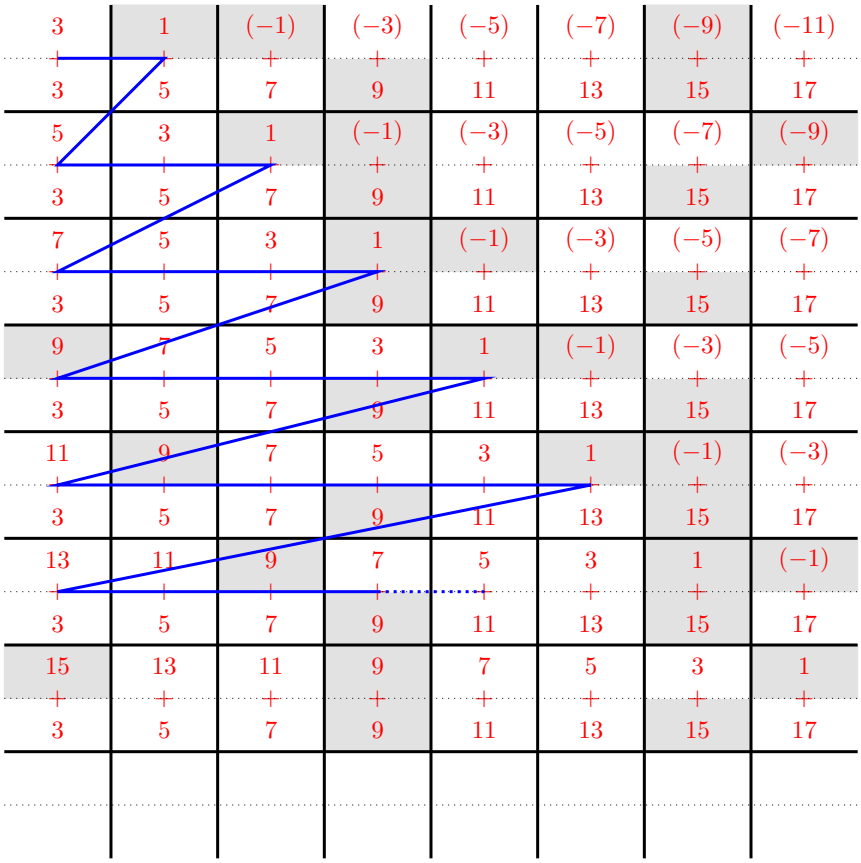
Si l'on oublie les nombres codés, on note que le pavage ne doit respecter que deux contraintes : les rectangles parties hautes des tuiles (codant toutes un même nombre) doivent coïncider (i.e. être de la même couleur) le long de diagonales descendantes tandis que les rectangles parties basses des tuiles (codant toutes un même nombre) doivent coïncider (i.e. être de la même couleur) verticalement.

3	1	(-1)	(-3)	(-5)	(-7)	(-9)	(-11)
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
5	3	1	(-1)	(-3)	(-5)	(-7)	(-9)
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
7	5	3	1	(-1)	(-3)	(-5)	(-7)
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
9	7	5	3	1	(-1)	(-3)	(-5)
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
11	9	7	5	3	1	(-1)	(-3)
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
13	11	9	7	5	3	1	(-1)
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
15	13	11	9	7	5	3	1
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
17	15	13	11	9	7	5	3
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
19	17	15	13	11	9	7	5
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17
21	19	17	15	13	11	9	7
+	+	+	+	+	+	+	+
3	5	7	9	11	13	15	17

On cherche à transformer ce pavage en un pavage de Penrose à base de triangles. On va pour cela associer au pavage une chaîne de booléens. Ensuite, on associera à cette chaîne de booléens un pavage de Penrose en appliquant l'opération inverse de celle fournie par Grünbaum et Shephard dans *Tilings and patterns* [3] : dans ce cadre, la chaîne de booléens associée à une petite tuile code la forme des tuiles qui la contiennent lors des modifications successives du pavage qui rendent les tuiles du pavage de plus en plus grosses.

Le codage du pavage qu'on a proposé par une chaîne de booléens s'effectuera en ayant à l'esprit celui de la diagonale de Cantor : on fait par exemple le choix arbitraire de ne s'intéresser qu'à la partie du pavage

dont les 2 sommants sont positifs, dont on parcourt les éléments dans l'ordre indiqué par la ligne brisée bleue. Pour chaque tuile carrée, on code d'abord le premier sommant (rectangle inférieur) puis le second sommant (rectangle supérieur) par un 0 s'il est blanc et par un 1 s'il est gris.



On obtient la suite de booléens suivante :

$$0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0, 1, \ldots$$

à mettre en regard de la suite de nombres :

$$3, 3, 5, 1, 3, 5, 5, 3, 7, 1, 3, 7, 5, 5, 7, 3, 9, 1, 9, 3, 9, \ldots$$

Nota : on aurait pu au lieu de ce choix parcourir les décompositions selon une spirale "à la Ulam", à partir de la décomposition $1 + (-1)$ par exemple.

Comment maintenant "repartir en arrière" de la chaîne de booléens trouvée à une portion d'un pavage de Penrose ?

On rappelle comment une chaîne de booléens est associée à une petite tuile du pavage initial : cette chaîne exprime la manière dont la petite tuile est progressivement "absorbée" dans des tuiles de plus en plus grosses.

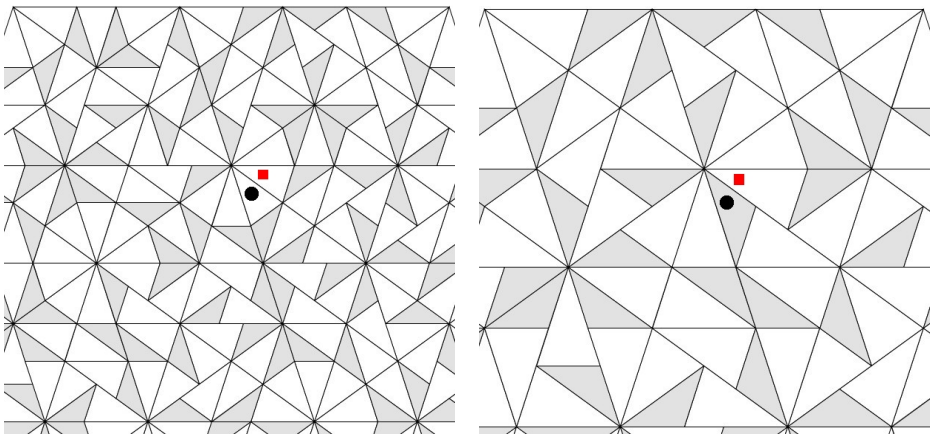
Un pavage de Penrose à base de triangles est constitué de deux sortes de tuiles : les grosses tuiles (de la forme du chapeau du clown blanc, triangles isocèles à deux grands côtés et un petit côté) et les petites tuiles (de la forme d'un chapeau chinois, triangles isocèles à deux petits côtés et un grand côté). Chaque triangle a deux sommets d'une couleur et un sommet d'une autre, une flèche oriente l'arc entre deux sommets de même couleur d'une tuile. Deux tuiles peuvent être accolées si leur arête commune a ses deux sommets de la même couleur dans les 2 tuiles ainsi que la même orientation.

On peut transformer un pavage en faisant grossir ses pièces. Pour cela, on applique successivement et alternativement 2 transformations :

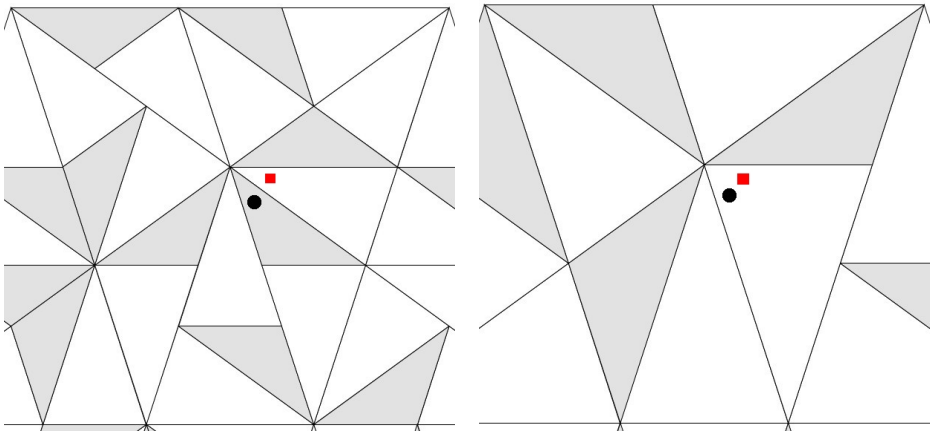
– l'une consiste à effacer toutes les arêtes courtes du pavage qui relient deux sommets qui sont de la même couleur ;

– l'autre consiste à effacer toutes les arêtes courtes du pavage qui relient des sommets de couleur différente.

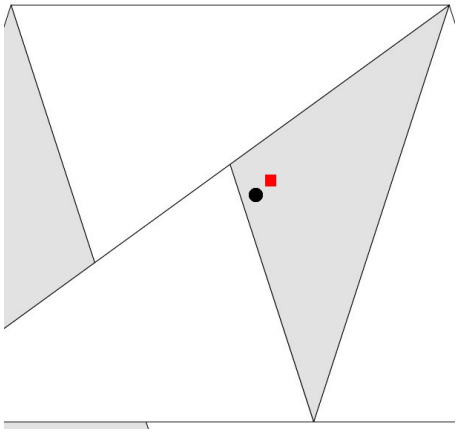
On associe une séquence de booléens à l'une des petites tuiles initiales du pavage en regardant la forme des pièces dans lesquelles elle se retrouve au fur et à mesure que sont effectuées les deux transformations du pavage explicitées ci-dessus : un booléen 1 à la position n de la séquence code que la pièce est dans un gros triangle (de la taille courante) au bout de n transformations tandis qu'un booléen 0 code que la pièce est dans un petit triangle (de la taille courante).



(1) (2)



(3) (4)



(5)

On a utilisé pour dessiner les figures ci-dessus le codage en Tikz du pavage de Penrose fourni par Paul Gaborit, que l'on remercie, dans cette page : http://www.texample.net/tikz/examples/penrose-tiling/.

La séquence de booléens associé à la forme marquée d'un petit disque noir est 10010 car cette pièce se trouve dans une petite pièce à la première étape, dans une grosse pièce aux seconde et troisième étape, dans une petite pièce à la quatrième étape et dans une grosse pièce à la cinquième étape.

La séquence de booléens associé à la forme marquée d'un petit carré rouge est 11110 car cette pièce se trouve dans une petite pièce aux quatre premières étapes et dans une grosse pièce à la cinquième étape.

Il est difficile de dessiner un pavage de Penrose tel que la séquence de booléens qu'on a identifiée par notre sorte de numérotation des pièces "à la Cantor" serait exactement associée à l'une de ses pièces mais cela doit être théoriquement envisageable.

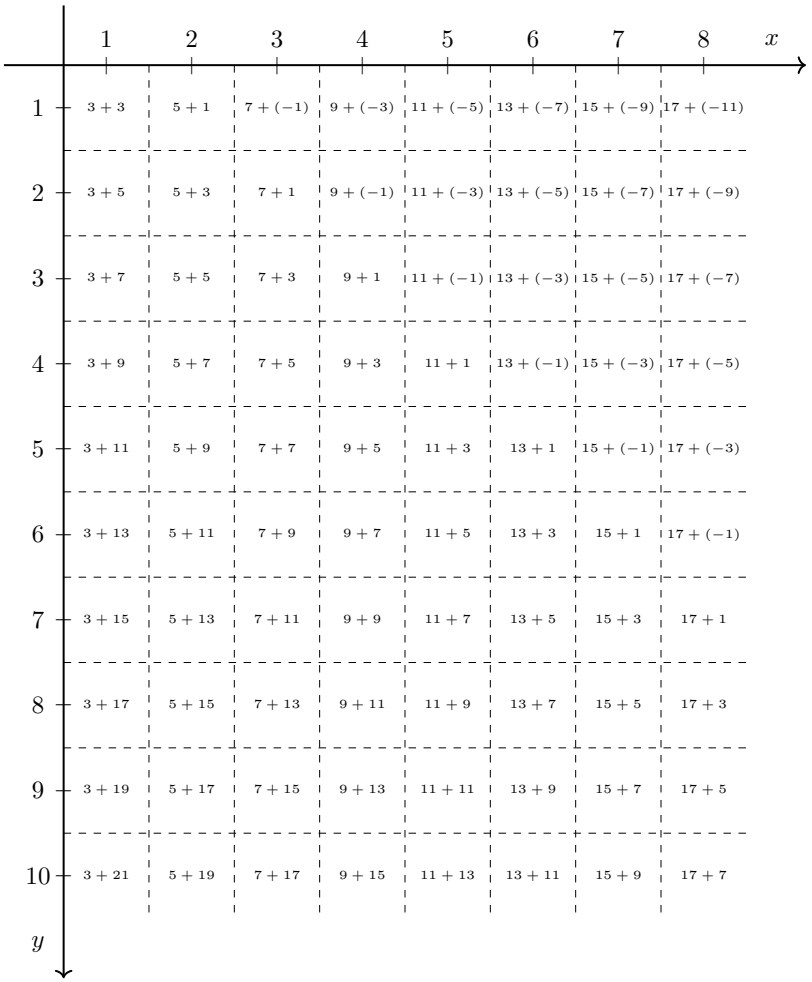
Bibliographie

[2] A. Connes, *Géométrie non-commutative*, Dunod, 1990.

[3] B. Grünbaum, G.C. Shephard, *Tilings and patterns*, Freeman and company, New York, 1987.

Les points de l'espace Goldbach commutent-ils ? (Denise Vella-Chemla, 5.6.2017)

On rappelle l'espace qu'on a choisi pour étudier la conjecture de Goldbach. On met en regard de cet espace deux axes de coordonnées cartésiennes habituels si ce n'est que les ordonnées croissent vers le bas.



La fonction suivante d permet de trouver la somme $s1 + s2$ associée à tel ou tel point du plan ($s1$ pour premier sommant et $s2$ pour second sommant).

$$d : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 2x+1 \\ 2y-2x+3 \end{pmatrix}$$

On la représente par la matrice 3×3 : $M : \begin{pmatrix} 2 & 0 & 1 \\ -2 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ qui permet d'associer au sommet du plan de coordonnées (x, y) représenté par le triplet $\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$ la somme $(2x + 1) + (2y - 2x + 3)$.

On peut étudier comment inverser les sommants de la somme $s1 + s2$ pour obtenir la somme $s2 + s1$. On représente cette opération par la matrice 3×3 : $N : \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Deux façons de procéder sont envisageables :

- on a un point du plan euclidien de coordonnées (x, y), on trouve la somme associée à ce point en appliquant l'opérateur M, on inverse les sommants en appliquant N, on applique l'opérateur M^{-1} inverse de M pour trouver les coordonnées du nouveau point ;

- on applique directement aux coordonnées du point auquel est associée la somme $s1+s2$ un opérateur qui permet de trouver les coordonnées du point correspondant à la somme inversée $s2+s1$ et qui est P : $\begin{pmatrix} -1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

  Cet opérateur correspond à une transformation affine dite *symétrie oblique* par rapport à une droite de pente -2 qui passe par les sommes triviales de la forme $x+x$ (correspondant aux décompositions triviales de Goldbach). Un point et son image ont même ordonnée par cette symétrie oblique.

On vérifie qu'on a bien $M^{-1}NM = P$.

$$\begin{pmatrix} 1/2 & 0 & -1/2 \\ 1/2 & 1/2 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 & 1 \\ -2 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Deux éléments font de notre espace Goldbach un espace non-commutatif :

- d'une part, le fait que les opérateurs identifiés ci-dessus ne commutent pas. Par exemple,

  $$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 0 & 1 \\ -2 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} -2 & 2 & 3 \\ 2 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

  tandis que

  $$\begin{pmatrix} 2 & 0 & 1 \\ -2 & 2 & 3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 1 \\ 2 & -2 & 3 \\ 0 & 0 & 1 \end{pmatrix} \quad ;$$

- d'autre part, on distingue la somme $s1+s2$ de la somme $s2+s1$, l'ordre des sommants étant très important pour les comptages, une décomposition de Goldbach de la forme $premier + composé$ n'étant pas comptabilisée par la même variable qu'une décomposition de la forme $composé + premier$.

Refaire ses gammes (Denise Vella-Chemla, 7.6.2017)

On va étudier les fréquences des notes de la gamme, suite au visionnage de la petite video Science étonnante #41 intitulée *Les mathématiques de la musique* qui se trouve ici https://www.youtube.com/watch?v=cTYvCpLRwao.

David Louapre explique dans cette video pourquoi il y a 12 notes dans la gamme chromatique et pourquoi certaines notes s'accordent bien (les écouter jouées ensemble est agréable à l'oreille).

On retiendra en résumant que la raison essentielle à cela est que $2^{19} = 524288 \simeq 3^{12} = 531441$ et qu'il s'agit d'écarter les notes entre elles en "mettant en face" 12 facteurs 2 ou 4 et 12 facteurs 3, ce qu'on fait en utilisant pour passer d'une note à la suivante immédiate les fractions rationnelles $\left\{\frac{3}{2}, \frac{3}{4}, \frac{3}{4}, \frac{3}{2}, \frac{3}{4}, \frac{3}{2}, \frac{3}{4}, \frac{3}{4}, \frac{3}{2}, \frac{3}{4}, \frac{3}{4}, \frac{3}{2}\right\}$ en partant initialement d'une note *La*.

L'ensemble des dénominateurs comprend 19 facteurs 2, et l'ensemble des numérateurs comprend 12 facteurs 3 et les fractions rationnelles $\frac{3}{2}$ sont équitablement réparties au sein de l'ensemble des fractions $\frac{3}{4}$ plus nombreuses.

Le tableau ci-dessous est celui fourni dans la video : on passe d'une note (de sa fréquence) à celle de la note à sa droite en "passant à la quinte", en multipliant la fréquence par $\frac{3}{2}$ ou par $\frac{3}{4}$ (on a mis le multiplicateur qui permet de passer des nombres d'une colonne à ceux de la suivante en bas de cette colonne) ; on passe d'une note à celle au-dessous dans la même colonne en "passant à l'octave" (en multipliant la fréquence par 2).

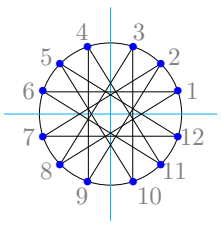
La	*Mi*	*Si*	*Fa#*	*Do#*	*Sol#*	*Ré#*	*La#*	*Fa*	*Do*	*Sol*	*Ré*	~~*La*~~
55	83	62	46	70	52	78	59	44	66	50	37	~~56~~
110	165	124	93	139	104	157	117	88	132	99	74	~~112~~
220	330	248	186	278	209	313	235	176	264	198	149	~~223~~
440	660	495	371	557	418	626	470	352	529	396	297	~~446~~
880	1320	990	743	1114	835	1253	940	705	1057	793	595	~~892~~
1760	2640	1980	1485	2228	1671	2506	1879	1410	2114	1586	1189	~~1784~~
3520	5280	3960	2970	4455	3341	5012	3759	2819	4229	3172	2379	~~3568~~
$\times\frac{3}{2}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{2}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{2}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{2}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{2}\nearrow$	
8	3	10	5	12	7	2	9	4	11	6	1	

Permutons maintenant les colonnes de ce tableau de façon à remettre les notes dans l'ordre habituel d'une gamme ascendante. On passe cette fois-ci de chaque fréquence à la suivante selon l'ordre habituel de lecture (de gauche à droite et de haut en bas) en multipliant cette fréquence par $\sqrt[12]{2} \simeq 1.059463\ldots$.

1	2	3	4	5	6	7	8	9	10	11	12	
Ré	*Ré#*	*Mi*	*Fa*	*Fa#*	*Sol*	*Sol#*	*La*	*La#*	*Si*	*Do*	*Do#*	
74	78	83	88	93	99	104	110	117	124	132	139	+4→+7
149	157	165	176	186	198	209	220	235	248	264	278	+8→+14
297	313	330	352	371	396	418	440	470	495	529	557	+16→+28
595	626	660	705	743	793	835	880	940	990	1057	1114	+31→+57
1189	1253	1320	1410	1485	1586	1671	1760	1879	1980	2114	2228	+64→+114
2379	2506	2640	2819	2970	3172	3341	3520	3759	3960	4229	4455	+127→+226
4758	5012	5280	5638	5940	6344	6682	7040	7518	7920	8458	8910	+254→+452

On peut calculer approximativement par ligne les additions à effectuer pour passer d'une note à la suivante. On les a notées en fin de lignes en gris, de la plus petite somme à effectuer à la plus grande.

On peut enfin en ayant numéroté les colonnes de 1 à 12, noter ces nombres sur un cercle pour bien montrer la cyclicité et relier les notes successives par "passage à la quinte" (on a reporté ces nombres dans la dernière ligne du premier tableau également). Du fait de la cyclicité, ce dessin possède de multiples symétries.



Ce qu'il semble intéressant de faire, c'est de prolonger notre tableau de fréquences vers le domaine de l'inaudible, en réappliquant vers le haut du tableau les divisions par 2 des nombres des colonnes : moyennant le passage du discret au continu, on a un rapprochement des valeurs qu'il faut garder à l'esprit, en se rappelant cependant que toutes les fréquences fournies dans les 2 tableaux sont des valeurs entières arrondies les plus proches de réels.

Ré	*Ré#*	*Mi*	*Fa*	*Fa#*	*Sol*	*Sol#*	*La*	*La#*	*Si*	*Do*	*Do#*
1	1	1	1	1	2	2	2	2	2	2	2
2	2	3	3	3	3	3	3	4	4	4	4
5	5	5	6	6	6	7	7	7	8	8	9
9	10	10	11	12	12	13	14	15	16	17	18
19	20	21	22	23	25	26	28	29	31	33	35
37	39	42	44	47	50	52	55	59	62	66	70
74	78	83	88	93	99	104	110	117	124	132	139

On pourrait de la même manière fabriquer une gamme à 3 notes : on utilise le fait que $2^7 = 128 \simeq 5^3 = 125$. On doit mettre 7 facteurs 2 en face de 3 facteurs 5. On utilise les 3 fractions rationnelles $\left\{\frac{5}{4}, \frac{5}{8}, \frac{5}{4}\right\}$.

Admettons qu'on parte du nombre 500. Multiplié par $\frac{5}{4}$, on obtient 625, qu'on multiplie par $\frac{5}{8}$ pour obtenir 391, qu'on multiplie quant à lui par $\frac{5}{4}$ pour obtenir 489. On est quasiment revenu au chiffre initial 500.

On remet les nombres dans l'ordre $391 \to 489 \to 500 \to 625$. On doit passer de l'un à l'autre par multiplication par $\sqrt[3]{2} \simeq 1.025992\ldots$ (la suite obtenue est $391, 493, 621$. Il manque un nombre de la séquence, le 500 qui a disparu...?).

On a également $7^5 \simeq 2^{14} \simeq 11^4$ et $13^4 \simeq 2^{15}$ mais les écarts sont de plus en plus grands : $2^{14} = 16384$, $7^5 = 16807$, $11^4 = 14641$ d'une part, et $2^{15} = 32768$ et $13^4 = 28561$ d'autre part, "presque" égaux.

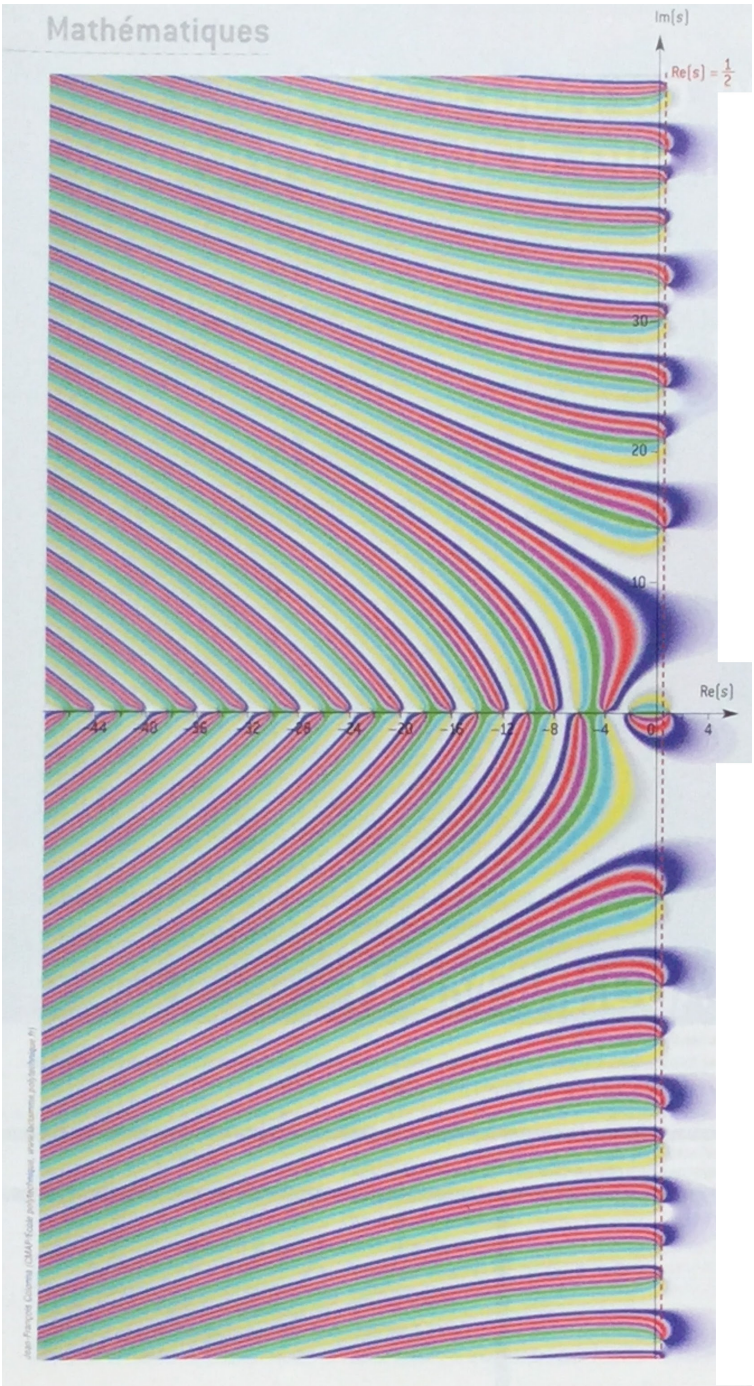
$\sqrt[4]{2} \simeq 1.18921\ldots$
$\sqrt[14]{11} \simeq 1.18682\ldots$
$\sqrt[15]{13} \simeq 1.18649\ldots$

$\sqrt[5]{2} \simeq 1.1487\ldots$
$\sqrt[14]{7} \simeq 1.14912\ldots$

Arc tangente (Denise Vella-Chemla, 18.6.2017)

On essaie, lentement, de se familiariser avec les images représentant la fonction zêta de Riemann dans le plan complexe. En particulier, il y a deux images : l'une en couleur, l'autre bicolore de forme spirale.

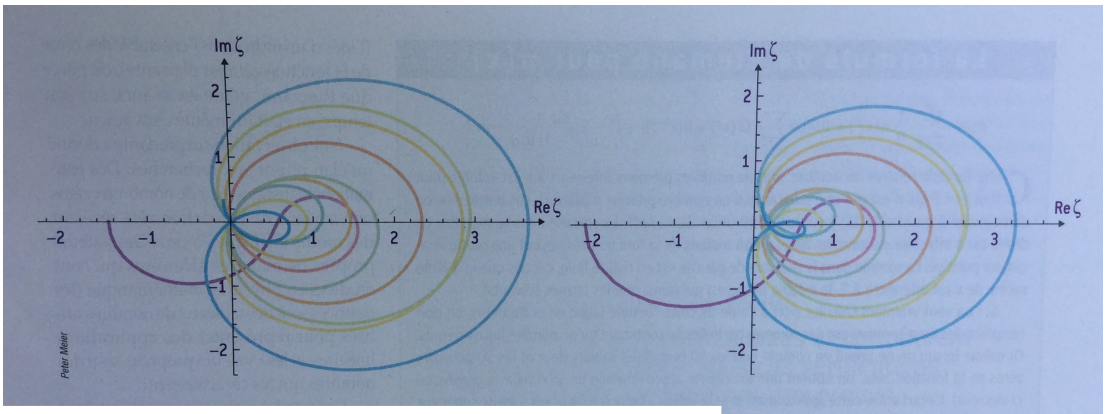
La représentation colorée de la fonction zêta permet de représenter pour chaque point antécédent complexe $a + ib$ à 2 coordonnées (a, b) une image complexe à deux coordonnées également $a' + ib'$. Comme on ne peut le faire, le $a' + ib'$ est représenté par une couleur que l'on obtient dans un disque palette, l'angle de parcours de ce disque (la coordonnée angulaire) permettant de passer subtilement d'une couleur à l'autre et la distance au centre du disque (coordonnée radiale) fournissant l'intensité de la couleur utilisée[1].



Il est très bien expliqué dans un article du magazine Pour la Science (n°377, mars 2009) de Peter Meier et

[1] cf https://en.wikipedia.org/wiki/Hue

Jörn Steuding que si l'on parcourt verticalement une droite dans la représentation colorée, on se promène en quelque sorte sur une spirale du plan complexe qui peut passer périodiquement par le point origine (zéro) ou bien ne jamais y passer (la spirale est alors décalée vers la droite).



4. LES VALEURS DE LA FONCTION ZÊTA $\zeta(s)$ sont ici représentées pour $s = 1/2 + it$ *(à gauche)* et $s = 5/8 + it$ *(à droite)*, dans le domaine $0 \leq t \leq 50$. Quand la partie réelle de s est égale à 1/2, la courbe traverse plusieurs fois le point $\zeta = 0$; ce sont les zéros de la fonction zêta. En dehors de la droite critique $\mathrm{Re}(s) = 1/2$, de tels passages par le point $\zeta = 0$ ne se produisent pas dans ce domaine – conformément à l'hypothèse de Riemann.

Ceci étudié, on a l'idée de calculer par la fonction arc-tangente l'angle associé aux zéros de la fonction zêta de Riemann.

Les valeurs des parties imaginaires des zéros sont trouvables sur la toile.
Par exemple, ici : http://lmfdb.org/zeros/zeta/?limit=100000N=1.

On utilise pour calculer les arcs-tangentes pour les zéros de zêta le programme ci-dessous : le côté opposé de l'angle est la partie imaginaire du zéro, le côté adjacent vaut $\frac{1}{2}$, il s'agit donc de calculer l'arc tangente de $2.\Im(z)$ pour z parcourant les valeurs du fichier.

```
#include <iostream>
#include <stdio.h>
#include <cmath>
#include <fstream>

int main (int argc, char* argv[])
{ int i, np ;
  float zeros[100005] ;

  std::ifstream fichier("leszeros", std::ios::in);
  if (fichier)
    {
      int entier1 ;
      float entier2 ;

      while (not fichier.eof()) {
        fichier >> entier1 >> entier2 ;
        zeros[entier1] = entier2 ;
      }
      fichier.close();
    }
  else std::cerr << "Impossible d'ouvrir le fichier !" << std::endl ;
  for (i = 1 ; i <= 100000 ; ++i) std::cout << i << " -> " << atan(2.0*zeros[i]) << "\n" ;
}
```

On trouve sur la toile ici https://fr.wikipedia.org/wiki/Formule_de_Machin quatre égalités surprenantes concernant certaines valeurs de la fonction arc-tangente :

$$\frac{\pi}{4} = 4arctan\frac{1}{5} - arctan\frac{1}{239} \qquad \text{(découverte par Machin en 1706)}$$

$$\frac{\pi}{4} = arctan\frac{1}{2} + arctan\frac{1}{3} \qquad \text{(découverte par Euler en 1706)}$$

$$\frac{\pi}{4} = 2arctan\frac{1}{2} - arctan\frac{1}{7} \qquad \text{(découverte par Herman en 1706)}$$

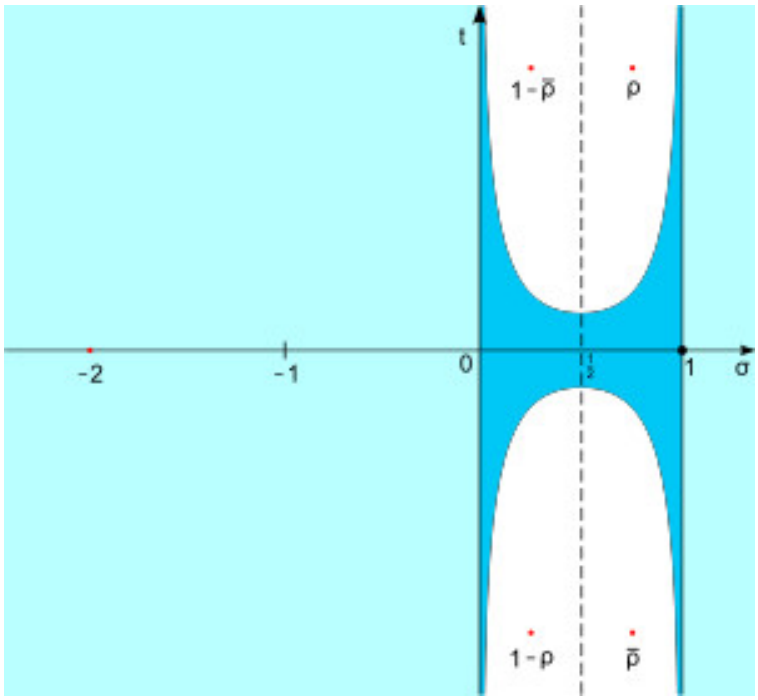
$$\frac{\pi}{4} = 2arctan\frac{1}{3} + arctan\frac{1}{7} \qquad \text{(découverte par Hutton en 1776).}$$

Pour 100000 zéros, à partir de la partie imaginaire du $55204^{ème}$ zéro, on atteint la valeur 1.57079 sur laquelle le programme se stabilise. En effet, la limite de la fonction $arctan(x)$ est $\frac{\pi}{2}$ en $+\infty$.

Si on considère que les couples de "couleurs complémentaires" sont (bleu, blanc), (rouge, jaune), (turquoise, violet) et (vert, vert), on constate une symétrie colorée entre points correspondant à des nombres complexes conjugués (qui doit peut-être correspondre au fait que l'image du conjugué d'un complexe est le conjugué de son image (si $\zeta(a+ib) = c+id$ alors $\zeta(a-ib) = c-id$). On notera que, bizarrement, les couleurs de l'arc-en-ciel ne sont pas dans l'ordre quand on "chemine" (par exemple verticalement).

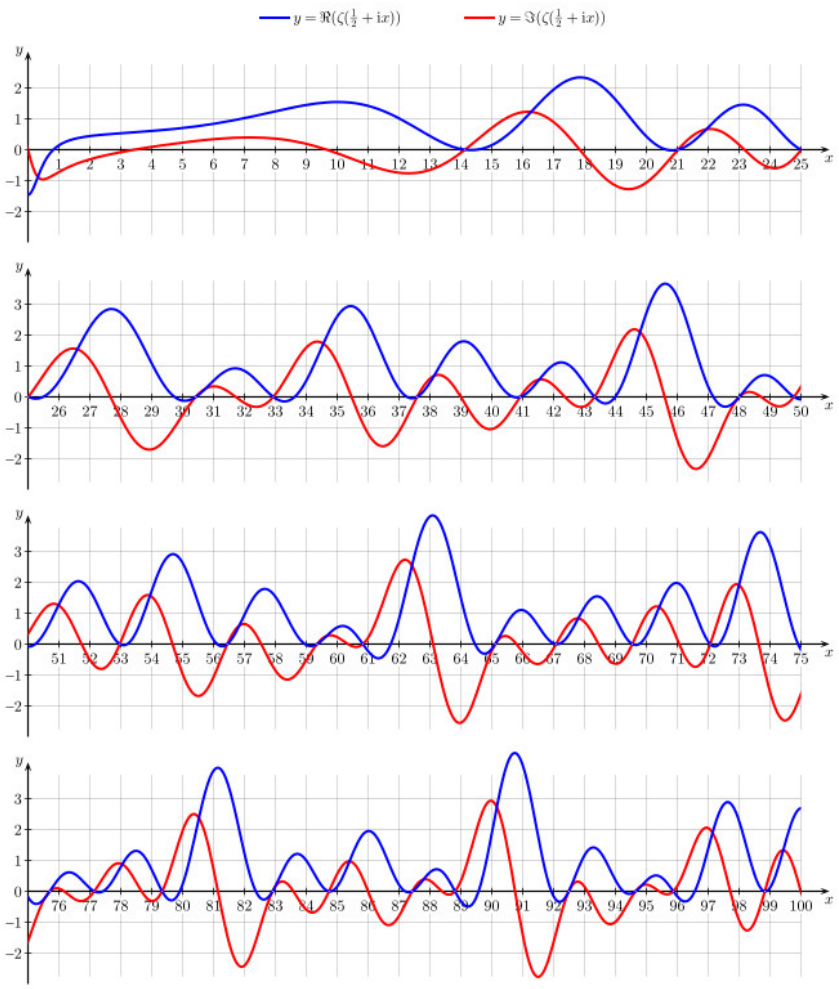
Enfin, deux graphiques à mémoriser, trouvés sur l'article de wikipedia concernant la fonction zêta de Riemann :

- le premier concernant les valeurs symétriques que prend la fonction zêta sur un complexe ρ, son conjugué $\overline{\rho}$, $1-\rho$ et $1-\overline{\rho}$;



  On a $\rho = a+ib, \overline{\rho} = a-ib, 1-\overline{\rho} = (1-a)+ib$ et $1-\rho = 1-(a+ib) = (1-a)-ib = \overline{(1-\overline{\rho})}$;

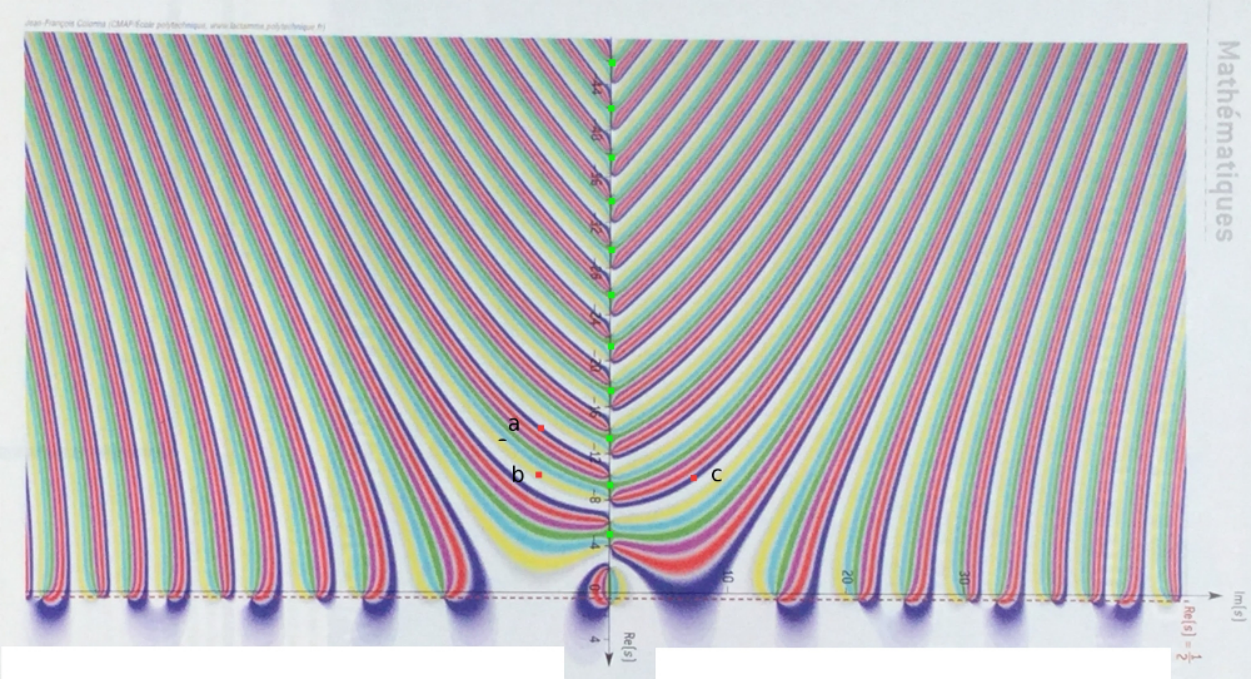
- le second montrant séparément les parties réelles et imaginaires des complexes le long de la droite critique ; la courbe rouge ressemble étrangement à la courbe bleue qu'on aurait décalée vers le bas et la gauche, en l'écrasant à moitié (au dessus de l'axe des abscisses, la courbe rouge semble systématiquement croiser la courbe bleue à la moitié des hauteurs des pics). Il faut aussi trouver un moyen d'aligner horizontalement ses minima.



A la recherche d'une transformation de la représentation graphique colorée de la fonction zêta, on voit qu'il faudrait peut-être considérer plein de petites symétries centrales à appliquer sur des portions du graphique, autour des points marqués de petits carrés verts ci-dessous, avec une inversion des couleurs, que l'on schématise par le passage du point a au point b au point c. Cette transformation s'applique sur l'axe de partie réelle $\dfrac{1}{2}$ pour lequel la symétrie s'effectue par rapport au point origine.

Pour avoir à l'esprit des réels plutôt que des complexes, on définit la fonction z sur $\mathbb{R}$ ainsi : si r est la partie imaginaire d'un nombre complexe annulant zêta,

$$\begin{aligned} z(r) &= 1 + \frac{1}{2^{\frac{1}{2}+ri}} + \frac{1}{3^{\frac{1}{2}+ri}} + \dots \\ &= 1 + \frac{1}{\sqrt{2}(cos(r\ ln\ 2) + i\ sin(r\ ln\ 2))} + \frac{1}{\sqrt{3}(cos(r\ ln\ 3) + i\ sin(r\ ln\ 3))} + \dots \\ &= \sum_{n=1}^{\infty} \frac{cos(r\ ln\ n) - i\ sin(r\ ln\ n)}{\sqrt{n}} \end{aligned}$$



La configuration de la représentation colorée ainsi que les positions des ρ et $1-\overline{\rho}$ autour de la droite critique dans la figure à dominante turquoise plus haut nous amène à la réflexion suivante : admettons qu'on ait deux zéros (puisqu'ils vont par 2) qui "tombent" hors de la droite, par exemple $1/4+ai$ et $3/4+ai$, pour que la fonction ζ s'annule, si ρ est l'angle correspondant à a, les dénominateurs identiques des formules fournies de $z(a)$ pour ces points doivent être nuls (les $\sum_{n=1}^{\infty} cos(\rho\ ln\ n) - i\ sin(\rho\ ln\ n)$ vus plus haut, les dénominateurs valant $\sqrt[4]{n}$ pour le point $1/4+ai$ et $\sqrt[4]{n^3}$ pour le point $3/4+ai$).

Mais alors, en prenant de manière dichotomique un troisième zéro entre les 2 premiers (ou plutôt deux autres zéros plus proches de la droite autour d'elle), on peut restreindre l'intervalle sur lequel l'annulation est forcée d'avoir lieu. On réitère le procédé de fois en fois de façon dichotomique et on voit alors la droite critique comme la limite sur laquelle les zéros doivent fatalement se trouver, les points extrémités de l'intervalle ayant pour partie réelle des $\frac{1}{2}+\varepsilon$ et $\frac{1}{2}-\varepsilon$, avec ε qui tend vers zéro. Ce raisonnement fait penser à une descente infinie de Fermat mais contrairement à elle, il ne permet pas d'aboutir à une contradiction car la descente infinie a lieu sur des réels et non sur des entiers.

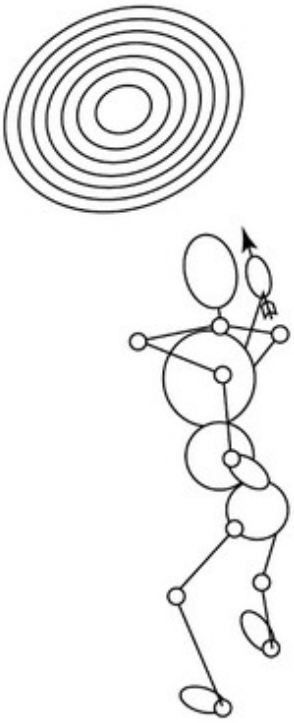
Ci-dessous, deux illustrations :

- la photo est la propriété de Jean-François Dars ; on peut la regarder à cette adresse : http://www.savoirs.essonne.fr/sections/ressources/photos/photo/michael-atiyah-et-alain-connes/ ainsi que dans le livre Les déchiffreurs [3] ; le geste des doigts illustre bien l'idée d'élément infinitésimal de distance ;
- la seconde illustration peut être trouvée dans des articles (dont on fournit les références en bibliographie) dans lesquels Alain Connes fournit sa vision des infinitésimaux.

On peut relier, de loin, cette idée de droite-critique-limite au paradoxe de Zénon d'une part (les zéros s'en approcheraient infiniment mais on n'arriverait pas à prouver qu'ils lui appartiennent) ; cela nous fait également penser à une anecdote vécue en enseignant à des élèves de niveau élémentaire : on peut jouer avec eux à "devine mon nombre", dès que sont abordés les décimaux, et ils comprennent vite grâce à ce jeu qu'entre deux nombres, on peut toujours en intercaler un troisième. Pour des élèves petits, il n'y a pas de nombre entre 4 et 5, dans la mesure où ils ont en tête la suite numérique ; plus tard, entre 13,4 et 13,5, transposant leur raisonnement initial, certains pensent qu'il n'y a pas de nombre non plus. Le jeu consiste pour les élèves à poser à l'enseignant des questions fermées : "le nombre est-il plus grand (ou plus petit) que tant ?" pour tenter de deviner le nombre que l'enseignante a choisi. Le fait pour l'enseignant

de “tricher” en ajoutant des décimales leur fait petit à petit comprendre que de même que la suite des nombres est infinie, entre 2 nombres, il y a une infinité de nombres.

You play a game of throwing darts at some target called Ω



and the question which is asked is: what is the probability $dp(x)$ that actually when you throw the dart it lands exactly at a given point $x \in \Omega$?

Bibliographie

[1] Noncommutative geometry and reality, Journal of mathematical physics, 36, p.6194, (1995).

[2] Visions in mathematics : GAFA (Geometrical Functional Analysis) 2000, Special Volume, part II, p.506, edité par Noga Alon, Jean Bourgain, Alain Connes, Mikhaïl Gromov, Vitali D. Milman.

[3] Les déchiffreurs, voyage en mathématiques, Jean-François Dars, Annick Lesne, Anne Papillault, Belin, 2008.

Très constante (Denise Vella-Chemla, 21.6.2017)

On continue de procéder expérimentalement, dans l'étude des parties imaginaires des zéros de la fonction zêta.

Il y a quelques temps, on avait eu l'idée de calculer les carrés des parties imaginaires et les nombres obtenus rappelaient les fréquences des notes de la gamme chromatique (cf. photo d'un petit carnet en annexe).

Ici, on effectue des calculs qui rapetissent les nombres réels parties imaginaires des zéros de zêta, en prenant par exemple leurs racines carrées, leurs racines cubiques, etc.

On utilise le programme suivant.

```
#include <iostream>
#include <stdio.h>
#include <cmath>
#include <fstream>

int main (int argc, char* argv[])
{
  const float PI = 3.14159265359 ;
  const float CONSTNEPER = 2.718281828459 ;
  const float BRUNJUM = 1,9021605823 ;
  const float RACTROIS = 1,7320508075 ;
  const float NBDOR = 1,6180339887 ;
  const float RACDEUX = 1,41421356237 ;
  const float ASYMPTOINDICEULER = 1.9435964368 ;

  int i, np, tranche ;
  float zeros[100005] ;
  int pe[100005] ;

  std::ifstream fichier("leszeros", std::ios::in);
  if (fichier) { int entier1 ; float entier2 ;
     while (not fichier.eof()) {
       fichier >> entier1 >> entier2 ;
       zeros[entier1] = entier2 ;
     }
     fichier.close();
  }
  else std::cerr << "Impossible d'ouvrir le fichier !" << std::endl ;

  for (i = 1 ; i <= 10000 ; ++i) {
    std::cout << i << " -> " << pow(zeros[i],1./CONSTGAUSS) << "\n" ;
    pe[i] = (int) pow(zeros[i],1./CONSTGAUSS) ;
  }
  for (i = 2 ; i <= 10000 ; ++i) {
    if (pe[i] == pe[i-1]) tranche = tranche+1 ;
    else { std::cout << tranche+1 << " " ; tranche = 0 ;}
  }
}
```

Pour les racines carrées, on remplace le $pow(zeros[i], 1./CONSTGAUSS)$ par $pow(zeros[i], 1./2)$. Pour les racines cubiques, on le remplace par $pow(zeros[i], 1./3)$. Pour les racines $\pi - ième$, on le remplace par $pow(zeros[i], 1./CONSTPI)$, etc.

Pour les racines carrées ou cubiques, on obtient les résultats que voici (on fournit les 100 premières racines

carrées de parties imaginaires des zéros de zêta) :

$1 \to 3.75962$	$26 \to 9.61727$	$51 \to 12.0831$	$76 \to 13.8953$
$2 \to 4.58498$	$27 \to 9.72889$	$52 \to 12.1418$	$77 \to 13.9737$
$3 \to 5.00109$	$28 \to 9.79136$	$53 \to 12.2496$	$78 \to 14.0313$
$4 \to 5.51587$	$29 \to 9.94139$	$54 \to 12.2852$	$79 \to 14.0718$
$5 \to 5.73891$	$30 \to 10.0657$	$55 \to 12.3703$	$80 \to 14.1868$
$6 \to 6.13076$	$31 \to 10.1846$	$56 \to 12.4945$	$81 \to 14.2300$
$7 \to 6.39677$	$32 \to 10.2687$	$57 \to 12.5538$	$82 \to 14.2895$
$8 \to 6.58233$	$33 \to 10.3522$	$58 \to 12.6036$	$83 \to 14.3316$
$9 \to 6.92857$	$34 \to 10.5371$	$59 \to 12.6960$	$84 \to 14.4190$
$10 \to 7.05506$	$35 \to 10.5771$	$60 \to 12.7683$	$85 \to 14.4768$
$11 \to 7.27807$	$36 \to 10.6921$	$61 \to 12.8661$	$86 \to 14.5496$
$12 \to 7.51307$	$37 \to 10.7808$	$62 \to 12.9300$	$87 \to 14.6064$
$13 \to 7.70370$	$38 \to 10.8991$	$63 \to 13.0036$	$88 \to 14.6474$
$14 \to 7.79947$	$39 \to 11.0168$	$64 \to 13.0350$	$89 \to 14.7027$
$15 \to 8.06923$	$40 \to 11.0881$	$65 \to 13.1686$	$90 \to 14.8009$
$16 \to 8.19023$	$41 \to 11.1471$	$66 \to 13.2195$	$91 \to 14.8565$
$17 \to 8.33945$	$42 \to 11.2923$	$67 \to 13.2831$	$92 \to 14.8805$
$18 \to 8.48924$	$43 \to 11.3833$	$68 \to 13.3558$	$93 \to 14.9669$
$19 \to 8.70084$	$44 \to 11.4494$	$69 \to 13.4133$	$94 \to 14.9994$
$20 \to 8.78321$	$45 \to 11.5541$	$70 \to 13.4984$	$95 \to 15.0805$
$21 \to 8.90715$	$46 \to 11.6085$	$71 \to 13.5969$	$96 \to 15.1439$
$22 \to 9.10551$	$47 \to 11.7523$	$72 \to 13.6235$	$97 \to 15.2069$
$23 \to 9.20519$	$48 \to 11.8210$	$73 \to 13.6832$	$98 \to 15.2311$
$24 \to 9.35015$	$49 \to 11.8795$	$74 \to 13.7629$	$99 \to 15.2870$
$25 \to 9.42386$	$50 \to 11.9629$	$75 \to 13.8574$	$100 \to 15.3793$

On décide de tronquer[1] les parties décimales en prenant systématiquement la partie entière des nombres. Un certain nombre de valeurs successives des images des parties imaginaires des zéros sont de ce fait égalisées. On a alors des “paquets” d’images successives identiques dont on compte les cardinaux. Les cardinaux trouvés par ces processus ne sont pas très satisfaisants, on préfèrerait trouver comme cardinaux des ensembles successifs de valeurs la suite des nombres entiers successifs (par une sorte de principe dit “de la vache qui rit”).

Voici les cardinaux des paquets pour les images fournies dans le tableau précédent.

1	1	3	4	5	7	8	9	12	12	15	17	17	20	22	23	26	27
30	31	34	35	37	41	41	44	47	48	51	53	55	57	61	62	64	68
69	72	74	77	79	81	84	86	89	92	94	97	99	101	105	107	108	112
115	118	119	123	125	129	130	133	137	138	142	144	147	149	154	155	158	161
163	167	169	173	174	178	181	183	187	189	192	195	197	202	203	207	210	212
215	219	221	224	227	231												

[1] Peut-être qu’approximer plutôt que tronquer serait plus judicieux.

Avec les racines cubiques des zêta plutôt que les racines carrées, voici les résultats obtenus :

$1 \to 2.41785$	$26 \to 4.52239$	$51 \to 5.26565$	$76 \to 5.77979$
$2 \to 2.75989$	$27 \to 4.55731$	$52 \to 5.28269$	$77 \to 5.80152$
$3 \to 2.92444$	$28 \to 4.57680$	$53 \to 5.31392$	$78 \to 5.81743$
$4 \to 3.12183$	$29 \to 4.62343$	$54 \to 5.32420$	$79 \to 5.82863$
$5 \to 3.20543$	$30 \to 4.66189$	$55 \to 5.34877$	$80 \to 5.86034$
$6 \to 3.34973$	$31 \to 4.69853$	$56 \to 5.38451$	$81 \to 5.87224$
$7 \to 3.44594$	$32 \to 4.72437$	$57 \to 5.40153$	$82 \to 5.88859$
$8 \to 3.51226$	$33 \to 4.74995$	$58 \to 5.41580$	$83 \to 5.90015$
$9 \to 3.63437$	$34 \to 4.80632$	$59 \to 5.44225$	$84 \to 5.92410$
$10 \to 3.67847$	$35 \to 4.81849$	$60 \to 5.46290$	$85 \to 5.93992$
$11 \to 3.75558$	$36 \to 4.85334$	$61 \to 5.49075$	$86 \to 5.95983$
$12 \to 3.8360$	$37 \to 4.88017$	$62 \to 5.50890$	$87 \to 5.97534$
$13 \to 3.90061$	$38 \to 4.91580$	$63 \to 5.52981$	$88 \to 5.98652$
$14 \to 3.93288$	$39 \to 4.95113$	$64 \to 5.53870$	$89 \to 6.00157$
$15 \to 4.02304$	$40 \to 4.97247$	$65 \to 5.57647$	$90 \to 6.02827$
$16 \to 4.06316$	$41 \to 4.99007$	$66 \to 5.59082$	$91 \to 6.04334$
$17 \to 4.11236$	$42 \to 5.03333$	$67 \to 5.60876$	$92 \to 6.04987$
$18 \to 4.16146$	$43 \to 5.06032$	$68 \to 5.62920$	$93 \to 6.07324$
$19 \to 4.23033$	$44 \to 5.07989$	$69 \to 5.64534$	$94 \to 6.08205$
$20 \to 4.25699$	$45 \to 5.11083$	$70 \to 5.66920$	$95 \to 6.10394$
$21 \to 4.29694$	$46 \to 5.12684$	$71 \to 5.69673$	$96 \to 6.12104$
$22 \to 4.36050$	$47 \to 5.16910$	$72 \to 5.70416$	$97 \to 6.13801$
$23 \to 4.39226$	$48 \to 5.18923$	$73 \to 5.72081$	$98 \to 6.14452$
$24 \to 4.43826$	$49 \to 5.20635$	$74 \to 5.74300$	$99 \to 6.15955$
$25 \to 4.46155$	$50 \to 5.23068$	$75 \to 5.76927$	$100 \to 6.18432$

3 11 27 47 77 113 159 212 275 346 429 521 620 733 855 987 1131 1284 1450

Du coup, on décide d'utiliser des racines "i-ième", avec i prenant successivement les valeurs π, $\sqrt{2}$, $\sqrt{3}$, $\frac{1+\sqrt{5}}{2}$ (le nombre d'or), 2.718281828459 (la constante de Neper) et $1,9021605823$ la constante des nombres premiers jumeaux. On fournit ci-dessous directement la taille des paquets de parties imaginaires de zéros successifs qui ont même image par la racine $i-ième$ en question.

Ci-dessous, les tailles des paquets de racines $\pi - ièmes$ de parties imaginaires de zéros de zêta successifs égales :

4 16 36 69 112 168 240 325 428 546 681 836 1009 1200 1412 1643

Ci-dessous, les tailles des paquets pour les racines $\sqrt{2} - ièmes$:

0	0	0	1	0	0	0	1	0	1	0	1	1	1	1	2	1	1	2	1
2	1	2	2	2	2	2	2	2	3	2	2	3	3	3	2	3	3	3	3
3	3	4	3	3	3	4	4	3	4	4	3	5	4	4	4	4	4	4	4
5	4	5	4	5	5	4	5	4	6	4	5	5	5	6	5	5	5	6	5
6	6	5	6	5	6	6	6	6	6	5	7	6	6	7	6	6	7	6	7
6	6	7	6	7	7	7	7	7	7	7	6	7	8	7	8	7	6	8	8
7	8	8	7	7	8	8	8	7	8	8	8	8	8	8	8	9	8	8	8
9	8	8	9	9	8	9	8	9	9	8	10	8	9	9	9	9	8	10	10
8	10	9	9	10	10	9	9	10	9	9	10	10	10	9	10	10	10	9	11
10	10	10	10	10	10	10	11	10	10	11	10	10	11	11	10	10	11	11	11
10	11	11	11	11	11	11	11	10	12	11	11	11	11	11	12	12	10	12	11
12	11	13	10	13	11	12	11	12	11	13	11	13	11	12	13	12	11	13	11
13	12	12	13	12	13	11	13	13	12	13	12	13	13	12	13	13	12	13	13
12	14	13	13	12	13	14	13	13	13	13	13	14	13	14	12	14	13	13	14
14	14	13	13	15	13	14	14	13	14	14	14	13	15	14	13	14	14	14	15
14	14	14	15	14	14	14	15	14	15	14	15	15	14	14	15	15	14	15	15
15	14	16	15	14	15	15	15	15	15	15	15	15	15	15	16	15	15	16	15
16	15	16	15	15	16	16	15	15	16	16	16	15	16	16	16	16	16	15	16
16	16	16	16	16	17	16	16	16	16	16	17	16	16	17	17	15	17	17	16
16	17	16	17	17	17	17	16	17	16	18	17	16	17	17	17	17	17	17	17
18	16	18	17	17	17	17	18	18	16	18	17	17	18	17	18	17	18	18	18
17	18	18	17	18	18	17	18	18	18	18	18	18	18	18	19	17	19	18	18
17	19	18	19	18	18	19	18	18	19	18	18	19	19	18	19	18	19	19	18
19	19	18	19	19	19	19	19	18	20	18	20	19	18	19	20	19	19	19	19
20	19	19	20	19	19	20	19	19	20	20	19	20	20	19	20	19	20	19	20
19	20	21	19	20	20	20	20	20	20	20	20	20	20	20	20	20	20	21	20
20	21	20	19	21	21	20	21	20	21	20	21	20	21	20	20	21	21	21	21
20	21	21	21	20	21	21	21	21	21	21	21	21	21	21	20	22	21	21	22
21	21	21	21	22	21	22	21	21	22	21	22	21	22	21	22	21	23	20	22
21	23	22	21	22	22	22	21	22	22	22	22	23	21	22	22	22	23	21	23
22	22	22	22	22	23	22	22	22	24	22	22	22	23	23	22	23	22	22	23
23	22	23	23	22	23	23	22	23	23	23	23	23	23	23	22	24	23	23	23
23	23	23	23	23	24	23	23	23	23	23	25	22	24	23	24	23	23	24	

Dans le tableau précédent ainsi que dans le suivant, on s'est trompé d'une unité pour chaque comptage, cela n'est pas important, ce qui nous intéresse étant d'observer les écarts et sauts entre les nombres.

Ci-dessous, les tailles des paquets pour les racines $\sqrt{3} - ièmes$:

0	0	0	1	2	2	2	3	4	4	4	5	6	5	7	7	7	8	9	9
10	9	11	11	13	12	12	14	13	15	14	16	16	16	17	17	18	19	19	20
19	21	21	21	23	22	23	24	24	25	25	26	26	26	28	28	28	28	30	29
31	31	31	32	32	33	33	34	34	36	35	36	36	38	37	38	38	40	39	40
40	41	42	42	42	43	44	44	44	45	46	45	47	47	48	48	49	49	49	50
50	51	52	52	53	53	53	54	54	56	55	56	56	57	58	58	58	58	60	61
60	61	61	62	62	64	63	63	65	64	66	66	66	67	67	68	68	69	69	70
70	71	71	72	72	72	74	72	76	74	74	77	76	76	77	77	78	79	79	79
80	80	82	81	81	82	83	84	83	84	86	84	86	86	87	87	88	87	89	89
89	91	89	92	91	92	92	93	93	93	95	95	95	96	96	96	98	97		

Ci-dessous, les tailles des paquets pour les racines nombre-d'or-ièmes :

1	1	1	2	2	2	2	3	3	4	3	4	5	4	4	5	6	6	6	6
6	7	7	8	7	8	8	8	9	9	9	10	10	9	10	11	11	11	11	12
12	12	13	12	13	13	13	14	13	15	14	15	15	15	15	15	17	16	15	18
16	17	18	17	18	18	18	19	19	19	19	19	20	20	20	20	21	21	21	21
23	21	22	22	23	22	23	24	23	24	24	24	24	25	24	25	26	25	26	26
26	26	26	27	28	27	28	27	28	28	29	28	28	30	28	31	29	30	30	30
30	31	31	32	31	31	33	31	32	33	32	33	34	33	33	34	34	34	35	34
35	35	35	35	36	36	36	36	37	37	36	37	38	37	38	38	38	39	38	38
39	40	39	39	40	40	41	40	41	40	40	42	42	41	42	41	43	42	43	42
44	42	44	43	45	44	43	44	45	45	45	45	45	46	45	47	46	46	46	48
46	48	47	47	48	48	48	49	48	48	50	48	50	49	50	49	50	51	50	51
51	51	51	51	52	52	52	52	53	52	52	53	53	53	53	55	53	55	53	55
54	56	54	56	55	55	56	56	56	56	57	57	56	57	57	58	58	57	59	57
58	59	59	59	59	59	59	60	60	60	60	61	60	61	61	61	62	61	61	62
62	62	63	63	62	63	63	63	64											

Ci-dessous, les tailles des paquets pour les racines constante-de-Neper-ièmes :

1	6	14	22	36	50	68	89	112	138	167	198	232	271	309	352
396	444	495	549	603	662	723	787	854	922	994					

Ci-dessous, les tailles des paquets pour les racines Constante-de-Brun-des-premiers-jumeaux-ièmes :

2	1	3	4	5	6	6	8	9	10	10	12	13	16	15	17
17	20	21	21	23	25	25	27	29	29	31	32	33	35	36	38
38	41	41	44	44	46	47	49	50	51	52	55	56	57	59	60
61	63	64	66	67	69	70	72	73	75	76	78	79	80	81	85
84	87	89	89	91	92	95	95	98	98	100	103	102	105	106	108
110	110	113	114	116	117	119	120	122	123	125	126	128	130	131	133
134	136	138	139	141	142	143	147	145	150	150	151	154	154	157	158
160	161	164	163	166	168	169	172	172							

Cette constante est la plus satisfaisante de toutes, compte-tenu de l'objectif : on s'attendait à un tel résultat car on souhaiterait "faire se rapprocher deux nombres premiers jumeaux de plus en plus jusqu'à ce qu'ils ne deviennent qu'un seul nombre premier". Qu'entend-on par là ? Deux nombres premiers impairs jumeaux sont séparés du plus petit intervalle qu'il est possible, qui est 2. On peut voir les nombres premiers (sous-entendu nombres premiers tout courts et non pas jumeaux) comme une limite des nombres premiers jumeaux lorsqu'on essaie encore de faire se rapprocher ceux-ci jusqu'à ce que les deux jumeaux d'un couple se confondent, la distance les séparant s'étant annulée.

On n'a pas encore trouvé une constante qui produirait exactement la suite des entiers successifs et on va continuer à la chercher par tâtonnement.

Ci-dessous, les tailles des paquets pour les racines Constante-Euler-Totient-ièmes (la constante asymptotique de l'indicatrice d'Euler vaut 1.9435964368)[2] :

1	1	2	4	4	5	7	8	9	10	11	14	13	16	17	20
19	22	23	25	25	28	29	32	32	34	36	37	40	40	43	44
45	47	50	51	53	54	57	57	60	62	63	65	67	69	70	73
74	76	78	80	82	83	86	87	89	92	92	96	96	99	101	102
105	106	108	111	112	115	116	118	120	123	124	126	128	130	132	134
136	138	141	141	145	145	149	150	152	155	156	158	161	162	165	166
169	171	172	175	177	179	182	182	185	188	190	191	194	196		

[2]On trouve les valeurs des constantes mathématiques ici http://free-vz.htnet.hr/nstepan/const/math.txt.

Ci-dessous, les tailles des paquets pour les racines Constante-Tetranacci-ièmes (la constante de Tetranacci vaut 1.927561975, on la trouve dans la séquence de l'OEIS A086088 et elle correspond à la section d'or d'un segment de ligne en 4 portions (cf un article de Seppo Mustonen, du département de mathématiques et statistiques de l'Université d'Helsinki) :

1	1	2	3	4	5	6	8	8	10	11	12	13	15	16	17
19	21	21	23	24	26	28	28	31	31	33	35	36	38	40	40
42	44	46	47	48	51	52	53	56	57	58	60	62	64	64	67
68	70	73	73	75	77	78	81	81	85	85	87	88	91	93	94
96	97	100	100	104	105	106	108	110	112	114	115	117	119	121	123
124	126	128	130	132	133	136	137	139	140	143	145	146	148	150	152
154	156	157	160	161	162	165	168	168	171	172	175	175	178	180	183
183	186	187													

On ajoute les suites de nombres trouvées pour les constantes pentanacci, hexanacci et heptanacci.

Taille des paquets pour les racines constante-de-pentanacci-ièmes :

1	1	3	3	5	5	7	9	10	11	13	14	16	17	19	20
22	24	25	27	29	31	33	34	35	38	39	42	43	46	46	50
51	53	55	57	58	61	63	65	67	68	71	73	75	77	79	82
83	85	87	90	92	93	96	99	100	103	104	107	109	112	113	115
119	120	122	125	127	129	131	134	136	137	141	142	145	148	149	152
154	157	158	162	163	166	168	171	173	175	177	181	182	184	187	190
192	194	196	200	201	203	206	209								

Taille des paquets pour les racines constante-de-hexanacci-ièmes :

1	1	3	3	6	6	8	9	10	12	14	15	17	18	20	22
24	25	28	30	30	34	35	37	39	41	43	44	47	50	51	53
56	57	59	63	63	67	68	71	73	75	77	80	82	84	87	88
91	93	97	97	101	103	105	108	110	113	114	118	120	122	125	126
130	133	134	138	139	141	145	147	150	152	155	158	159	162	165	168
170	173	175	178	180	184	185	189	191	194	196	198	201	205	208	208
213	215	217	220												

Taille des paquets pour les racines constante-de-heptanacci-ièmes :

1	1	3	4	5	7	7	9	12	12	13	16	18	19	21	23
24	27	28	31	32	34	37	38	40	43	44	47	49	51	54	55
58	60	61	65	67	69	71	74	75	79	81	82	86	88	90	93
95	98	100	102	106	107	109	113	115	117	121	122	126	128	130	133
135	139	140	144	146	149	151	154	156	159	162	166	167	170	173	175
178	181	184	187	188	193	194	198	200	203	206	209	210	215	217	220
223	225														

La constante qui semble le mieux convenir s'avère être 1.842. Elle permet d'aboutir au nombre 143 en 143 nombres. Il s'agit donc pour les parties imaginaires des zéros de zéta (notées r) de calculer leur racine $1.842 - ième$ qu'on note $\sqrt[1.842]{r}$ et de calculer les tailles des paquets d'images d'antécédents successifs qui ont même partie entière. On aboutit aux tailles de paquets suivantes (on a travaillé avec les 10000 premiers zéros) :

0	1	1	2	3	3	4	6	6	6	8	8	9	11	11	12
13	14	15	15	17	17	19	19	21	21	22	23	24	25	26	27
28	29	30	32	31	34	33	35	36	37	38	39	39	41	42	44
43	45	46	47	48	49	50	51	53	52	54	55	57	57	59	58
61	61	62	64	64	65	67	67	69	69	70	72	73	74	74	77
76	78	79	80	81	82	84	83	86	86	88	88	89	91	91	93
94	94	96	97	97	99	100	101	102	103	105	105	106	107	109	109
111	112	112	114	115	116	117	117	120	120	121	122	124	123	126	127
127	129	129	131	133	132	134	135	136	138	138	139	140	142	143	

Une autre idée : par quels complexes $a+bi$ faut-il multiplier les $\frac{1}{2}+ri$ pour obtenir 1 ?

On appelle r les parties imaginaires des zéros de zêta successifs.

r prend donc les valeurs $14.13, 21.02, 25.01, 30.42, 32.93, \ldots$ On cherche à résoudre $\left(\frac{1}{2}+ir\right)(a+ib)=1$. On développe le produit et on rassemble la partie réelle et la partie imaginaire du complexe obtenu :

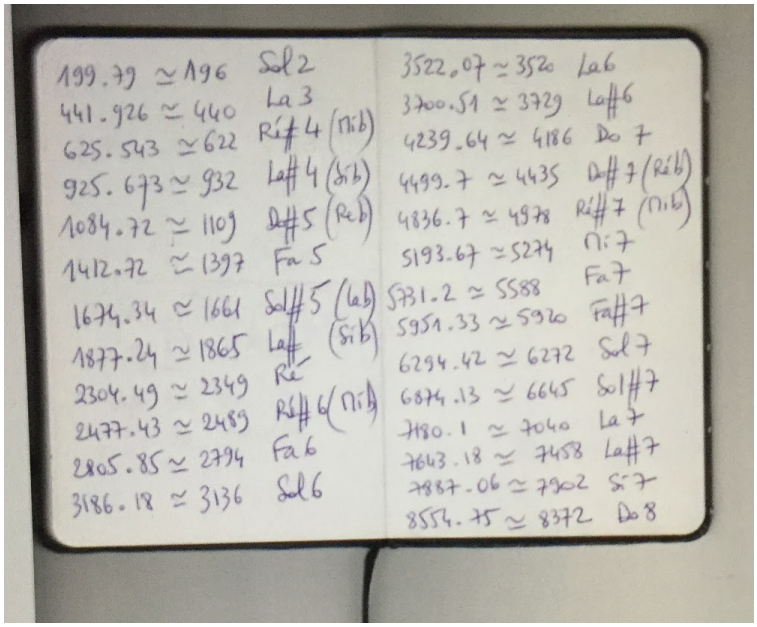
$$\left(\frac{1}{2}a-rb\right)+\left(ra+\frac{1}{2}b\right)i=1.$$

Pour que l'égalité soit vérifiée, la partie imaginaire doit être nulle, la partie réelle doit être égale à 1. On aboutit à :

$$\left(r-\frac{1}{2}\right)a+\left(r+\frac{1}{2}b\right)=-1.$$

Prenons le premier des zéros de zêta, pour lequel $r=14.13$. Pour lui, $a=\frac{1}{2}$ amène $b=-\frac{1}{2}$ dans l'égalité ci-dessus. $a=1$ amène $b=-1$, $a=0$ amène $b=-\frac{1}{14.63}$, $a=2$ amène $b=\frac{-1-2\times 13.63}{14.63}=-1.9316$. Chaque complexe (dont les zéros de zêta) a ainsi une infinité d'inverses. On abandonne cette idée.

Annexe : petite expérience initiale : retrouver les fréquences des notes de la gamme chromatique dans les carrés des parties imaginaires des zéros de zêta



Transcription de la traduction de Laugel en français de l'article de Bernhard Riemann (Denise Vella-Chemla, 24.6.2017)

wikisource Note de Riemann

SUR LE NOMBRE DES NOMBRES PREMIERS INFERIEURS A UNE GRANDEUR DONNEE

Monatsberichte der Berliner Akademie, novembre 1859.
Oeuvres de Riemann, $2^{ième}$ édition, pages 145-155.

Je ne crois pouvoir mieux exprimer mes remerciements à l'Académie pour la distinction à laquelle elle m'a fait participer en m'admettant au nombre de ses Correspondants qu'en faisant immédiatement usage du privilège attaché à ce titre pour lui communiquer une étude sur la fréquence des nombres premiers. C'est un sujet qui, par l'intérêt que Gauss et Dirichlet lui ont voué pendant de longues années, ne me semble peut-être pas indigne de faire l'objet d'une telle Communication.

Je prendrai pour point de départ dans cette étude la remarque faite par Euler[1] que le produit

$$\prod \frac{1}{1-\frac{1}{p^s}} = \sum \frac{1}{n^s}$$

lorsque p prend pour valeur tous les nombres premiers et n tous les nombres entiers. La fonction de la variable complexe s, qui sera représentée par ces deux expressions, tant qu'elles convergent, je la désignerai par $\zeta(s)$. Toutes deux convergent qu'autant que la partie réelle de s est supérieure à 1. Néanmoins il est facile de trouver pour la fonction une expression qui reste toujours valable.

En faisant usage de l'équation

$$\int_0^\infty e^{-nx} x^{s-1} dx = \frac{\prod(s-1)}{n^s}$$

on obtient d'abord

$$\prod(s-1)\zeta(s) = \int_0^\infty \frac{x^{s-1}dx}{e^x - 1}$$

Si maintenant l'on considère l'intégrale

$$\int \frac{(-x)^{s-1}dx}{e^x - 1}$$

prise dans le sens positif de $+\infty$ à $+\infty$ et autour d'un domaine de grandeurs qui contient à son intérieur la valeur 0 mais qui ne contient aucune autre valeur de discontinuité de la fonction sous le signe d'intégration, on obtient aisément pour la valeur de cette intégrale

$$(e^{-\pi si} - e^{\pi si}) \int_0^\infty \frac{x^{s-1}dx}{e^x - 1}$$

en faisant l'hypothèse que dans la fonction multiforme

$$(-x)^{s-1} = e^{(s-1)log(-x)}$$

le logarithme de $-x$ est déterminé de telle sorte qu'il soit réel pour x négatif. On aura donc

$$2\ sin\ \pi s \prod(s-1)\zeta(s) = i \int_0^\infty \frac{(-x)^{s-1}dx}{e^x - 1}$$

l'intégrale étant définie de la manière indiquée ci-dessus.

Cette équation donne maintenant la valeur de la fonction $\zeta(s)$ pour chaque valeur complexe de s et nous enseigne que cette fonction est uniforme, qu'elle est finie pour toutes les valeurs finies de s, sauf 1, et aussi qu'elle s'évanouit lorsque s est égal à un entier pair négatif[2].

Lorsque la partie réelle de s est négative, l'intégrale, au lieu d'être prise dans le sens positif autour du domaine de grandeurs assigné, peut être prise dans le sens négatif autour du domaine de grandeurs qui contient toutes les grandeurs complexes restantes, car l'intégrale, pour des valeurs dont le module est infiniment grand est alors infiniment petite. Mais, à l'intérieur de ce domaine, la fonction sous le signe d'intégration ne devient discontinue que lorsque x est égal à un multiple entier de $\pm 2\pi i$ et l'intégrale, par

conséquent, est égale à la somme des intégrales prises dans le sens négatif autour de ces valeurs. Mais l'intégrale relative à la valeur $n2\pi i$ égale $(-n2\pi i)^{s-1}(-2\pi i)$; on obtient donc

$$2sin\ \pi s \prod(s-1)\zeta(s) = (2\pi)^s \sum n^{s-1}[(-i)^{s-1} + i^{s-1}]$$

c'est-à-dire une relation entre $\zeta(s)$ et $\zeta(s-1)$ qui, en vertu de propriétés connues de la fonction $\prod$ peut aussi s'exprimer ainsi : la quantité

$$\prod\left(\frac{s}{2}-1\right)\pi^{-\frac{s}{2}}\zeta(s)$$

reste inaltérée lorsque s est remplacé par $1-s$.

Cette propriété de la fonction m'a engagé à introduire, au lieu de l'intégrale $\prod(s-1)$, l'intégrale $\prod\left(\frac{s}{2}-1\right)$ dans le terme général de la série $\sum\frac{1}{n^s}$, ce qui fournit une expression très commode de la fonction $\zeta(s)$. On a en effet

$$\frac{1}{n^s}\prod\left(\frac{s}{2}-1\right)\pi^{-\frac{s}{2}} = \int_0^\infty e^{-n^2\pi x}x^{\frac{s}{2}-1}dx;$$

et, par conséquent, si l'on pose

$$\sum_1^\infty e^{-n^2\pi x} = \psi(x)$$

on a

$$\prod\left(\frac{s}{2}-1\right)\pi^{-\frac{s}{2}}\zeta(s) = \int_0^\infty \psi(x)x^{\frac{s}{2}-1}dx;$$

ou bien, puisque

$$2\psi(x)+1 = x^{-\frac{1}{2}}\left[2\psi\left(\frac{1}{x}\right)+1\right]^{[3]},$$

on a encore

$$\prod\left(\frac{s}{2}-1\right)\pi^{-\frac{s}{2}}\zeta(s) = \int_1^\infty \psi(x)x^{\frac{s}{2}-1}dx + \int_0^1 \psi\left(\frac{1}{x}\right)x^{\frac{s-3}{2}}dx + \frac{1}{2}\int_0^1 \psi(x)\left(x^{\frac{s-3}{2}} - x^{\frac{s}{2}-1}\right)dx$$

$$= \frac{1}{s(s-1)} + \int_1^\infty \psi(x)\left(x^{\frac{s}{2}-1} + x^{-\frac{1+s}{2}}\right)dx$$

Je pose maintenant

$$s = \frac{1}{2} + ti$$

et

$$\prod\left(\frac{s}{2}\right)(s-1)\pi^{-\frac{s}{2}}\zeta(s) = \xi(t)$$

en sorte que

$$\xi(t) = \frac{1}{2} - \left(t^2+\frac{1}{4}\right)\int_1^\infty \psi(x)x^{-\frac{3}{4}}cos\left(\frac{1}{2}t\ log\ x\right)dx,$$

ou encore

$$\xi(t) = 4\int_1^\infty \frac{d\left[x^{\frac{3}{2}}\psi'(x)\right]}{dx}x^{-\frac{1}{4}}cos\left(\frac{1}{2}t\ log\ x\right)dx$$

Cette fonction est finie pour toutes les valeurs finies de t et peut être développée suivant les puissances de t^2 en une série qui converge très rapidement. Puisque, pour une valeur de s dont la partie réelle est plus grande que 1, $log\ \zeta(x) = -\sum log(1-p^{-s})$ reste fini et que ce même fait a lieu pour les logarithmes des facteurs restants de $\xi(t)$, la fonction $\xi(t)$ peut seulement s'évanouir lorsque la partie imaginaire de t se trouve comprise entre $\frac{1}{2}i$ et $-\frac{1}{2}i$. Le nombre de racines de $\xi(t)=0$ dont les parties réelles sont comprises entre 0 et T est environ égal à

$$\frac{T}{2\pi}log\frac{T}{2\pi} - \frac{T}{2\pi}$$

car l'intégrale $\int d\ log\ \xi(t)$ prise le long d'un contour décrit dans le sens positif, comprenant à son intérieur l'ensemble des valeurs de t dont les parties imaginaires sont comprises entre $\frac{1}{2}i$ et $-\frac{1}{2}i$ et les parties réelles entre 0 et T est égale (abstraction faite d'une partie fractionnaire de même ordre de grandeur que la

grandeur $\frac{1}{T}$) à $(Tlog\ \frac{T}{2\pi} - T)i$; or cette intégrale est égale au nombre de racines de $\xi(t) = 0$ situées dans ce domaine, multiplié par $2\pi i$. On trouve, en effet, entre ces limites un nombre environ égal à celui-ci, de racines réelles, et il est très probable que toutes les racines sont réelles[4].

Il serait à désirer, sans doute, que l'on eût une démonstration rigoureuse de cette proposition ; néanmoins j'ai laissé cette recherche de côté pour le moment après quelques rapides essais infructueux, car elle paraît superflue pour le but immédiat de mon étude.

Si l'on désigne par α toute racine de l'équation $\xi(\alpha) = 0$, on peut exprimer $log\ \xi(t)$ par

$$\sum log\left(1 - \frac{t^2}{\alpha^2}\right) + log\ \xi(0)$$

En effet, puisque la densité des racines de grandeur t augmente seulement avec t comme le fait $log\ \frac{t}{2\pi}$, cette expression converge et pour t infini ne devient infinie que comme l'est $t\ log\ t$; elle diffère de $log\ \xi(t)$ par conséquent d'une fonction de t^2 qui, pour t fini, reste finie et continue et qui, divisée par t^2, sera infiniment petite pour t infini.

Cette différence, par suite, est une constante dont la valeur peut être déterminée en posant $t = 0$.

A l'aide de ces principes auxiliaires, nous pouvons maintenant déterminer le nombre des nombres premiers qui sont inférieurs à x.

Soit $F(x)$ ce nombre lorsque x n'est pas exactement égal à un nombre premier, et soit $F(x)$ ce nombre augmenté de $\frac{1}{2}$ lorsque x est premier, de telle sorte que, pour une valeur de x, pour laquelle $F(x)$ varie par un saut brusque, on ait,

$$F(x) = \frac{F(x+0) + F(x-0)}{2}$$

Si, maintenant, dans l'expression

$$log\ \zeta(s) = -\sum log(1 - p^{-s}) = \sum p^{-s} + \frac{1}{2}\sum p^{-2s} + \frac{1}{3}\sum p^{-3s}$$

on remplace p^{-s} par $s\int_p^\infty x^{-s-1}dx, p^{-2s} = s\int_{p^2}^\infty x^{-s-1}dx, \ldots$, on obtient

$$\frac{log\ \zeta(s)}{s} = \int_1^\infty f(x)x^{-s-1}dx,$$

où l'on a désigné par $f(x)$ l'expression $F(x) + \frac{1}{2}F(x^{\frac{1}{2}}) + \frac{1}{3}F(x^{\frac{1}{3}}) + \ldots$

Cette équation a lieu pour toute valeur complexe $a + bi$ de s, pourvu que $a > 1$. Mais lorsque, sous ces hypothèses, l'équation suivante

$$g(s) = \int_0^\infty h(x)x^{-s}d\ log\ x$$

a lieu, l'on peut, à l'aide du théorème de Fourier, exprimer la fonction h par la fonction g. Cette équation, quand $h(x)$ est réel et que

$$g(a + bi) = g_1(b) + ig_2(b)$$

se décompose en les deux suivantes :

$$g_1(b) = \int_0^\infty h(x)x^{-a}\cos(b\log x)d\log x,$$

$$ig_2(b) = -i\int_0^\infty h(x)x^{-a}\sin(b\log x)d\log x.$$

Lorsque l'on multiplie les deux équations par

$$[\cos(b\log y) + i\sin(b\log y)]\,db,$$

et que l'on intègre de $-\infty$ à $+\infty$, l'on obtient, en vertu du théorème de Fourier, dans les seconds membres des deux équations $\pi h(y) y^{-a}$, et, par conséquent, en ajoutant les deux équations et multipliant par iy^a, on a

$$2\pi i h(y) = \int_{a-\infty i}^{a+\infty i} g(s) y^s ds,$$

où l'intégration doit être prise de telle sorte que la partie réelle de s reste constante[5].

Cette intégrale représente, pour une valeur de y pour laquelle a lieu une variation par saut brusque de la fonction, la valeur moyenne des valeurs de la fonction h de chaque côté du saut. Avec les modes de détermination exposés ci-dessus, la fonction $f(x)$ possède cette même propriété, et l'on a donc, d'une manière générale,

$$f(y) = \frac{1}{2\pi i} \int_{a-\infty i}^{a+\infty i} \frac{\log \zeta(s)}{s} y^s ds$$

On peut maintenant substituer à $log\ \zeta$, l'expression trouvée précédemment[6]

$$\frac{s}{2} \log \pi - \log(s-1) - \log \prod \frac{s}{2} + \sum_{\alpha} \log \left[1 + \frac{(s - \frac{1}{2})^2}{\alpha^2} \right] + \log \xi(0)$$

Mais les intégrales de chaque terme de cette expression, prises jusqu'à l'infini, ne convergent pas ; il sera donc convenable de transformer l'équation précédente à l'aide d'une intégration par parties en

$$f(x) = -\frac{1}{2\pi i} \frac{1}{\log x} \int_{a-\infty i}^{a+\infty i} \frac{d \frac{\log \zeta(s)}{s}}{ds} x^s ds$$

Comme

$$-\log \prod \frac{s}{2} = \lim \left[\sum_{n=1}^{n=m} \log \left(1 + \frac{s}{2n} \right) - \frac{s}{2} \log m \right],$$

pour $m = \infty$, et que, par suite

$$-\frac{d \frac{1}{s} \log \prod \left(\frac{s}{2} \right)}{ds} = \sum_{1}^{\infty} \frac{d \frac{1}{s} \log \left(1 + \frac{s}{2n} \right)}{ds},$$

tous les termes de l'expression de $f(x)$, à l'exception de

$$\frac{1}{2\pi i} \frac{1}{\log x} \int_{a-\infty i}^{a+\infty i} \frac{1}{s^2} \log \xi(0) x^s ds = \log \xi(0),$$

prennent alors la forme

$$\pm \frac{1}{2\pi i} \frac{1}{\log x} \int_{a-\infty i}^{a+\infty i} \frac{d \left[\frac{1}{s} \log \left(1 - \frac{s}{\beta} \right) \right]}{ds} x^s ds.$$

Mais on a maintenant

$$\frac{d \left[\frac{1}{s} \log \left(1 - \frac{s}{\beta} \right) \right]}{d\beta} = \frac{1}{(\beta - s)\beta}$$

et, lorsque la partie réelle de s est plus grande que la partie réelle de β,

$$-\frac{1}{2\pi i} \int_{a-\infty i}^{a+\infty i} \frac{x^s ds}{(\beta - s)\beta} \quad = \frac{x^\beta}{\beta} \quad = \int_{\infty}^{x} x^{\beta - 1} dx,$$

ou bien

$$= \int_{0}^{x} x^{\beta - 1} dx,$$

selon que la partie réelle de β est négative ou positive. On a donc, dans le premier cas,

$$\frac{1}{2\pi i}\frac{1}{\log x}\int_{a-\infty i}^{a+\infty i}\frac{d\left[\frac{1}{s}\log\left(1-\frac{s}{\beta}\right)\right]}{ds}x^s ds$$

$$=-\frac{1}{2\pi i}\int_{a-\infty i}^{a+\infty i}\frac{1}{s}\log\left(1-\frac{s}{\beta}\right)x^s ds$$

$$=\int_{\infty}^{x}\frac{x^{\beta-1}}{\log x}dx+\text{const.},$$

et, dans le second cas,

$$=\int_{0}^{x}\frac{x^{\beta-1}}{\log x}dx+\text{const.}$$

Dans le premier cas, la constante d'intégration peut être déterminée en faisant tendre la partie réelle de β vers l'infini négatif.

Dans le second cas, l'intégrale de 0 à x prend des valeurs qui diffèrent de $2\pi i$, lorsque l'intégrale relative à des valeurs complexes est prise dans le sens positif ou dans le sens négatif, et elle sera, prise dans ce dernier sens, infiniment petite lorsque le coefficient de i dans la valeur de β est égal à l'infiniment grand positif ; mais ce fait aura lieu, dans le premier cas, lorsque le coefficient est égal à l'infiniment grand négatif.

Ceci nous enseigne comment $log(1-\frac{s}{\beta})$ doit être déterminé dans le premier membre de manière à faire disparaître la constante d'intégration.

En portant ces valeurs dans l'expression de $f(x)$ on obtient

$$f(x)=Li(x)-\sum_{\alpha}\left[Li\left(x^{\frac{1}{2}+\alpha i}\right)+Li\left(x^{\frac{1}{2}-\alpha i}\right)\right]$$

$$+\int_{x}^{\infty}\frac{1}{x^2-1}\frac{dx}{x\log x}+\log\xi(0),$$

[7],[8]

où, dans la série $\sum_{\alpha}$ on donnera à α pour valeurs toutes les racines positives (ou à parties réelles positives) de l'équation $\xi(\alpha)=0$ en les rangeant par ordre de grandeur. On peut alors, après une discussion plus approfondie de la fonction ξ, démontrer aisément que lorsque les termes sont rangés, comme il est prescrit ci-dessus, dans la série

$$\sum\left[Li\left(x^{\frac{1}{2}+\alpha i}\right)+Li\left(x^{\frac{1}{2}-\alpha i}\right)\right],$$

celle-ci converge vers la même limite que l'expression

$$\frac{1}{2\pi i}\int_{a-bi}^{a+bi}\frac{d\frac{1}{s}\sum\log\left[1+\frac{\left(s-\frac{1}{2}\right)^2}{\alpha^2}\right]}{ds}x^s ds,$$

lorsque la grandeur b croît sans limites. Mais, si l'on changeait cet ordre des termes de la série, on pourrait obtenir pour résultat n'importe quelle valeur réelle.

A l'aide de $f(x)$ l'on obtient $F(x)$ par inversion de la relation

$$f(x)=\sum\frac{1}{n}F\left(x^{\frac{1}{n}}\right),$$

ce qui donne l'équation

$$F(x)=\sum(-1)^{\mu}\frac{1}{m}f\left(x^{\frac{1}{m}}\right),$$

où m doit être remplacé successivement par tous les nombres qui ne sont divisibles par aucun carré excepté 1 et où μ désigne le nombre des facteurs premiers de m.

Si on limite $\sum_{\alpha}$ à un nombre fini de termes, la dérivée de l'expression $f(x)$ c'est-à-dire, abstraction faite d'une partie qui décroît très rapidement lorsque x croît,

$$\frac{1}{\log x} - 2\sum_{\alpha} \frac{\cos(\alpha \log x) x^{-\frac{1}{2}}}{\log x},$$

fournit une expression approchée pour la densité des entiers premiers + la moitié de la densité des carrés, + le tiers de celle des cubes, + ... des entiers premiers inférieurs à x.

La formule approchée connue $F(x) = Li(x)$ n'est, par conséquent, exacte qu'aux grandeurs près de l'ordre de $x^{\frac{1}{2}}$ et fournit une valeur un peu trop grande ; car les termes non périodiques[9] dans l'expression de $F(x)$ sont, abstraction faite de grandeurs qui ne croissent pas indéfiniment avec x,

$$Li(x) - \frac{1}{2}Li\left(x^{\frac{1}{2}}\right) - \frac{1}{3}Li\left(x^{\frac{1}{3}}\right) - \frac{1}{5}Li\left(x^{\frac{1}{5}}\right) + \frac{1}{6}Li\left(x^{\frac{1}{6}}\right) - \frac{1}{7}Li\left(x^{\frac{1}{7}}\right) + \ldots$$

Du reste, la comparaison, entreprise par Gauss et Goldschmidt[10], de $Li(x)$ avec le nombre de nombres premiers inférieurs à x et poursuivie jusqu'à $x =$ trois millions a révélé que ce nombre, à partir de la première centaine de mille, est toujours inférieur à $Li(x)$ et que la différence des valeurs, soumises à maintes oscillations, croît néanmoins toujours avec x[11]. Mais la fréquence et la réunion plus dense par endroits des nombres premiers, si l'on peut s'exprimer ainsi, sous l'influence des termes périodiques, avaient déjà attiré l'attention, lors du dénombrement des nombres premiers, sans que l'on eût aperçu la possibilité d'établir une loi à ce sujet.

Il serait intéressant dans un nouveau dénombrement, d'étudier l'influence de chaque terme périodique contenu dans l'expression donnée pour la totalité des nombres premiers. Une marche plus régulière que celle donnée par $F(x)$ serait obtenue à l'aide de la fonction $f(x)$ qui, cela se reconnaît déjà très évidemment dans la première centaine, coïncide en moyenne avec $Li(x) + log\ \xi(0)$.

Notes

1. Leonhard Euler, *Introductio in analysin infinitorum.* Bd. 1. Lausanne 1748, p. 221-252, ch. 15 (*De Seriebus ex evolutione Factorum ortis*).

2. [Note du trad.] Ce mode d'existence de la fonction $\zeta(s)$ se reconnaît en se servant de la seconde forme de cette fonction

$$2\zeta(s) = \pi i \prod(-s) \int_{-\infty}^{+\infty} \frac{(-x)^{s-2}}{e^{x-1}} dx$$

et en remarquant, en outre, que $\frac{1}{e^x - 1} - \frac{1}{2}$, dans le développement suivant les puissances ascendantes de x, ne contient que des puissances impaires.

3. Riemann se réfère à Carl Gustav Jacob Jacobi, *Fundamenta Nova Theoriae Functionum Ellipticarum.* Königsberg 1829, p. 184, § 65, Nr. 6. La formule utilisée n'est pas donnée ici explicitement ; Jacobi la déduit à un autre endroit dans *Suite des notices sur les fonctions elliptiques.*, in Journal de Crelle 3 (1828), p. 303-310.

4. Cette phrase constitue le premier énoncé de "l'hypothèse de Riemann".

5. Note du trad. L'énoncé de ce théorème manque de rigueur. Les deux équations traitées séparément comme il est indiqué, les limites d'intégration $0, \infty$ se rapportant à $log\ x$, donnent

$$\pi y^{-\alpha} \left[h(y) \pm h\left(\frac{1}{y}\right)\right],$$

et, par conséquent, fournissent en premier lieu par leur somme la formule du texte.

6. Le manuscrit Lien du Clay Mathematical Institute (p. 4) et les *Gesammelte Werke* (p. 141) introduisent encore un $\sum_{\alpha}$ devant l'avant-dernier logarithme. Dans les *Monatsberichte* le signe somme manque :

$$\frac{s}{2} log\ \pi - log(s-1) - log \prod \frac{s}{2} + log\left(1 + \frac{(s-\frac{1}{2})^2}{\alpha\alpha}\right) + log\ \xi(0)$$

7. Note HME 1974, p. 31. Riemann écrit $log\ \xi(0)$ à la place de $-log\ 2$, mais puisqu'il utilise ξ pour noter une fonction différente à savoir la fonction $\xi(\frac{1}{2} + it)$, son $\xi(0)$ dénote $\xi(\frac{1}{2}) \neq \frac{1}{2}$. Cette erreur a été

détectée du vivant de Riemann par Angelo Genocchi (1817-1889), *Formole per determinare quanti siano i numeri primi fino ad un dato limite*, in Annali di Matematica Pura ed Applicata 3 (1860), p. 52-59.

8. Note du trad. La fonction $Li(x)$ doit être définie pour les valeurs réelles de x qui sont plus grandes que 1 par l'intégrale

$$\int_0^x \frac{dx}{log\ x} \pm \pi i$$

où l'on doit prendre le signe supérieur ou bien le signe inférieur, selon que l'intégration est prise relativement à des valeurs complexes dans le sens positif ou bien dans le sens négatif. De là l'on déduit aisément le développement donné par Scheibner (Schlömilch's Zeitschrift, t. V)

$$Li(x) = log\ log\ x - \Gamma'(1) + \sum_{1,\infty}^{x} \frac{(log\ x)^n}{n.n!},$$

qui est valable pour toutes les valeurs de x, et présente une discontinuité pour les valeurs réelles négatives (comparer la correspondance entre Gauss et Bessel).

Si l'on poursuit le calcul indiqué par Riemann, on trouve dans la formule $log\ \frac{1}{2}$ au lieu de $log\ \xi(0)$. Il est très possible que ceci ne soit qu'un *lapsus calami*, ou une faute d'impression, $log\ \xi(0)$ au lieu de $log\ \zeta(0)$; en effet, $log\ \zeta(0) = \frac{1}{2}$.

9. Note H.M.E. En toute rigueur, les termes $Li(x^{\frac{1}{2}+\alpha i})$ ne sont pas périodiques mais oscillatoires.

10. Carl Wolfgang Benjamin Goldschmidt (1807-1851), un élève de Gauss.

11. Lettre de Carl Friedrich Gauss à Johann Franz Encke (1791-1865) du 24 décembre 1849.

Proposer une autre formule de calcul du nombre de nombres premiers inférieurs à un nombre donné (Denise Vella-Chemla, 1.7.2017)

On voudrait ici proposer une formule légèrement différente de celle que Bernhard Riemann a élaborée pour compter le nombre de nombres premiers inférieurs à un nombre donné.

Bien que moins performante que la formule de Riemann, le but de cette nouvelle formule, basée sur une idée de Gauss, pourrait être de faciliter l'appréhension des processus à l'oeuvre dans les petites fluctuations qui interviennent pour le calcul des nombres de nombres premiers, pour le calcul des ratios aux logarithmes, ou bien pour le calcul des tailles des différents intervalles qui sont utilisés dans l'article que Riemann a consacré à la fonction $\pi(x)$.

On ne s'intéresse ici qu'aux formules suivantes de l'article de Riemann, soit que ces formules possèdent une propriété de symétrie, soit qu'elles permettent (c'est le cas pour la dernière) d'obtenir une formule exacte de décompte des nombres premiers. Il est dit que la volonté d'obtenir une formule exacte était l'une des motivations de Riemann lorsqu'il a écrit l'article qui énonce sa célèbre hypothèse.

1) $f(x) = \pi(x) + \frac{1}{2}\pi\left(x^{\frac{1}{2}}\right) + \frac{1}{3}\pi\left(x^{\frac{1}{3}}\right) + \frac{1}{4}\pi\left(x^{\frac{1}{4}}\right) + \frac{1}{5}\pi\left(x^{\frac{1}{5}}\right) + \ldots$

2) $\pi(x) = \frac{\mu(2)}{2}f\left(x^{\frac{1}{2}}\right) + \frac{\mu(3)}{3}f\left(x^{\frac{1}{3}}\right) + \frac{\mu(4)}{4}f\left(x^{\frac{1}{4}}\right) + \frac{\mu(5)}{5}f\left(x^{\frac{1}{5}}\right) + \ldots = \sum \frac{\mu(k)}{k}f\left(x^{\frac{1}{k}}\right)$

3) $\pi(x) = Li(x) + \frac{\mu(2)}{2}Li\left(x^{\frac{1}{2}}\right) + \frac{\mu(3)}{3}Li\left(x^{\frac{1}{3}}\right) + \frac{\mu(4)}{4}Li\left(x^{\frac{1}{4}}\right) + \frac{\mu(5)}{5}Li\left(x^{\frac{1}{5}}\right) + \ldots = \sum \frac{\mu(k)}{k}Li\left(x^{\frac{1}{k}}\right)$

4) $f(x) = Li(x) - \sum_{\rho}(Li(x^{\rho}) + Li(x^{\overline{\rho}})) + \int_x^{\infty} \frac{du}{u(u^2-1)ln\ u} + ln\ 2$

(avec $\rho = \frac{1}{2} + \alpha\ i$ et $\overline{\rho} = \frac{1}{2} - \alpha\ i$)

Les formules 2) et 3) utilisent la fonction de Moebius qui a comme propriété de permettre d'inverser certains calculs (par l'inversion de Moebius), i.e. elle permet d'obtenir l'image par une fonction d'un nombre en agrégeant les images de ses diviseurs. La fonction de Moebius "élimine les carrés" et compte la parité du nombre de diviseurs des produits purs (elle vaut -1 pour les nombres produits purs d'un nombre impair de diviseurs (ex : $30 = 2.3.5$ a 3 diviseurs) et 1 pour les nombres produits purs d'un nombre pair de diviseurs (ex : $210 = 2.3.5.7$ a 4 diviseurs). La fonction de Moebius "équilibre" à peu près les ajouts et les soustractions (jusqu'à 10 racines, 4 signes - pour 2 signes +, jusqu'à 100, 30 signes + et 30 signes - à égalité, jusqu'à 1000, 304 signes + pour 303 signes -, jusqu'à 10000, 3029 signes + pour 3053 signes -, jusqu'à 10^5, 30372 signes + pour 30421 signes -, etc.).

A la place de la formule de Moebius, on propose de compter, comme Gauss le préconise dans le chapitre des Recherches arithmétiques consacré à la loi de réciprocité quadratique, la parité du nombre de facteurs de la forme $4k-1$ intervenant dans les factorisations des nombres et de remplacer les valeurs fournies par la fonction de Moebius par celles fournies par ce nouveau comptage. On appelle le résultat de notre fonction $D(x)$.

$$D(x) = \pi(x) + \sum_k \frac{4kmoins1(k)}{k} \frac{x^{\frac{1}{k}}}{log\left(x^{\frac{1}{k}}\right)}.$$

On peut calculer les résultats obtenus pour cette nouvelle formule par le programme ci-après.

Ce programme n'est pas efficace du tout. De plus, on a mal initialisé le cumul : il aurait fallu l'initialiser à $\frac{x}{log(x)}$ plutôt qu'à $\pi(x)$. Toujours est-il que la différence entre la valeur finale de $D(x)$ et $\pi(x)$ est tout de même suffisamment petite pour présenter un intérêt ($D(x) - \pi(x) = 58$ pour 80 000). Il faudrait comprendre comment les différentes variables évoluent en analysant les premières valeurs (pour x jusqu'à 100). Il faudrait sûrement réfléchir dans une direction qui considère qu'un $4n+1$ peut être mis sous la forme $(-2\sqrt{n}+i)(-2\sqrt{n}-i)$ (les deux facteurs du produit étant deux points conjugués du plan complexe situés de part et d'autre du point réel $-2\sqrt{n}$, l'un en haut, l'autre en bas, sur la droite des complexes de partie réelle $-2\sqrt{n}$) tandis qu'un nombre de la forme $4n-1$ peut être mis sous la forme $(-2\sqrt{n}+1)(-2\sqrt{n}-1)$ (les deux facteurs étant deux réels situés de part et d'autre à distance 1 d'un zéro trivial). Mais ces idées sont pour l'instant trop spéculatives pour pouvoir être exploitées.

```
#include <iostream>
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <cmath>

int tabfacteurs[1000005], tabpuiss[1000005], tabexpo[1000005], tabcpte4kmoins1[1000005] ;

int prime(int atester) {
  bool pastrouve=true;
  unsigned long k = 2;
  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else if ((atester % k) == 0) {
      return 0 ;
    }
    else k++;
  }
}

int arrondi(float nombre) {
  return nombre + 0.5;
}

int main(int argc,char **argv) {
  int  x, k, i, d, pix, p, nbdiv, tempo, expo ;
  float res, cumul ;
  int compte4kmoins1 ;

  compte4kmoins1 = 1 ;
  for (i = 1 ; i <= 1000000 ; ++i) {
    std::cout << "\n" << i << " -> " ;
    tabfacteurs[i] = 1 ;
    tabpuiss[i] = 1 ;
    tabexpo[i] = 1 ;
    tempo = i ;
    p = i/2 ;
    nbdiv = 1 ;
    if (prime(tempo)) {
      tabfacteurs[1] = tempo ;
      tabpuiss[1] = tempo ;
      tabexpo[1] = 1 ;
    }
    else while ((tempo > 1) && (p > 1)) {
      if ((prime(p)) && ((tempo%p) == 0)) {
        tabfacteurs[nbdiv] = p ;
        nbdiv = nbdiv+1 ;
        tempo = tempo/p ;
      }
      p=p-1 ;
    }
```

```
if (not(prime(i))) nbdiv=nbdiv-1 ;
    if ((nbdiv == 1) && (prime(i))) {
      tabpuiss[1] = i ;
      tabexpo[1] = 1 ;
    }
    else if ((nbdiv == 1) && (not(prime(i)))) {
      tempo = tabfacteurs[1] ;
      tabpuiss[1] = i ;
      expo = 1 ;
      while (tempo < i) {
        tempo=tempo*tabfacteurs[1] ;
        expo = expo+1 ;
      }
      tabexpo[1] = expo ;
    }
    else if (nbdiv > 1) {
      for (k = 1 ; k <= nbdiv ; ++k){
        tempo = tabfacteurs[k] ;
        expo = 1 ;
        while (((i % tempo) == 0) && (tempo < i)) {
          tempo=tempo*tabfacteurs[k] ;
          expo = expo+1 ;
  }
  tabpuiss[k] = tempo/tabfacteurs[k] ;
  tabexpo[k] = expo-1 ;
      }
    }
    for (k = 1 ; k <= nbdiv ; ++k) {
      std::cout << tabfacteurs[k] << "^" ;
      std::cout << tabexpo[k] << "." ;
      if ((tabfacteurs[k] % 4) == 3)
      if ((tabexpo[k] %2 ) == 1)
      compte4kmoins1 = compte4kmoins1 * (-1) ;
    }
    tabcpte4kmoins1[i] = compte4kmoins1 ;
  }
  std::cout << "\n" ;
  for (x = 2 ; x <= 1000000 ; ++x) {
    std::cout << x << " -->    " ;
    pix = 0 ;
    for (i = 2 ; i <= x ; ++i) if (prime(i)) pix = pix+1 ;
    std::cout << "pi("<< x << ")=" << pix ;
    std::cout << "  compte4kmoins1 " << tabcpte4kmoins1[x] << "\n" ;

    cumul = (float) pix ;
    for (k = 2 ; k <= sqrt(x) ; ++k) {
      res = pow(x,1./k) ;
      cumul = cumul+(tabcpte4kmoins1[k]/(float) k)*(res/log(res)) ;
    }
    std::cout << "res final " << arrondi(cumul) << "\n\n" ;
  }
}
```

Le tableau ci-dessous fournit les différences entre le nombre calculé par la fonction proposée ici $D(x)$ et la valeur effective de $\pi(x)$. Il fournit également les différences entre la fonction $Li(x)$ et la fonction $\pi(x)$. Pour 10^6, on voit que l'estimation la plus juste proposée par Riemann ($R(x)$ est bien meilleure que l'approximation proposée ici (30 (valeur trouvée dans la littérature) $\ll$ 60). En ce qui concerne le calcul de la formule 3), il n'est qu'approximatif : on a approximé les logarithmes intégrals en faisant calculer par Python les logarithmes intégrals de nombres entiers jusqu'à 1000000. Malgré cela, la formule 3) est la meilleure. Ne disposant pas d'un logiciel de calcul formel permettant de calculer les logarithmes intégrals, on ne peut pas pour l'instant voir l'efficacité de la formule 4).

x	$\pi(x)$	$Li(x)$	$Li(x)-\pi(x)$	$D(x)$	$D(x)-\pi(x)$	$formule\ 1)$	$formule\ 3)$
500	95	101	6	95	0	101	94
1 000	168	177	9	168	0	176	168
2 000	303	314	11	304	1	313	303
5 000	669	684	15	672	3	683	669
10 000	1 229	1 245	16	1 235	6	1 247	1 227
20 000	2 262	2 288	26	2 271	9	2 285	2 264
50 000	5 133	5 165	33	5 149	16	5 164	5 133
100 000	9 592	9 629	37	9 614	22	9 633	9 587
200 000	17 984	18 035	51	18 014	30	18 037	17 981
500 000	41 638	41 606	32	41 584	46	41 614	41 529
995 907	78 262	78 332	70	78 199	63	78 298	78 231
1 000 000	78 498	78 627	130	78 558	60	78 726	78 528
10 000 000	664 579	664 917	338			664 829	664 668
100 000 000	5 761 455	5 762 208	753			5 761 554	5 761 551
1 000 000 000	50 847 534	50 849 233	1 699			50 847 633	50 847 455

Ci-dessous, le tableau des écarts à $\pi(x)$, plus parlant :

x	$\pi(x)$	$D(x)-\pi(x)$	$formule\ 1)-\pi(x)$	$formule\ 3)-\pi(x)$
500	95	0	6	1
1 000	168	0	8	0
2 000	303	1	10	0
5 000	669	3	14	0
10 000	1 229	6	18	2
20 000	2 262	9	23	2
50 000	5 133	16	31	0
100 000	9 592	22	41	5
200 000	17 984	30	53	3
500 000	41 638	−46	−24	9
995 907	78 262	−63	36	31
1 000 000	78 498	60	228	30
10 000 000	664 579		250	89
100 000 000	5 761 455		99	96
1 000 000 000	50 847 534		99	79

En annexe sont fournies les valeurs calculées au fur et à mesure de l'application des formules 1 et 3 pour le nombre 995907, on voit bien les fluctuations autour de la valeur finalement atteinte.

Fournissons les valeurs qui ont été calculées pour estimer $D(1\ 000\ 000) = \pi(10^6) + \sum_k \frac{4kmoins1(k)}{k} \frac{x^{\frac{1}{k}}}{log\left(x^{\frac{1}{k}}\right)}$ et qui font intervenir les racines n-ièmes de 1000000 (les racines n-ièmes au-delà de la $20^{ème}$ sont trop petites (i.e.

inférieures strictement à 2, $\sqrt[20]{1\ 000\ 000} = 1.99526$), leur $\pi(k)$ est nul, elles n'ont pas à être prises en compte :

$\frac{1}{2}\frac{1000}{log(1000)}$	72.3824	$\frac{1}{11}\frac{3.51119}{log(3.51119)}$	0.254149
$\frac{-1}{3}\frac{100}{log(100)}$	−7.23824	$\frac{-1}{12}\frac{3.16228}{log(3.16228)}$	−0.228893
$\frac{-1}{4}\frac{31.6228}{log(31.6228)}$	−2.28893	$\frac{-1}{13}\frac{2.89427}{log(2.89427)}$	−0.209494
$\frac{-1}{5}\frac{15.8429}{log(15.8429)}$	−1.14718	$\frac{1}{14}\frac{2.6827}{log(2.6827)}$	0.19418
$\frac{1}{6}\frac{10}{log(10)}$	0.723824	$\frac{-1}{15}\frac{2.51189}{log(2.51189)}$	−0.181816
$\frac{-1}{7}\frac{7.19686}{log(7.19686)}$	−0.520926	$\frac{-1}{16}\frac{2.37137}{log(2.37137)}$	−0.171646
$\frac{-1}{8}\frac{5.62341}{log(5.62341)}$	−0.407036	$\frac{-1}{17}\frac{2.25393}{log(2.25393)}$	−0.163145
$\frac{-1}{9}\frac{4.64159}{log(4.64159)}$	−0.335969	$\frac{-1}{18}\frac{2.15443}{log(2.15443)}$	−0.155943
$\frac{-1}{10}\frac{3.98107}{log(3.98107)}$	−0.28816	$\frac{1}{19}\frac{2.06914}{log(2.06914)}$	0.149769

Annexe 1 : sources permettant de tester les fonctions moins performantes

Le programme ci-dessous a permis de trouver les valeurs de $f(x)$ jusqu'à 1 000 000 000 selon la première formule fournie (formule proposée en 1) dans la première page).

```
#include <iostream>
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <cmath>

int prime(int atester) {
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else if ((atester % k) == 0) {
      return 0 ;
    }
    else k++;
  }
}

int moebius(int n) {
  int moebius, p, nbdiv, carre ;

  moebius = -2 ;
  nbdiv = 0 ;
  for (p=2 ; p <= n ; p++) {
    if (prime (p)) {
      carre = p*p ;
      if ((n % carre) == 0) moebius = 0 ;
      if ((n % p) == 0) nbdiv++ ;
    }
  }
  if (moebius == 0) return 0 ;
  else {
    if ((nbdiv % 2) == 1) return -1 ;
    else return 1 ;
  }
}

int arrondi(float nombre) {
  return nombre + 0.5;
}
```

```
int main(int argc,char **argv) {
  int  x, y, tempo ;
  float somme, pix, restempo ;
  int stocke[100005] ;

  for (x = 2 ; x <= 100000 ; ++x) stocke[x] = 0 ;
  for (x = 2 ; x <= 100000 ; ++x) {
    pix = 0 ;
    for (y = 1 ; y <= x ; ++y)
      if (prime(y)) pix = pix+1 ;
    stocke[x] = pix ;
  }
  for (x = 2 ; x <= 100000 ; ++x) std::cout << x << " -> pi(x) " << stocke[x] << " moebius(x) " <<
      moebius(x) << "\n" ;

  for (x = 2 ; x <= 100000 ; ++x) {
    std::cout << x << " --> " ;
    somme = stocke[x] ;
    tempo = 2 ;
    while (pow(x, 1./tempo) >= 2) {
      restempo = (1.0/(float)tempo)*((float)stocke[(int)pow(x, 1./tempo)]) ;
      std::cout << "rs " << restempo << "\n" ;
      somme = somme+restempo ;
      tempo = tempo+1 ;
   }
   std::cout << (int) somme << "\n" ;
  }
  std::cout << "\n\n" ;
}
```

Le programme ci-dessous a permis de trouver les valeurs de $\pi(x)$ jusqu'à 1 000 000 000 selon la troisième formule fournie (formule proposée en 3) dans la première page). Les logarithmes intégrals ont été calculés avec gnu-octave et stockés préalablement dans un fichier dans lequel on va les chercher.

```
#include <iostream>
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <cmath>
#include <fstream>

int prime(int atester) {
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else if ((atester % k) == 0) {
      return 0 ;
    }
    else k++;
  }
}
```

```
1
2  int moebius(int n) {
3    int moebius, p, racine, nbdiv, carre ;
4
5    moebius = -2 ;
6    nbdiv = 0 ;
7    racine = sqrt(n) ;
8    for (p=2 ; p <= n ; p++) {
9      if (prime (p)) {
10       carre = p*p ;
11       if ((n % carre) == 0) moebius = 0 ;
12       if ((n % p) == 0) nbdiv++ ;
13     }
14   }
15   if (moebius == 0) return 0 ;
16   else {
17     if ((nbdiv % 2) == 1) return -1 ;
18     else return 1 ;
19   }
20 }
21
22 int arrondi(float nombre) {
23   return nombre + 0.5;
24 }
25
26 int main(int argc,char **argv) {
27   int  x, y, pix, mu, k, i ;
28   float res, cumul ;
29   int stocke[10005] ;
30   float logainte[10005] ;
31
32   for (x = 2 ; x <= 10000 ; ++x) stocke[x] = 0 ;
33   for (x = 2 ; x <= 10000 ; ++x) {
34     pix = 0 ;
35     for (y = 1 ; y <= x ; ++y)
36       if (prime(y)) pix = pix+1 ;
37     stocke[x] = pix ;
38   }
39   for (x = 2 ; x <= 10000 ; ++x) {
40     std::cout << x << " -> pi(x) " << stocke[x] ;
41     std::cout << "  moebius(x) " << moebius(x) << "\n" ;
42   }
43   std::ifstream fichier("Li10000", std::ios::in);
44   if (fichier) {
45     float flotte ;
46
47     i = 2 ;
48     while (not fichier.eof()) {
49       fichier >> flotte ;
50       logainte[i] = flotte ;
51       std::cout << "li(" << i << ") = " << logainte[i] << "\n" ;
52       i = i+1 ;
53     }
54     fichier.close();
55   }
56   else std::cerr << "Impossible dâouvrir le fichier !" << std::endl ;
57   for (x = 2 ; x <= 10000 ; ++x) {
58      std::cout << x << " --> " ;
59     cumul = (float) logainte[x] ;
60     for (k = 2 ; k <= x ; ++k)
61       cumul = cumul+((float) moebius(k) /(float) k)*(logainte[(int) pow(x, 1./k)]) ;
62     std::cout << cumul << "\n" ;
63   }
64 }
```

Annexe 2 : quelques valeurs de racines n-ièmes

x	500	1000	2000	5000	10000	20000	50000	100000	200000	500000	995907	10^6	10^9
$\sqrt[2]{x}$	22.3607	31.6228	44.7214	70.7107	100	141.421	223.607	316.228	447.214	707.107	997.951	1000	31622.8
$\sqrt[3]{x}$	7.93701	10	12.5992	17.0998	21.5443	27.1442	36.8403	46.4159	58.4804	79.3701	99.8634	100	1000
$\sqrt[4]{x}$	4.72871	5.62341	6.6874	8.40896	10	11.8921	14.9535	17.7828	21.1474	26.5915	31.5904	31.6228	177.828
$\sqrt[5]{x}$	3.46572	3.98107	4.57305	5.4928	6.30957	7.2478	8.70551	10	11.487	13.7973	15.8359	15.8489	63.0957
$\sqrt[6]{x}$	2.81727	3.16228	3.54954	4.13519	4.64159	5.21001	6.06962	6.81292	7.64724	8.90899	9.99317	10	31.6228
$\sqrt[7]{x}$	2.42978	2.6827	2.96194	3.37617	3.72759	4.1156	4.69117	5.17947	5.7186	6.51836	7.19264	7.19686	19.307
$\sqrt[8]{x}$	2.17456	2.37137	2.586	2.89982	3.16228	3.44849	3.86697	4.21697	4.59863	5.15669	5.62053	5.62341	13.3352
$\sqrt[9]{x}$	1.99474	2.15443	2.32692	2.5763	2.78256	3.00533	3.32742	3.59381	3.88153	4.29753	4.63947	4.64159	10
$\sqrt[10]{x}$		1.99526	2.13847	2.34367	2.51189	2.69217	2.95051	3.16228	3.38925	3.71447	3.97944	3.98107	7.94328
$\sqrt[11]{x}$			1.99569	2.16905	2.31013	2.46038	2.67411	2.84804	3.03328	3.29677	3.50988	3.51119	6.57933
$\sqrt[12]{x}$				2.03352	2.15443	2.28254	2.46366	2.61016	2.76537	2.98479	3.1612	3.16228	5.62341
$\sqrt[13]{x}$				1.92547	2.03092	2.14214	2.29858	2.42446	2.55724	2.74399	2.89335	2.89427	4.92388
$\sqrt[14]{x}$					1.9307	2.02869	2.16591	2.27585	2.39136	2.55311	2.68191	2.6827	4.39397
$\sqrt[15]{x}$						1.93524	2.05714	2.15443	2.25633	2.39845	2.5112	2.51189	3.98107
$\sqrt[16]{x}$							1.96646	2.05353	2.14444	2.27084	2.37077	2.37137	3.65174
$\sqrt[17]{x}$								1.96842	2.05034	2.16388	2.25339	2.25393	3.38386
$\sqrt[18]{x}$									1.97016	2.07305	2.15394	2.15443	3.16228
$\sqrt[19]{x}$										1.99501	2.06869	2.06914	2.97635
$\sqrt[20]{x}$											1.99485	1.99526	2.81838
$\sqrt[21]{x}$													2.6827
$\sqrt[22]{x}$													2.56502
$\sqrt[23]{x}$													2.46209
$\sqrt[24]{x}$													2.37137
$\sqrt[25]{x}$													2.29087
$\sqrt[26]{x}$													2.21898
$\sqrt[27]{x}$													2.15443
$\sqrt[28]{x}$													2.09618
$\sqrt[29]{x}$													2.04336
$\sqrt[30]{x}$													1.99526

Annexe 3 : Valeurs intermédiaires dans les calculs des formules 1 et 3 pour 995907

res = 78199.0.
+(1.0/2.0)*168.0 → 78283.00000
+ (1.0/3.0) ∗ 25.0 → 78291.33333
+ (1.0/4.0) ∗ 11.0 → 78294.08333
+ (1.0/5.0) ∗ 6.0 → 78295.28333
+ (1.0/6.0) ∗ 4.0 → 78295.95000
+ (1.0/7.0) ∗ 4.0 → 78296.52143
+ (1.0/8.0) ∗ 3.0 → 78296.89643
+ (1.0/9.0) ∗ 2.0 → 78297.11865
+ (1.0/10.0) ∗ 2.0 → 78297.31865
+ (1.0/11.0) ∗ 2.0 → 78297.50047
+ (1.0/12.0) ∗ 2.0 → 78297.66714
+ (1.0/13.0) ∗ 1.0 → 78297.74406
+ (1.0/14.0) ∗ 1.0 → 78297.81549
+ (1.0/15.0) ∗ 1.0 → 78297.88215
+ (1.0/16.0) ∗ 1.0 → 78297.94465
+ (1.0/17.0) ∗ 1.0 → 78298.00348
+ (1.0/18.0) ∗ 1.0 → 78298.05903
+ (1.0/19.0) ∗ 1.0 → 78298.11166
$formule\ 1\ \rightarrow\ 78298.11166$

res = 78330.198822562036 (=li(995907)-li(2)).
−(1.0/2.0)*176.268 → 78242.06482
− (1.0/3.0) ∗ 29.0513 → 78232.38106
− (1.0/5.0) ∗ 7.41526 → 78230.89800
+ (1.0/6.0) ∗ 5.11747 → 78231.75092
− (1.0/7.0) ∗ 3.8102 → 78231.20660
+ (1.0/10.0) ∗ 1.90756 → 78231.39736
− (1.0/11.0) ∗ 1.55148 → 78231.25631
− (1.0/13.0) ∗ 1.101972 → 78231.17155
+ (1.0/14.0) ∗ 0.813336 → 78231.22964
+ (1.0/15.0) ∗ 0.634324 → 78231.27193
− (1.0/17.0) ∗ 0.336776 → 78231.25212
− (1.0/19.0) ∗ 0.0967475 → 78231.24703
$formule\ 3\ \rightarrow\ 78231.24703$

Annexe 4 : Valeurs intermédiaires dans les calculs des formules 1 et 3 pour 10^6

res = 78627.549159.
+(1.0/2.0)*168.0 → 78711.54916
+ (1.0/3.0) ∗ 25.0 → 78719.88249
+ (1.0/4.0) ∗ 11.0 → 78722.63249
+ (1.0/5.0) ∗ 6.0 → 78723.83249
+ (1.0/6.0) ∗ 4.0 → 78724.49916
+ (1.0/7.0) ∗ 4.0 → 78725.07059
+ (1.0/8.0) ∗ 3.0 → 78725.44559
+ (1.0/9.0) ∗ 2.0 → 78725.66781
+ (1.0/10.0) ∗ 2.0 → 78725.86781
+ (1.0/11.0) ∗ 2.0 → 78726.04963
+ (1.0/12.0) ∗ 2.0 → 78726.21629
+ (1.0/13.0) ∗ 1.0 → 78726.29322
+ (1.0/14.0) ∗ 1.0 → 78726.36465
+ (1.0/15.0) ∗ 1.0 → 78726.43131
+ (1.0/16.0) ∗ 1.0 → 78726.49381
+ (1.0/17.0) ∗ 1.0 → 78726.55264
+ (1.0/18.0) ∗ 1.0 → 78726.60819
+ (1.0/19.0) ∗ 1.0 → 78726.66082
$formule\ 1\ \rightarrow\ 78726.66082$

res = 78627.549159 (=li(1000000)-li(2)).
$-(1.0/2.0)$*176.56449 $\rightarrow$ 78539.26691
$-\ (1.0/3.0) * 29.080977 \rightarrow 78529.57326$
$-\ (1.0/5.0) * 7.41996 \rightarrow 78528.08926$
$+\ (1.0/6.0) * 5.120435 \rightarrow 78528.94267$
$-\ (1.0/7.0) * 3.81234 \rightarrow 78528.39805$
$+\ (1.0/10.0) * 1.90874 \rightarrow 78528.58892$
$-\ (1.0/11.0) * 1.55252 \rightarrow 78528.44778$
$-\ (1.0/13.0) * 1.02059 \rightarrow 78528.36928$
$+\ (1.0/14.0) * 0.814136 \rightarrow 78528.42743$
$+\ (1.0/15.0) * 0.635074 \rightarrow 78528.46977$
$-\ (1.0/17.0) * 0.33744 \rightarrow 78528.44992$
$-\ (1.0/19.0) * 0.0973665 \rightarrow 78528.44479$
$formule\ 3\ \rightarrow\ 78528.44479$

Annexe 5 : Valeurs intermédiaires dans les calculs des formules 1 et 3 pour 10^7

res = 664579.0.
$+(1.0/2.0)$*446.0 $\rightarrow$ 664802.00000
$+\ (1.0/3.0) * 47.0 \rightarrow 664817.66667$
$+\ (1.0/4.0) * 25.0 \rightarrow 664823.91667$
$+\ (1.0/5.0) * 9.0 \rightarrow 664825.71667$
$+\ (1.0/6.0) * 6.0 \rightarrow 664826.71667$
$+\ (1.0/7.0) * 4.0 \rightarrow 664827.28810$
$+\ (1.0/8.0) * 4.0 \rightarrow 664827.78810$
$+\ (1.0/9.0) * 4.0 \rightarrow 664828.23254$
$+\ (1.0/10.0) * 3.0 \rightarrow 664828.53254$
$+\ (1.0/11.0) * 2.0 \rightarrow 664828.71436$
$+\ (1.0/12.0) * 2.0 \rightarrow 664828.88102$
$+\ (1.0/13.0) * 2.0 \rightarrow 664829.03487$
$+\ (1.0/14.0) * 2.0 \rightarrow 664829.17773$
$+\ (1.0/15.0) * 1.0 \rightarrow 664829.24439$
$+\ (1.0/16.0) * 1.0 \rightarrow 664829.30689$
$+\ (1.0/17.0) * 1.0 \rightarrow 664829.36572$
$+\ (1.0/18.0) * 1.0 \rightarrow 664829.42127$
$+\ (1.0/19.0) * 1.0 \rightarrow 664829.47391$
$+\ (1.0/20.0) * 1.0 \rightarrow 664829.52391$
$+\ (1.0/21.0) * 1.0 \rightarrow 664829.57152$
$+\ (1.0/22.0) * 1.0 \rightarrow 664829.61698$
$+\ (1.0/23.0) * 1.0 \rightarrow 664829.66046$
$formule\ 1\ \rightarrow\ 664829.66046$

res = 664917.359884 (=li(10000000)-li(2)).
$-(1.0/2.0)$*461.916 $\rightarrow$ 664686.40188
$-\ (1.0/3.0) * 52.0412 \rightarrow 664669.05482$
$-\ (1.0/5.0) * 10.5047 \rightarrow 664666.95388$
$+\ (1.0/6.0) * 6.99028 \rightarrow 664668.11892$
$-\ (1.0/7.0) * 5.12043572 \rightarrow 664667.38743$
$+\ (1.0/10.0) * 2.59679 \rightarrow 664667.64711$
$-\ (1.0/11.0) * 2.15298 \rightarrow 664667.45139$
$-\ (1.0/13.0) * 1.50758 \rightarrow 664667.33542$
$+\ (1.0/14.0) * 1.26268 \rightarrow 664667.42561$
$+\ (1.0/15.0) * 1.05275 \rightarrow 664667.49579$
$-\ (1.0/17.0) * 0.708872 \rightarrow 664667.45410$
$-\ (1.0/19.0) * 0.435926 \rightarrow 664667.43115$
$+\ (1.0/21.0) * 0.2115 \rightarrow 664667.44122$
$+\ (1.0/22.0) * 0.113026 \rightarrow 664667.44636$
$-\ (1.0/23.0) * 0.0220097 \rightarrow 664667.44540$
$formule\ 3\ \rightarrow\ 664667.44540$

Annexe 6 : Valeurs intermédiaires dans les calculs des formules 1 et 3 pour 10^8

res = 5761455.0.
+(1.0/2.0)*168.0 → 5761539.00000
+ (1.0/3.0) ∗ 25.0 → 5761547.33333
+ (1.0/4.0) ∗ 11.0 → 5761550.08333
+ (1.0/5.0) ∗ 6.0 → 5761551.28333
+ (1.0/6.0) ∗ 4.0 → 5761551.95000
+ (1.0/7.0) ∗ 4.0 → 5761552.52143
+ (1.0/8.0) ∗ 3.0 → 5761552.89643
+ (1.0/9.0) ∗ 2.0 → 5761553.11865
+ (1.0/10.0) ∗ 2.0 → 5761553.31865
+ (1.0/11.0) ∗ 2.0 → 5761553.50047
+ (1.0/12.0) ∗ 2.0 → 5761553.66714
+ (1.0/13.0) ∗ 1.0 → 5761553.74406
+ (1.0/14.0) ∗ 1.0 → 5761553.81549
+ (1.0/15.0) ∗ 1.0 → 5761553.88215
+ (1.0/16.0) ∗ 1.0 → 5761553.94465
+ (1.0/17.0) ∗ 1.0 → 5761554.00348
+ (1.0/18.0) ∗ 1.0 → 5761554.05903
+ (1.0/19.0) ∗ 1.0 → 5761554.11166
$formule\ 1\ \rightarrow\ 5761554.11166$

res = 5762208.330284 (=li(100000000)-li(2)).
−(1.0/2.0)*1245.0920 → 5761585.78428
− (1.0/3.0) ∗ 94.9471 → 5761554.13525
− (1.0/5.0) ∗ 14.743 → 5761551.18665
+ (1.0/6.0) ∗ 9.36926 → 5761552.74819
− (1.0/7.0) ∗ 6.69582 → 5761551.79165
+ (1.0/10.0) ∗ 3.34743 → 5761552.12639
− (1.0/11.0) ∗ 2.79446 → 5761551.87235
− (1.0/13.0) ∗ 2.01134 → 5761551.71763
+ (1.0/14.0) ∗ 1.72081 → 5761551.84055
+ (1.0/15.0) ∗ 1.47471 → 5761551.93886
− (1.0/17.0) ∗ 1.07737 → 5761551.87549
− (1.0/19.0) ∗ 0.767058 → 5761551.83511
− (1.0/21.0) ∗ 0.515185 → 5761551.81058
− (1.0/22.0) ∗ 0.405563 → 5761551.79215
− (1.0/23.0) ∗ 0.304730 → 5761551.77890
− (1.0/26.0) ∗ 0.0441204 → 5761551.77720
$formule\ 3\ \rightarrow\ 5761551.77720$

Annexe 7 : Valeurs intermédiaires dans les calculs des formules 1 et 3 pour 10^9

res = 50847534.0.
+(1.0/2.0)*168.0 → 50847618.00000
+ (1.0/3.0) ∗ 25.0 → 50847626.33333
+ (1.0/4.0) ∗ 11.0 → 50847629.08333
+ (1.0/5.0) ∗ 6.0 → 50847630.28333
+ (1.0/6.0) ∗ 4.0 → 50847630.95000
+ (1.0/7.0) ∗ 4.0 → 50847631.52143
+ (1.0/8.0) ∗ 3.0 → 50847631.89643
+ (1.0/9.0) ∗ 2.0 → 50847632.11865
+ (1.0/10.0) ∗ 2.0 → 50847632.31865
+ (1.0/11.0) ∗ 2.0 → 50847632.50047
+ (1.0/12.0) ∗ 2.0 → 50847632.66714
+ (1.0/13.0) ∗ 1.0 → 50847632.74406
+ (1.0/14.0) ∗ 1.0 → 50847632.81549
+ (1.0/15.0) ∗ 1.0 → 50847632.88215
+ (1.0/16.0) ∗ 1.0 → 50847632.94465
+ (1.0/17.0) ∗ 1.0 → 50847633.00348
+ (1.0/18.0) ∗ 1.0 → 50847633.05903

$+ (1.0/19.0) * 1.0 \rightarrow 50847633.11166$
$formule\ 1\ \rightarrow\ 50847633.11166$

res = 50849233.911838 (=li(1000000000)-li(2)).
$-(1.0/2.0)$*3432.87 $\rightarrow$ 50847517.47684
$- (1.0/3.0) * 176.5644942 \rightarrow 50847458.62201$
$- (1.0/5.0) * 20.6717 \rightarrow 50847454.48767$
$+ (1.0/6.0) * 12.4509 \rightarrow 50847456.56282$
$- (1.0/7.0) * 8.62744 \rightarrow 50847455.33033$
$+ (1.0/10.0) * 4.18123 \rightarrow 50847455.74845$
$- (1.0/11.0) * 3.49223 \rightarrow 50847455.43097$
$- (1.0/13.0) * 2.5419 \rightarrow 50847455.23544$
$+ (1.0/14.0) * 2.19725 \rightarrow 50847455.39239$
$+ (1.0/15.0) * 1.90874 =\rightarrow 50847455.51964$
$- (1.0/17.0) * 1.44963 \rightarrow 50847455.43437$
$- (1.0/19.0) * 1.09682 \rightarrow 50847455.37664$
$- (1.0/21.0) * 0.814136 \rightarrow 50847455.33787$
$- (1.0/22.0) * 0.692111 \rightarrow 50847455.30641$
$- (1.0/23.0) * 0.58041 \rightarrow 50847455.28117$
$- (1.0/26.0) * 0.294016 \rightarrow 50847455.26987$
$- (1.0/29.0) * 0.0616036 \rightarrow 50847455.26774$
$formule\ 3\ \rightarrow\ 50847455.26774$

Suite des calculs des formules de Riemann (Denise Vella-Chemla, 7.7.2017)

On étudie ici les calculs de la formule 2) ci-dessous fournie dans l'article que Riemann a consacré au nombre de nombres premiers pour les nombres 995 907, 10^6, 10^7, 10^8, 10^9.

$$1)\ \ f(x) = \pi(x) + \frac{1}{2}\pi\left(x^{\frac{1}{2}}\right) + \frac{1}{3}\pi\left(x^{\frac{1}{3}}\right) + \frac{1}{4}\pi\left(x^{\frac{1}{4}}\right) + \frac{1}{5}\pi\left(x^{\frac{1}{5}}\right) + \ldots$$

$$2)\ \ \pi(x) = \frac{\mu(2)}{2}f\left(x^{\frac{1}{2}}\right) + \frac{\mu(3)}{3}f\left(x^{\frac{1}{3}}\right) + \frac{\mu(4)}{4}f\left(x^{\frac{1}{4}}\right) + \frac{\mu(5)}{5}f\left(x^{\frac{1}{5}}\right) + \ldots = \sum \frac{\mu(k)}{k}f\left(x^{\frac{1}{k}}\right)$$

La formule 2) utilise les valeurs de f calculées au préalable qu'on fournit dans le tableau ci-après en regard des racines k-ièmes des nombres choisis (à gauche de la flèche dans chaque case, la racine k-ième, à droite, son image par f).

f	$\sqrt[2]{x}$		$\sqrt[3]{x}$		$\sqrt[5]{x}$		$\sqrt[6]{x}$		$\sqrt[7]{x}$		$\sqrt[10]{x}$	
995 907	997.951	$\to 176$	99.8634	$\to 28$	15.8359	$\to 7$	9.99317	$\to 5$	7.19264	$\to 4$	3.97944	$\to 2$
10^6	1000	$\to 176$	100	$\to 28$	15.8489	$\to 7$	10	$\to 5$	7.19686	$\to 4$	3.98107	$\to 2$
10^7	3162.28	$\to 458$	215.443	$\to 52$	25.1189	$\to 11$	14.678	$\to 7$	10	$\to 5$	5.01187	$\to 3$
10^8	10000	$\to 1247$	464.159	$\to 96$	39.8107	$\to 14$	21.5443	$\to 9$	13.895	$\to 7$	6.30957	$\to 3$
10^9	31622.8	$\to 3428$	1000	$\to 176$	63.0957	$\to 21$	31.6228	$\to 13$	19.307	$\to 9$	7.94328	$\to 4$
f	$\sqrt[11]{x}$		$\sqrt[13]{x}$		$\sqrt[14]{x}$		$\sqrt[15]{x}$		$\sqrt[17]{x}$		$\sqrt[19]{x}$	
995 907	3.50988	$\to 2$	2.89335	1	2.68191	$\to 1$	2.5112	$\to 1$	2.25339	$\to 1$	2.06869	$\to 1$
10^6	3.51119	$\to 2$	2.89427	$\to 1$	2.6827	$\to 1$	2.51189	$\to 1$	2.25393	$\to 1$	2.06914	$\to 1$
10^7	4.32876	$\to 2$	3.45511	$\to 2$	3.16228	$\to 1$	2.92864	$\to 1$	2.58086	$\to 1$	2.33572	$\to 1$
10^8	5.3356	$\to 3$	4.12463	$\to 2$	3.72759	$\to 2$	3.41455	$\to 2$	2.95521	$\to 1$	2.63665	$\to 1$
10^9	6.57933	$\to 3$	4.92388	$\to 2$	4.39397	$\to 2$	3.98107	$\to 2$	3.38386	$\to 2$	2.97635	$\to 1$
f	$\sqrt[21]{x}$		$\sqrt[22]{x}$		$\sqrt[23]{x}$		$\sqrt[26]{x}$		$\sqrt[29]{x}$			
995 907	–		–		–		–		–			
10^6	–		–		–		–		–			
10^7	2.15443	$\to 1$	2.08057	$\to 1$	2.01534	$\to 1$	–		–			
10^8	2.4041	$\to 1$	2.31013	$\to 1$	2.22754	$\to 1$	2.03092	$\to 1$	–			
10^9	2.6827	$\to 1$	2.56502	$\to 1$	2.46209	$\to 1$	2.21898	$\to 1$	2.04336	$\to 1$		

La fonction de Moebius "équilibre" à peu près les ajouts et les soustractions.

x	$\pi(x)$	$formule\ 2)$
995 907	78 262	78 199
1 000 000	78 498	78 627
10 000 000	664 579	664 555
100 000 000	5 761 455	5 760 896
1 000 000 000	50 847 534	50 845 856

Ci-dessous, le tableau des écarts à $\pi(x)$, plus parlant :

x	$\pi(x)$	$formule\ 2(x) - \pi(x)$
995 907	78 262	-63
1 000 000	78 498	$+129$
10 000 000	664 579	-24
100 000 000	5 761 455	-559
1 000 000 000	50 847 534	-1678

Ci-dessous les valeurs calculées au fur et à mesure de l'application de la formule 2 pour les nombres choisis.

Valeurs intermédiaires dans les calculs de la formule 2 pour 995907

res = 78 298 (= f(995907)).
$-(1.0/2.0)$*176 $\to$ 78210.00000
$-\ (1.0/3.0) * 28 \to 78200.66667$
$-\ (1.0/5.0) * 7 \to 78199.26667$
$+\ (1.0/6.0) * 5 \to 78200.10000$
$-\ (1.0/7.0) * 4 \to 78199.52857$

$+ (1.0/10.0) * 2 \rightarrow 78199.72857$
$- (1.0/11.0) * 2 \rightarrow 78199.54675$
$- (1.0/13.0) * 1 \rightarrow 78199.46983$
$+ (1.0/14.0) * 1 \rightarrow 78199.54126$
$+ (1.0/15.0) * 1 \rightarrow 78199.60793$
$- (1.0/17.0) * 1 \rightarrow 78199.54910$
$- (1.0/19.0) * 1 \rightarrow 78199.49647$
$formule\ 2\ \rightarrow\ 78199.49647$

Valeurs intermédiaires dans les calculs de la formule 2 pour 10^6

res = 78 726 (= f(10^6)).
$-(1.0/2.0) * 176 \rightarrow 78638.00000$
$- (1.0/3.0) * 28 \rightarrow 78628.66667$
$- (1.0/5.0) * 7 \rightarrow 78627.26667$
$+ (1.0/6.0) * 5 \rightarrow 78628.10000$
$- (1.0/7.0) * 4 \rightarrow 78627.52857$
$+ (1.0/10.0) * 2 \rightarrow 78627.72857$
$- (1.0/11.0) * 2 \rightarrow 78627.54675$
$- (1.0/13.0) * 1 \rightarrow 78627.46983$
$+ (1.0/14.0) * 1 \rightarrow 78627.54126$
$+ (1.0/15.0) * 1 \rightarrow 78627.60793$
$- (1.0/17.0) * 1 \rightarrow 78627.54910$
$- (1.0/19.0) * 1 \rightarrow 78627.49647$
formule 2 $\rightarrow$ 78627.49647

Valeurs intermédiaires dans les calculs de la formule 2 pour 10^7

res = 664 829 (= f(10^7)).
$-(1.0/2.0) * 458 \rightarrow 664600.00000$
$- (1.0/3.0) * 128 \rightarrow 664557.33333$
$- (1.0/5.0) * 11 \rightarrow 664555.13333$
$+ (1.0/6.0) * 7 \rightarrow 664556.30000$
$- (1.0/7.0) * 5 \rightarrow 664555.58571$
$+ (1.0/10.0) * 4 \rightarrow 664555.98571$
$- (1.0/11.0) * 2 \rightarrow 664555.80390$
$- (1.0/13.0) * 2 \rightarrow 664555.65005$
$+ (1.0/14.0) * 1 \rightarrow 664555.72148$
$+ (1.0/15.0) * 1 \rightarrow 664555.78815$
$- (1.0/17.0) * 1 \rightarrow 664555.72932$
$- (1.0/19.0) * 1 \rightarrow 664555.67669$
$+ (1.0/21.0) * 1 \rightarrow 664555.72431$
$+ (1.0/22.0) * 1 \rightarrow 664555.76976$
$- (1.0/23.0) * 1 \rightarrow 664555.72629$
formule 2 $\rightarrow$ 664555.72629

Valeurs intermédiaires dans les calculs de la formule 2 pour 10^8

res = 5 761 554 (= f(10^8)).
$-(1.0/2.0) * 1247 \rightarrow 5760930.50000$
$- (1.0/3.0) * 96 \rightarrow 5760898.50000$
$- (1.0/5.0) * 14 \rightarrow 5760895.70000$
$+ (1.0/6.0) * 9 \rightarrow 5760897.20000$
$- (1.0/7.0) * 7 \rightarrow 5760896.20000$
$+ (1.0/10.0) * 3 \rightarrow 5760896.50000$
$- (1.0/11.0) * 3 \rightarrow 5760896.22727$
$- (1.0/13.0) * 2 \rightarrow 5760896.07343$
$+ (1.0/14.0) * 2 \rightarrow 5760896.21628$
$+ (1.0/15.0) * 2 \rightarrow 5760896.34962$
$- (1.0/17.0) * 1 \rightarrow 5760896.29079$
$- (1.0/19.0) * 1 \rightarrow 5760896.23816$
$- (1.0/21.0) * 1 \rightarrow 5760896.19054$

$-(1.0/22.0)*1 \to 5760896.14509$
$-(1.0/23.0)*1 \to 5760896.10161$
$-(1.0/26.0)*1 \to 5760896.06315$
formule 2 $\to$ 5760896.06315

Valeurs intermédiaires dans les calculs de la formule 2 pour 10^9

res = 50 847 633 $(= \mathrm{f}(10^9))$.
$-(1.0/2.0)*3428 \to 50845919.00000$
$-(1.0/3.0)*176 \to 50845860.33333$
$-(1.0/5.0)*21 \to 50845856.13333$
$+(1.0/6.0)*13 \to 50845858.30000$
$-(1.0/7.0)*9 \to 50845857.01429$
$+(1.0/10.0)*4 \to 50845857.41429$
$-(1.0/11.0)*3 \to 50845857.14156$
$-(1.0/13.0)*2 \to 50845856.98771$
$+(1.0/14.0)*2 \to 50845857.13057$
$+(1.0/15.0)*2 \to 50845857.26390$
$-(1.0/17.0)*2 \to 50845857.14626$
$-(1.0/19.0)*1 \to 50845857.09362$
$-(1.0/21.0)*1 \to 50845857.04601$
$-(1.0/22.0)*1 \to 50845857.00055$
$-(1.0/23.0)*1 \to 50845856.95707$
$-(1.0/26.0)*1 \to 50845856.91861$
$-(1.0/29.0)*1 \to 50845856.88413$
formule 2 $\to$ 50845856.88413

Concernant le dernier paragraphe de l'article de Bernhard Riemann :

> *"Il serait intéressant dans un nouveau dénombrement, d'étudier l'influence de chaque terme périodique*[1] *contenu dans l'expression donnée pour la totalité des nombres premiers. Une marche plus régulière que celle donnée par $F(x)$ serait obtenue à l'aide de la fonction $f(x)$ qui, cela se reconnaît déjà très évidemment dans la première centaine, coïncide en moyenne avec $Li(x) + log\ \xi(0)$.",*

il s'agit de comparer $Li(x)$ et $f(x)$ dont on rappelle quelques valeurs :

x	$f(x)$	$Li(x)$	$Li(x) - f(x)$
500	101	101	0
10^3	176	177	1
2.10^3	313	314	1
5.10^3	683	684	1
10^4	1247	1245	-2
2.10^4	2285	2288	3
5.10^4	5164	5165	1
10^5	9633	9629	-4
2.10^5	18037	18035	-2
5.10^5	41614	41606	-8
995 907	78 298	78 332	34
10^6	78 726	78 627	-99
10^7	664 829	664 917	88
10^8	5 761 554	5 762 208	654
10^9	50 847 633	50 847 534	-99

Il faut peut-être, dans la comparaison "en moyenne", considérer, comme le fait le traducteur, que $log\ \xi(0)$ est une coquille typographique et doit prendre la valeur $\frac{1}{2}$, ou bien selon l'idée d'autres, remplacer $log\ \xi(0)$ par $li(2) = 1.045164$.

[1] selon le traducteur, penser ici oscillatoire plutôt que périodique.

Toujours est-il que le rapport $\frac{50\,847\,633}{50\,847\,534}$ pour $x = 10^9$ vaut 1.000001947 et que donc, puisque $f(x) = \pi(x) + \frac{1}{2}\pi\left(x^{\frac{1}{2}}\right) + \frac{1}{3}\pi\left(x^{\frac{1}{3}}\right) + \frac{1}{4}\pi\left(x^{\frac{1}{4}}\right) + \frac{1}{5}\pi\left(x^{\frac{1}{5}}\right) + \ldots$, il suffirait, si l'hypothèse de Riemann était démontrée, pour trouver quasi-exactement le nombre de nombres premiers inférieurs à x de calculer $Li(x) = li(x) - li(2)$ et de lui soustraire la moitié du nombre de nombres premiers inférieurs à la racine carrée de x, ainsi que le tiers du nombre de nombres premiers inférieurs à la racine cubique de x, ainsi que le quart du nombre de nombres premiers de la racine quatrième de x, en poursuivant les retraits jusqu'à la dernière racine k-ième de x supérieure ou égale à 2.

On vérifie cela avec le nombre 10^9 uniquement ; on calcule $\pi(x) = Li(x) - \sum \frac{1}{k}\pi(\sqrt[k]{x})$:

res = Li(10^9) = 50849233.0-(1.0/2.0) $*$ 3401.0 = 50847532.500000
$-$ (1.0/3.0) $*$ 168.0 = 50847476.500000
$-$ (1.0/4.0) $*$ 40.0 = 50847466.500000
$-$ (1.0/5.0) $*$ 18.0 = 50847462.900000
$-$ (1.0/6.0) $*$ 11.0 = 50847461.066667
$-$ (1.0/7.0) $*$ 8.0 = 50847459.923810
$-$ (1.0/8.0) $*$ 6.0 = 50847459.173810
$-$ (1.0/9.0) $*$ 4.0 = 50847458.729365
$-$ (1.0/10.0) $*$ 4.0 = 50847458.329365
$-$ (1.0/11.0) $*$ 3.0 = 50847458.056638
$-$ (1.0/12.0) $*$ 3.0 = 50847457.806638
$-$ (1.0/13.0) $*$ 2.0 = 50847457.652792
$-$ (1.0/14.0) $*$ 2.0 = 50847457.509935
$-$ (1.0/15.0) $*$ 2.0 = 50847457.376601
$-$ (1.0/16.0) $*$ 2.0 = 50847457.251601
$-$ (1.0/17.0) $*$ 2.0 = 50847457.133954
$-$ (1.0/18.0) $*$ 2.0 = 50847457.022843
$-$ (1.0/19.0) $*$ 1.0 = 50847456.970211
$-$ (1.0/20.0) $*$ 1.0 = 50847456.920211
$-$ (1.0/21.0) $*$ 1.0 = 50847456.872592
$-$ (1.0/22.0) $*$ 1.0 = 50847456.827138
$-$ (1.0/23.0) $*$ 1.0 = 50847456.783660
$-$ (1.0/24.0) $*$ 1.0 = 50847456.741993
$-$ (1.0/25.0) $*$ 1.0 = 50847456.701993
$-$ (1.0/26.0) $*$ 1.0 = 50847456.663531
$-$ (1.0/27.0) $*$ 1.0 = 50847456.626494
$-$ (1.0/28.0) $*$ 1.0 = 50847456.590780
$-$ (1.0/29.0) $*$ 1.0 = 50847456.556297

L'écart rapporté à $\pi(x)$ de la valeur finale obtenue $\frac{50847534 - 50847456}{50847534}$ est égal à 0.00000153098 mais dès la première soustraction, en ôtant simplement $\frac{1}{2}\pi(\sqrt{x})$, on a un écart aussi petit que $\frac{50847534 - 50847532}{50847534} = 3,93332743.10^{-8}$.

Annexe : autres résultats

Calculs pour 10^8

res = Li(10^8) = 5762208.0
− (1.0/2.0) ∗ 1229.0 = 5761593.500000
− (1.0/3.0) ∗ 90.0 = 5761563.500000
− (1.0/4.0) ∗ 25.0 = 5761557.250000
− (1.0/5.0) ∗ 12.0 = 5761554.850000
− (1.0/6.0) ∗ 8.0 = 5761553.516667
− (1.0/7.0) ∗ 6.0 = 5761552.659524
− (1.0/8.0) ∗ 4.0 = 5761552.159524
− (1.0/9.0) ∗ 4.0 = 5761551.715079
− (1.0/10.0) ∗ 3.0 = 5761551.415079
− (1.0/11.0) ∗ 3.0 = 5761551.142352
− (1.0/12.0) ∗ 2.0 = 5761550.975685
− (1.0/13.0) ∗ 2.0 = 5761550.821839
− (1.0/14.0) ∗ 2.0 = 5761550.678982
− (1.0/15.0) ∗ 2.0 = 5761550.545649
− (1.0/16.0) ∗ 2.0 = 5761550.420649
− (1.0/17.0) ∗ 1.0 = 5761550.361825
− (1.0/18.0) ∗ 1.0 = 5761550.306270
− (1.0/19.0) ∗ 1.0 = 5761550.253638
− (1.0/20.0) ∗ 1.0 = 5761550.203638
− (1.0/21.0) ∗ 1.0 = 5761550.156019
− (1.0/22.0) ∗ 1.0 = 5761550.110565
− (1.0/23.0) ∗ 1.0 = 5761550.067086
− (1.0/24.0) ∗ 1.0 = 5761550.025420
− (1.0/25.0) ∗ 1.0 = 5761549.985420
− (1.0/26.0) ∗ 1.0 = 5761549.946958

Erreur = $(5761455 - 5761593)/5761455 = 2,39.10^{-5}$ si on s'arrête à la racine carrée et qui tombe à $.10^{-}$ si on va au bout des calculs ((5761455-5761549)/5761455=$1,63.10^{-5}$).

Calculs pour 10^7

res = Li(10^7) = 664917.0
− (1.0/2.0) ∗ 446.0 = 664694.000000
− (1.0/3.0) ∗ 47.0 = 664678.333333
− (1.0/4.0) ∗ 16.0 = 664674.333333
− (1.0/5.0) ∗ 9.0 = 664672.533333
− (1.0/6.0) ∗ 6.0 = 664671.533333
− (1.0/7.0) ∗ 4.0 = 664670.961905
− (1.0/8.0) ∗ 4.0 = 664670.461905
− (1.0/9.0) ∗ 3.0 = 664670.128571
− (1.0/10.0) ∗ 3.0 = 664669.828571
− (1.0/11.0) ∗ 2.0 = 664669.646753
− (1.0/12.0) ∗ 2.0 = 664669.480087
− (1.0/13.0) ∗ 2.0 = 664669.326240
− (1.0/14.0) ∗ 2.0 = 664669.183383
− (1.0/15.0) ∗ 1.0 = 664669.116717
− (1.0/16.0) ∗ 1.0 = 664669.054217
− (1.0/17.0) ∗ 1.0 = 664668.995393
− (1.0/18.0) ∗ 1.0 = 664668.939838
− (1.0/19.0) ∗ 1.0 = 664668.887206
− (1.0/20.0) ∗ 1.0 = 664668.837206
− (1.0/21.0) ∗ 1.0 = 664668.789587
− (1.0/22.0) ∗ 1.0 = 664668.744132
− (1.0/23.0) ∗ 1.0 = 664668.700654

Erreur = $(664579 - 664694)/664579 = 1,73.10^{-4}$ si on s'arrête à la racine carrée et qui tombe à $1,33.10^{-4}$ si on va au bout des calculs (=(664579-664668)/664579).

Calculs pour 10^6

res = Li(10^6) = 78627.0
− (1.0/2.0) ∗ 168.0 = 78543.000000
− (1.0/3.0) ∗ 25.0 = 78534.666667
− (1.0/4.0) ∗ 11.0 = 78531.916667
− (1.0/5.0) ∗ 7.0 = 78530.516667
− (1.0/6.0) ∗ 4.0 = 78529.850000
− (1.0/7.0) ∗ 4.0 = 78529.278571
− (1.0/8.0) ∗ 3.0 = 78528.903571
− (1.0/9.0) ∗ 2.0 = 78528.681349
− (1.0/10.0) ∗ 2.0 = 78528.481349
− (1.0/11.0) ∗ 2.0 = 78528.299531
− (1.0/12.0) ∗ 2.0 = 78528.132864
− (1.0/13.0) ∗ 1.0 = 78528.055941
− (1.0/14.0) ∗ 1.0 = 78527.984513
− (1.0/15.0) ∗ 1.0 = 78527.917846
− (1.0/16.0) ∗ 1.0 = 78527.855346
− (1.0/17.0) ∗ 1.0 = 78527.796523
− (1.0/18.0) ∗ 1.0 = 78527.740967
− (1.0/19.0) ∗ 1.0 = 78527.688335

Erreur = $(78543 - 78498)/78498 = 5.10^{-4}$ si on s'arrête à la racine carrée et qui tombe à 3.10^{-4} si on va au bout des calculs (=(78527-78498)/78498).

Calculs pour 10^5

res = Li(10^5) = 9629.0
− (1.0/2.0) ∗ 25.0 = 9616.500000
− (1.0/3.0) ∗ 8.0 = 9613.833333
− (1.0/4.0) ∗ 4.0 = 9612.833333
− (1.0/5.0) ∗ 3.0 = 9612.233333
− (1.0/6.0) ∗ 2.0 = 9611.900000
− (1.0/7.0) ∗ 2.0 = 9611.614286
− (1.0/8.0) ∗ 2.0 = 9611.364286
− (1.0/9.0) ∗ 2.0 = 9611.142063
− (1.0/10.0) ∗ 2.0 = 9610.942063
− (1.0/11.0) ∗ 2.0 = 9610.760245
− (1.0/12.0) ∗ 2.0 = 9610.593579
− (1.0/13.0) ∗ 2.0 = 9610.439732

Erreur = $(9616 - 9592)/9592 = 2.10^-3$ si on s'arrête à la racine carrée et divisée par 2 si on va au bout des calculs.

Calculs pour 10^4

res = Li(10^4) = 1245.0
− (1.0/2.0) ∗ 25.0 = 1232.500000
− (1.0/3.0) ∗ 8.0 = 1229.833333
− (1.0/4.0) ∗ 4.0 = 1228.833333
− (1.0/5.0) ∗ 3.0 = 1228.233333
− (1.0/6.0) ∗ 2.0 = 1227.900000
− (1.0/7.0) ∗ 2.0 = 1227.614286
− (1.0/8.0) ∗ 2.0 = 1227.364286
− (1.0/9.0) ∗ 1.0 = 1227.253175
− (1.0/10.0) ∗ 1.0 = 1227.153175
− (1.0/11.0) ∗ 1.0 = 1227.062266
− (1.0/12.0) ∗ 1.0 = 1226.978932
− (1.0/13.0) ∗ 1.0 = 1226.902009

Erreur = $(1232 - 1229)/1229 = 2.10^{-3}$ si on s'arrête à la racine carrée et qui reste à 2.10^{-3} (en négatif) si on va au bout des calculs (=(1226-1229)/1229).

Calculs pour 10^3

res = $\mathrm{Li}(10^3) = 177.0$
$-\ (1.0/2.0) * 31.0 = 161.500000$
$-\ (1.0/3.0) * 4.0 = 160.166667$
$-\ (1.0/4.0) * 3.0 = 159.416667$
$-\ (1.0/5.0) * 2.0 = 159.016667$
$-\ (1.0/6.0) * 2.0 = 158.683333$
$-\ (1.0/7.0) * 1.0 = 158.540476$
$-\ (1.0/8.0) * 1.0 = 158.415476$
$-\ (1.0/9.0) * 1.0 = 158.304365$

Erreur $= (161 - 168)/168 = -4.10^{-2}$ si on s'arrête à la racine carrée et qui devient -5.10^{-2} si on va au bout des calculs (=(158-168)/168).

Emerveillement (Denise Vella-Chemla, 8.7.2017)

Après avoir étudié la note de Bernhard Riemann *"Sur le nombre des nombres premiers inférieurs à une grandeur donnée"* et en avoir programmé quelques formules, on aboutit au programme suivant, en C++, qui résume toute la puissance de la fonction Logarithme intégral $Li(x)$, qui permet l'obtention d'une excellente approximation du nombre de nombres premiers inférieurs à un nombre donné à partir de son logarithme intégral auquel on soustrait la moitié du nombre de nombres premiers inférieurs à sa racine carrée.

Présentons les résultats que l'on peut obtenir par programme (la colonne dans laquelle on soustrait directement le nombre de nombres premiers inférieurs à la racine du nombre considéré plutôt que la moitié d'un tel nombre est dû au fait d'une coquille de programmation initiale qui montre que l'une ou l'autre des possibilités donnent des résultats semblables (du moins jusqu'à 10^9).

x	$Li(x)$	$\sqrt{x}$	$\pi(\sqrt{x})$	$\pi(x)$	$Li(x) - \pi(\sqrt{x})$	$Li(x) - (1/2)\pi(\sqrt{x})$
10^2	29	10	4	25	25	27
10^3	177	31	11	168	166	172
10^4	1 245	100	25	1 229	1 220	1 233
10^5	9 629	316	65	9 592	9 564	9 597
10^6	78 627	1 000	168	78 498	78 459	78 543
10^7	664 917	3 162	446	664 579	664 471	664 694
10^8	5 762 208	10 000	1 229	5 761 455	5 760 979	5 761 594
10^9	50 849 233	31 622	3 401	50 847 534	50 845 832	50 847 533

Voici le tableau des écarts relatifs à $\pi(x)$.

x	$\frac{\pi(x)-(Li(x)-\pi(\sqrt{x})))}{\pi x}$	$\frac{\pi(x)-(Li(x)-\frac{1}{2}\pi(\sqrt{x})))}{\pi(x)}$
10^2	0	-0.08 ($= -2/25$)
10^3	0.0119 ($=$ 2/168)	0.0238 ($=$ 4/168)
10^4	0.0073 ($=$ 9/1 229)	0.003254 ($=$ 4/1 229)
10^5	0.0029 ($=$ 28/9 592)	0.00052126 ($=$ 5/9 592)
10^6	0.00049 ($=$ 39/78 498)	0.00057326 ($=$ 45/78 498)
10^7	0.000162 ($=$ 108/664 579)	0.000173041 ($=$ 115/664 579)
10^8	0.00008261 ($=$ 476/5 761 455)	0.000024125 ($=$ 139/5 761 455)
10^9	0.00000586065 ($=$ 298/50 847 534)	$1,96.10^{-8}$ ($=$ 1/50 847 533)

```cpp
#include <iostream>
#include <stdio.h>
#include <cmath>
#include <fstream>

int prime(int atester) {
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else
      if ((atester % k) == 0) return 0 ;
      else k++;
    }
}

int main (int argc, char* argv[]) {
  int n, i, nbpremiers ;
  float res, rac, nbpremrac ;
  float logainte[10010] ;

  std::ifstream fichier("petitlog", std::ios::in);
  if (fichier) {
    float flotte ;

    i = 2 ;
    while (not fichier.eof()) {
      fichier >> flotte ;
      logainte[i] = flotte-1.04516378011749 ;
      //std::cout << "li(" << i << ") = " << logainte[i] << "\n" ;
      i = i+1 ;
    }
    fichier.close();
  }
  else std::cerr << "Impossible d'ouvrir le fichier !" << std::endl ;

  for (n = 1 ; n <= 10000 ; ++n) {
    rac = sqrt(n) ;
    nbpremrac = 0 ;
    nbpremiers = 0 ;
    for (i = 2 ; i <= rac ; ++i) if (prime(i)) nbpremrac = nbpremrac+1 ;
    for (i = 2 ; i <= n ; ++i) if (prime(i)) nbpremiers = nbpremiers+1 ;
    res = logainte[n]-0.5*nbpremrac ;
    std::cout << n << " -> " << nbpremiers << " approx " << res ;
    std::cout << `` erreur = `` << (nbpremiers-res)/nbpremiers << ``\n'' ;
  }
}
```

Les premières et dernières lignes de l'exécution de ce programme sont :

```
3 -> 2 approx 1.11842 erreur 0.440788
4 -> 2 approx 1.42242 erreur 0.288789
5 -> 3 approx 2.08942 erreur 0.303525
6 -> 3 approx 2.67706 erreur 0.107647
7 -> 4 approx 3.21189 erreur 0.197028
8 -> 4 approx 3.70855 erreur 0.0728613
9 -> 4 approx 3.67607 erreur 0.0809815
10 -> 4 approx 4.12044 erreur -0.0301089
11 -> 5 approx 4.54585 erreur 0.0908309
12 -> 5 approx 4.95538 erreur 0.00892324
13 -> 6 approx 5.35138 erreur 0.108103
14 -> 6 approx 5.73566 erreur 0.0440563
15 -> 6 approx 6.10966 erreur -0.0182769
16 -> 6 approx 6.47455 erreur -0.0790921
17 -> 7 approx 6.8313 erreur 0.0240998
18 -> 7 approx 7.18071 erreur -0.0258157
19 -> 8 approx 7.52346 erreur 0.0595673
20 -> 8 approx 7.86014 erreur 0.017483
21 -> 8 approx 8.19123 erreur -0.0239042
22 -> 8 approx 8.51719 erreur -0.0646486
23 -> 9 approx 8.83838 erreur 0.0179575
24 -> 9 approx 9.15515 erreur -0.017239
25 -> 9 approx 8.96779 erreur 0.00357861
26 -> 9 approx 9.27657 erreur -0.03073
27 -> 9 approx 9.58172 erreur -0.0646358
28 -> 9 approx 9.88346 erreur -0.0981627
29 -> 10 approx 10.182 erreur -0.0181988
30 -> 10 approx 10.4775 erreur -0.0477468
31 -> 11 approx 10.7701 erreur 0.0209031
32 -> 11 approx 11.0599 erreur -0.00544799
33 -> 11 approx 11.3472 erreur -0.0315625


9971 -> 1228 approx 1229.44 erreur -0.00117498
9972 -> 1228 approx 1229.55 erreur -0.00126345
9973 -> 1229 approx 1229.66 erreur -0.000537149
9974 -> 1229 approx 1229.77 erreur -0.000625449
9975 -> 1229 approx 1229.88 erreur -0.000713848
9976 -> 1229 approx 1229.99 erreur -0.000802247
9977 -> 1229 approx 1230.09 erreur -0.000890646
9978 -> 1229 approx 1230.2 erreur -0.000978946
9979 -> 1229 approx 1230.31 erreur -0.00106735
9980 -> 1229 approx 1230.42 erreur -0.00115565
9981 -> 1229 approx 1230.53 erreur -0.00124404
9982 -> 1229 approx 1230.64 erreur -0.00133244
9983 -> 1229 approx 1230.75 erreur -0.00142074
9984 -> 1229 approx 1230.85 erreur -0.00150914
9985 -> 1229 approx 1230.96 erreur -0.00159744
9986 -> 1229 approx 1231.07 erreur -0.00168584
9987 -> 1229 approx 1231.18 erreur -0.00177424
9988 -> 1229 approx 1231.29 erreur -0.00186254
9989 -> 1229 approx 1231.4 erreur -0.00195094
9990 -> 1229 approx 1231.51 erreur -0.00203924
9991 -> 1229 approx 1231.61 erreur -0.00212764
9992 -> 1229 approx 1231.72 erreur -0.00221594
9993 -> 1229 approx 1231.83 erreur -0.00230434
9994 -> 1229 approx 1231.94 erreur -0.00239264
9995 -> 1229 approx 1232.05 erreur -0.00248104
9996 -> 1229 approx 1232.16 erreur -0.00256934
9997 -> 1229 approx 1232.27 erreur -0.00265774
9998 -> 1229 approx 1232.37 erreur -0.00274604
9999 -> 1229 approx 1232.48 erreur -0.00283443
10000 -> 1229 approx 1232.59 erreur -0.00292273
```

En python, le programme est plus court, et plus rapide à l'exécution :

```
import mpmath
from mpmath import *
from math import *

def prime(atester):
  pastrouve = True
  k = 2
  if (atester == 1): return False
  if (atester == 2): return True
  if (atester == 3): return True
  if (atester == 5): return True
  if (atester == 7): return True
  while (pastrouve):
    if ((k * k) > atester):
        return True
    else:
        if ((atester % k) == 0):
            return False
        else: k=k+1

def pi(x):
    nbpremiers = 0
    for y in range(1,x):
        if prime(y):
            nbpremiers=nbpremiers+1
    return nbpremiers

x=int(input())
res = li(x)-li(2)
a = pi(x)
print "pi(x) = %d" %a
b = int(sqrt(x))
c = pi(b)
res=res-(1.0/2.0)*c
print "res = %10.6f" %res
erreur = (res-a)/a
print "erreur = %10.6f" %erreur
```

Par exécution des programmes en python, on obtient les résultats suivants, légèrement différents de ceux obtenus en c++ : x = 100 pi(x) = 25
res = 27.080978
erreur = 0.083239

x = 1000 pi(x) = 168
res = 171.564494
erreur = 0.021217

x = 10000 pi(x) = 1229
res = 1232.592052
erreur = 0.002923

x = 100000 pi(x) = 9592
res = 9596.263837
erreur = 0.000445

x = 1000000 pi(x) = 78498
res = 78542.503996
erreur = 0.000567

x = 10000000 pi(x) = 664579
res = 664694.359885
erreur = 0.000174

x = 100000000 pi(x) = 5761455
res = 5761593.830284
erreur = 0.000024

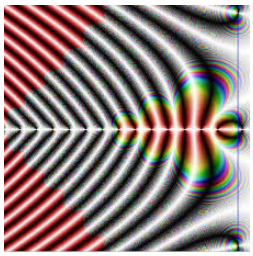
Référence

Traduction en français par L.Laugel in *Riemann, œuvres mathématiques*, Gauthier-Villars, 1898., de *Über die Anzahl der Primzahlen unter einer gegebenen Grösse, Monat. der Königl. Preuss. Akad. der Wissen. zu Berlin aus der Jahre 1859 (1860) 671-680.*

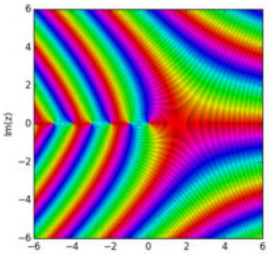
Petit memo (Denise Vella-Chemla, 11.7.2017)

• Γ d'Euler, c'est l'extension de la factorielle aux complexes ;

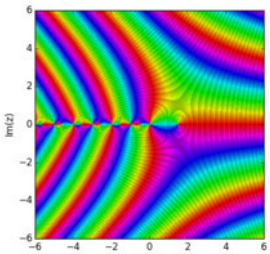
• c'est Γ qui semble donner sa forme à ζ ;



$\zeta(z)$



$\Gamma(z)$



$\Gamma'(z)$

• on cherche un opérateur qui envoie une fonction sur une fonction (l'intégration fait ça par exemple) ;

• calcul des raies d'un spectre d'absorption : on calcule les différences entre les fréquences de ses différentes raies et la fréquence de la raie d'émission, on obtient une équation de droite, ça permet de calculer les raies manquantes ;

• spirale logarithmique (équation $r = ae^{m\theta} = ab^{\theta}$ avec a réel, m réel non nul) ; la tangente fait un angle constant α avec tout rayon tel que $tan\ \alpha = \dfrac{1}{ln\ b}$; la longueur de tout arc est proportionnelle à OM (le rayon de la spirale) avec comme coefficient de proportionnalité $\dfrac{1}{cos\ \alpha} = 1 + \dfrac{1}{(ln\ b)^2}$ et du coup, si on fait rouler une spirale logarithmique sur sa tangente, son centre se déplace sur une droite faisant avec la tangente un angle constant valant $\dfrac{\pi}{2} - \alpha$; et d'autre part, l'aire balayée est proportionnelle au carré du rayon selon un coefficient de proportionnalité de $\dfrac{1}{4\ ln\ b}$;

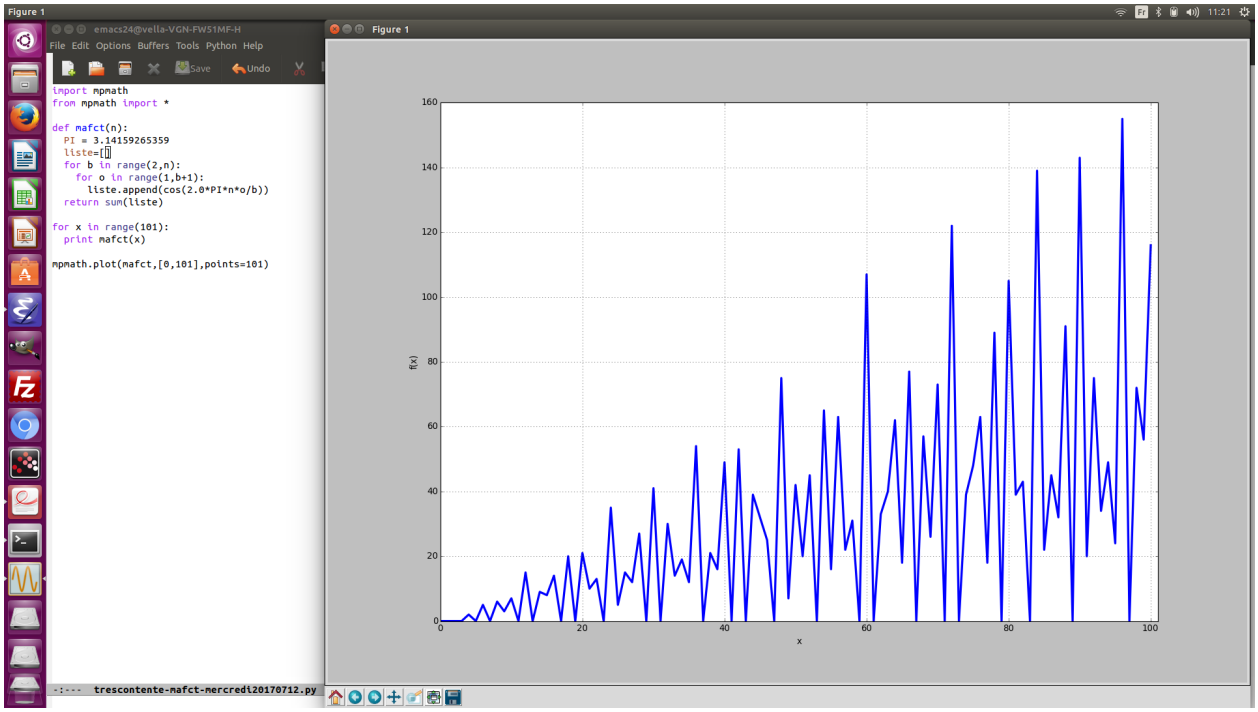
• moyenne géométrique (peut-être prendre la factorielle sous la racine) :

$$\sqrt[n]{\prod x_i} = \sum \sqrt[n_i]{\prod x_1^{n_1} x_2^{n_2} ... x_k^{n_k}} = \frac{\sum (n_i\ log x_i)}{\sum n_i}$$

• Lucas, Théorie des nombres : le plus grand exposant d'un premier p dans une factorielle $n!$ (vaut $\sum\limits_k \dfrac{n}{p^k}$, ex : plus grande puissance de 7 dans 10000! ; on calcule $10000/7 = 1428$ et $1428/7 = 204$ et $204/7 = 29$ et $29/7 = 4$ et on fait la somme $1428 + 204 + 29 + 4 = 1665$, plus grande puissance de 7 cherchée) ;

• Transformation de Laplace bilatérale ($d(x + a) = dx$, de $-\infty$ à $+\infty$) tandis que transformation de Mellin $\left(\dfrac{d(ax)}{ax} = \dfrac{dx}{x}\right)$;

• Vue de mes yeux vue : elle, c'est simple, je l'adore ! Pour sûr, elle part à l'infini, mais à chaque fois qu'elle redescend sur terre, c'est pour indiquer un nombre premier...



• S'octroyer le droit de conjecturer aussi. Conjecturons, conjecturons donc : je crois que du fait que ζ s'appuie sur Γ, il faut chercher pour comprendre ζ du côté de la divisibilité des factorielles (Γ est l'extension de la factorielle au plan complexe). J'ai lu dans la Théorie des nombres de Lucas un théorème intéressant sur la divisibilité des factorielles. Pour trouver l'exposant de 7 dans la factorielle de 10000, il divise itérativement 10000 par 7 et il ajoute les quotients. Cela a comme conséquence qu'un nombre premier est le seul nombre dont on soit sûr qu'il apparaît à puissance de 1 dans la factorisation de sa factorielle, les premiers plus petits que lui peuvent apparaître à puissance plus grande (par exemple dans la factorisation de 7!, 3 est dans 3 mais aussi caché dans 6). Peut-être que cette propriété mise au jour par Lucas permettrait de plaquer un ordre total sur les nombres, ce que ne permet pas la divisibilité qui plaque un ordre partiel sur eux. C'est peut-être aussi cette propriété qui aurait pour conséquence l'alignement des zéros...

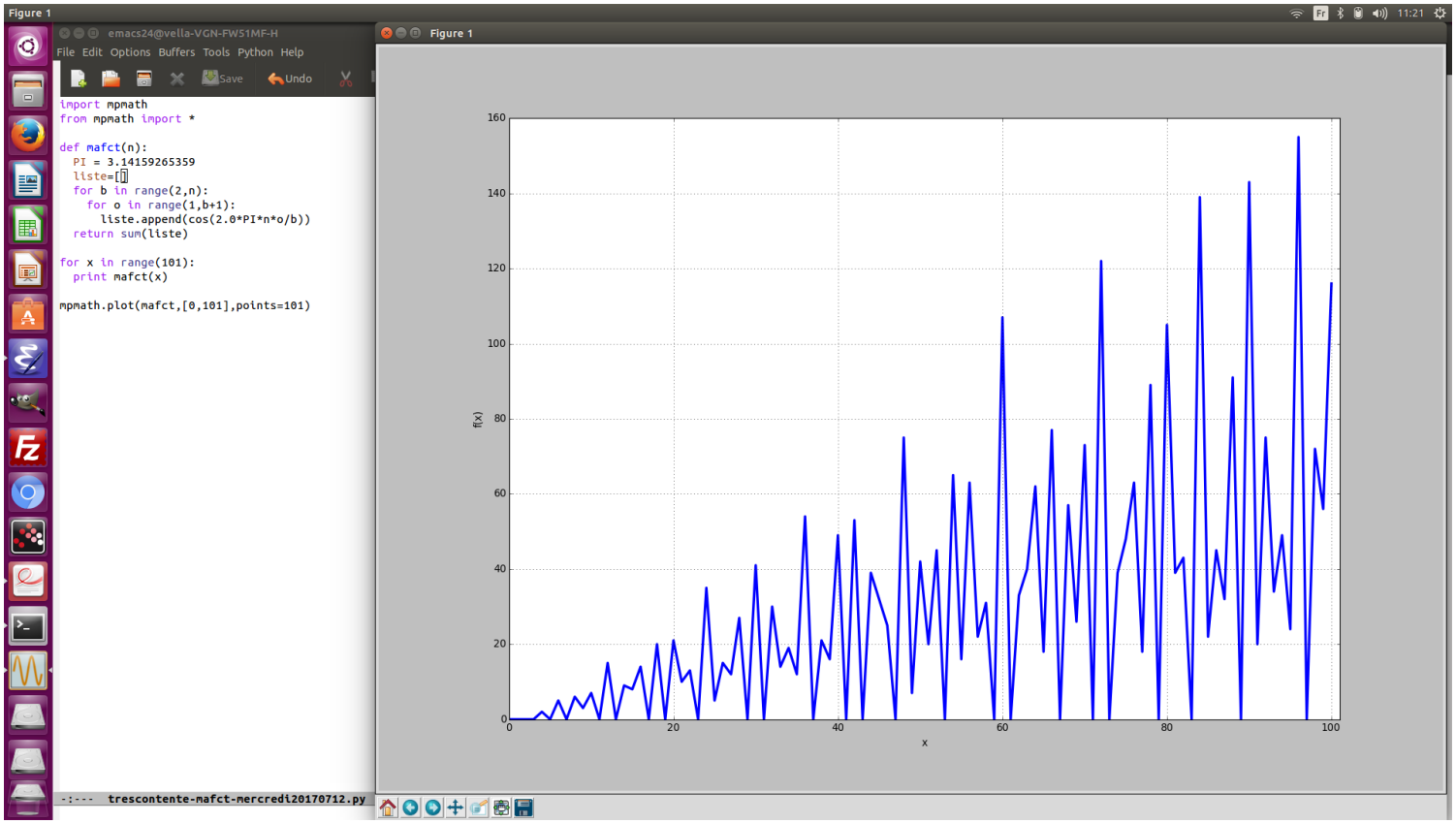


Figure 1
emacs24@vella-VGN-FW51MF-H
File Edit Options Buffers Tools Python Help
Save
Undo
import mpmath
from mpmath import *
def mafct(n):
PI = 3.14159265359
liste=[]
for b in range(2,n):
for o in range(1,b+1):
liste.append(cos(2.0*PI*n*o/b))
return sum(liste)
for x in range(101):
print mafct(x)
mpmath.plot(mafct,[0,101],points=101)
-:---
trescontente-mafct-mercredi20170712.py
Figure 1
f(x)
x
0
20
40
60
80
100
120
140
160

Valuations p-adiques dans les factorisations des factorielles (Denise Vella-Chemla, 13.7.2017)

Lucas consacre dans sa théorie des nombres un paragraphe à la divisibilité des factorielles. Il fournit une procédure pour trouver la puissance d'un nombre premier p dans la factorisation de la factorielle d'un nombre entier n. Prenons un exemple ; pour connaître la puissance de 7 dans la factorielle de 10000, on divise successivement 10000 par 7, en obtenant comme quotients successifs 1428, 204, 29 et 4 et on ajoute ces quotients pour obtenir la valuation p-adique de 7 dans 10000 ! et qui est 1428+204+29+4=1665.

En réfléchissant un peu à cette idée, on réalise qu'un nombre premier p est à puissance 0 dans la factorisation de la factorielle de tout nombre qui lui est inférieur, à puissance 1 dans toute factorisation de la factorielle d'un entier de l'intervalle $[p, 2p[$ et à puissance supérieure à 1 pour les factorielles des nombres supérieurs ou égaux à $2p$.

Un nombre composé se distingue d'un nombre premier par le fait qu'il est à puissance au moins 2 dans la factorisation de sa propre factorielle (par exemple, 6 dans la factorielle de 6 apparaît "en tant que lui-même" mais également comme produit de ses 2 sous-facteurs 2 et 3 qui sont dans la factorielle l'un et l'autre séparément).

Cette propriété qu'un nombre premier p apparaît à puissance de 1 dans la factorisation de sa factorielle fournit une fonction qui permet de distinguer les nombres premiers des nombres composés (cette fonction associe à un nombre sa factorielle, puis extrait du nombre obtenu la valuation p-adique du nombre en question) ; les nombres premiers sont les seuls antécédents de 1 par cette fonction.

Ces propriétés permettent à nouveau d'illustrer ce que l'on peut entendre par "coïncidence de fonctions" : représentons le début de la droite numérique ainsi que les premiers nombres premiers. Représentons par des intervalles de valeurs ce qui a été énoncé ci-dessus. La deuxième ligne montre que la valuation p-adique de 3 dans les factorisations des factorielles des nombres compris entre 3 inclus et 6 exclus vaut 1 (et 0 pour des nombres inférieurs à 3 et plus que 1 pour des nombres supérieurs ou égaux à 6).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	8	19	20	21	22	23
2	0	[	1	[							>1												
3		0	[	1		[							>1										
5			0		[		1			[						>1							

203. Divisibilité des factorielles. — Nous commencerons par résoudre le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre a qui ne surpasse pas un nombre donné n.*

Une première méthode, directe, consiste à calculer le Tableau des puissances successives de a, jusqu'à ce que l'on obtienne un exposant α tel que l'on ait

$$a^{\alpha} \leqslant n < a^{\alpha+1},$$

et l'exposant cherché est α; on peut déterminer ainsi, par exemple, le plus grand exposant de la puissance de 2 contenue dans un nombre donné (n° 189, Remarque II).

Mais, au lieu d'employer les multiplications successives par a, on peut aussi employer les divisions successives par a. Cette méthode repose sur le théorème suivant : *Si q désigne le quotient par défaut de la division de n par a, et si q' désigne le quotient par défaut de la division de q par b, le nombre q' est égal*

au quotient par défaut de la division de n par le produit ab. En effet, on a par définition,

$$n = aq + r, \qquad q = bq' + s,$$

r désignant l'une des valeurs 0, 1, 2, ..., $(a-1)$, et s l'une des valeurs 0, 1, 2, ..., $(b-1)$. On déduit

$$n = abq' + (as + r);$$

mais le nombre non négatif $(as + r)$ est au plus égal à

$$a(b-1) + (a-1) \quad \text{ou} \quad (ab-1);$$

donc q' est le quotient exact, ou approché par défaut, de la division de n par ab.

On désigne habituellement le plus grand nombre entier contenu dans $\frac{n}{a}$ par la notation $\mathrm{E}\frac{n}{a}$, que l'on prononce *entier de n par a* : on a donc

$$\mathrm{E}\,\frac{\mathrm{E}\,\frac{n}{a}}{b} = \mathrm{E}\,\frac{n}{ab},$$

et cette formule s'applique, en général, à l'entier de $\frac{n}{abc\ldots}$.

Cela posé, nous résoudrons le problème suivant : *Déterminer le plus grand exposant de la puissance d'un nombre premier p contenue dans le produit n! des n premiers nombres.* Les entiers qui contiennent p en facteur dans la factorielle $n!$ sont tous les multiples de p

$$p, 2p, 3p, \ldots, \mathrm{E}\,\frac{n}{p}\,p, \qquad \text{en nombre } \mathrm{E}\,\frac{n}{p};$$

par suite, l'exposant de p dans cette factorielle est égal à l'exposant de p dans le produit

$$1.2.3\ldots.\,\mathrm{E}\,\frac{n}{p},$$

augmenté du dernier facteur. En répétant le même raisonnement sur cette nouvelle factorielle, et en appliquant le théorème précédent, il en résulte que l'exposant du nombre premier p dans la

factorielle $n!$ est égal à la somme

$$\mathrm{E}\frac{n}{p} + \mathrm{E}\frac{n}{p^2} + \mathrm{E}\frac{n}{p^3} + \dots.$$

Lorsque n est une puissance de p, les quotients de n par $p, p^2, p^3, \dots$, sont tous entiers, et l'on trouve pour l'exposant cherché

$$\frac{n-1}{p-1}.$$

Si l'on écrit le nombre n dans le système de numération de base p, en supposant

$$n = a + bp + cp^2 + dp^3 + \dots,$$

on trouve facilement que l'exposant cherché a pour valeur

$$\frac{n - (a + b + c + \dots)}{p-1},$$

et a pour limite supérieure

$$\frac{n}{p-1}.$$

Exemple I. — Quel est l'exposant de 7 dans le produit des 10000 premiers nombres?

On dispose le calcul de la manière suivante :

10000	7						
30	1428	7					
20	028	204	7				
60	0	64	29	7			
4		1	1	4			

et le nombre cherché est

$$1428 + 204 + 29 + 4 = 1665.$$

Exemple II. — Le produit des 1000 premiers nombres se termine par 249 zéros.

Exemple III. — Trouver le plus grand exposant de la puissance du nombre premier p contenue dans le nombre combinatoire C_m^n.

On a

$$\mathrm{C}_m^n = \frac{m!}{n!(m-n)!},$$

Toujours est-il que le rapport $\frac{50\,847\,633}{50\,847\,534}$ pour $x = 10^9$ vaut 1.000001947 et que donc, puisque $f(x) = \pi(x) + \frac{1}{2}\pi\left(x^{\frac{1}{2}}\right) + \frac{1}{3}\pi\left(x^{\frac{1}{3}}\right) + \frac{1}{4}\pi\left(x^{\frac{1}{4}}\right) + \frac{1}{5}\pi\left(x^{\frac{1}{5}}\right) + \ldots$, il suffirait, si l'hypothèse de Riemann était démontrée, pour trouver quasi-exactement le nombre de nombres premiers inférieurs à x de calculer $Li(x) = li(x) - li(2)$ et de lui soustraire la moitié du nombre de nombres premiers inférieurs à la racine carrée de x, ainsi que le tiers du nombre de nombres premiers inférieurs à la racine cubique de x, ainsi que le quart du nombre de nombres premiers de la racine quatrième de x, en poursuivant les retraits jusqu'à la dernière racine k-ième de x supérieure ou égale à 2.

$$exp(li(\kappa.t.i.o(n))).exp(e^{\partial i.t.i^{\nu e}})$$

Les zéros de zêta ne peuvent pas être ailleurs que sur la droite critique parce que sinon, admettons qu'il y en ait à peine 2 qui ne soient pas sur la droite des nombres de partie réelle $\frac{1}{2}$, que l'un soit de la forme $\rho = \alpha + \beta i$ et que son conjugué soit de la forme $\alpha - \beta i$, quand, dans la formule de Riemann

$$f(x) = Li(x) - \sum_{\rho}(Li(x^{\rho}) + Li(x^{\overline{\rho}})) + \int_{x}^{\infty} \frac{du}{u(u^2-1)ln\ u} - ln\ 2,$$

on ajouterait les logarithmes intégrals de ces 2 zéros conjugués, alors que lorsque les zéros appartiennent bien à la droite critique, les parties imaginaires s'annulent entraînant l'ajout seulement du double de la partie réelle commune aux deux zéros, là, pour ces deux zéros hors droite critique, on obtiendrait comme valeur de la somme des logarithmes intégrals de ces deux complexes un nombre complexe, et alors on serait obligé de conclure par une phrase du style "jusqu'à 3 000 456 278, il y a $5\ 678 + 8\ 528i$ nombres premiers, ce qui, on l'avouera, ne veut strictement rien dire". Nous ne voyons pas d'autre explication...

Interpréter géométriquement l'hypothèse de Riemann (Denise Vella-Chemla, 7.8.2017)

On essaie d'interpréter géométriquement la formulation littérale de la fonction ζ de Riemann qui est :

$$\zeta(s) = \sum_{n=1}^{\infty} \left(\frac{1}{n}\right)^s$$

Cette somme est une somme de nombres complexes. A chacun de ces nombres complexes est associé un point du plan complexe. On peut voir la somme comme une spirale brisée qui à l'infini s'enroulerait autour d'un point du plan complexe à déterminer.

L'hypothèse de Riemann correspondrait alors au fait que seules les racines carrées des entiers successifs seraient admissibles aux dénominateurs pour calculer les longueurs des côtés successifs de la spirale mais que toute autre sorte de longueurs ne permettrait pas que la spirale finisse par aboutir au point origine.

Les angles de rotation $\theta, \theta', \theta''$ qui séparent deux côtés successifs de la spirale sont tous différents : quand on écrit littéralement la somme $\zeta(s)$ avec $s = a + ib$, on obtient

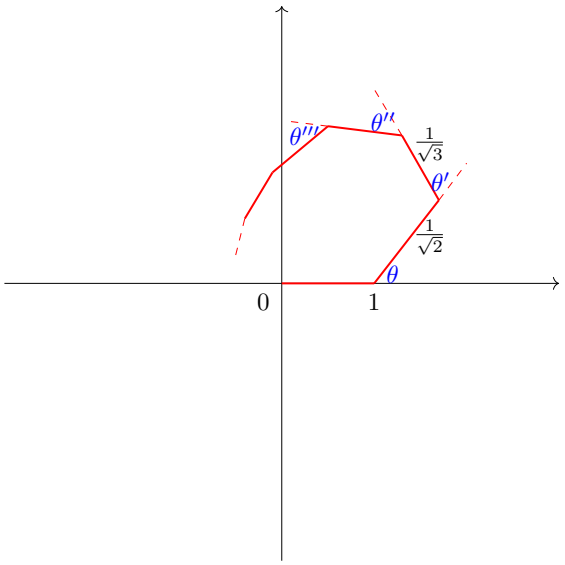
$$1 + \frac{1}{2}^a e^{-ib\ ln\ 2} + \frac{1}{3}^a e^{-ib\ ln\ 3} + \frac{1}{4}^a e^{-ib\ ln\ 4} + \ldots$$

Les deux premiers points de la spirale sont $z = 0$ et $z = 1$.

Dans le cas où $a = \frac{1}{2}$, les côtés successifs de la spirale brisée ont pour longueur $\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{4}}, \ldots$.

Dans le cas où $a = \frac{1}{3}$ par exemple, les côtés successifs de la spirale brisée ont pour longueur $\frac{1}{\sqrt[3]{2}}, \frac{1}{\sqrt[3]{3}}, \ldots$.

Les transformations qui permettent d'obtenir un côté de la spirale à partir du côté précédent (une translation, une homothétie et une rotation) ne commutent pas et doivent être effectuées dans l'ordre énoncé.



Pour les complexes appartenant à la droite critique (i.e. qui ont pour partie réelle $\frac{1}{2}$), on peut voir les longueurs des côtés de la spirale de la forme $\frac{1}{\sqrt{n}}$ comme les longueurs d'hypothénuses de triangles rectangles d'autres côtés de longueurs 1 et $\frac{1}{\sqrt{n-1}}$. Les seules longueurs admissibles pour les côtés successifs de la spirale seraient selon l'hypothèse les inverses des racines carrées des entiers successifs. Il faudrait identifier une propriété que seuls auraient les inverses des racines carrées et que n'auraient pas toute autre sorte de nombres, et qui aurait pour conséquence que les zéros de ζ ne pourraient qu'appartenir à la droite critique.

Il me semble qu'il faut se focaliser sur la notion de racine carrée comme ayant une propriété spécifique et négliger les angles car je crois que ces angles étant en nombre infini, on peut trouver pour chacun d'eux son complémentaire au tour complet, ce qui permet de toujours pouvoir "se ramener à" l'orientation de l'axe des réels.

wikisource Manuscrits de Galois, édition Tannery 1908, Introduction

INTRODUCTION

Les manuscrits de Galois ont été remis à Joseph Liouville par Auguste Chevalier : Liouville a légué sa bibliothèque et ses papiers à l'un de ses gendres, M. de Blignières [1]. Mme de Blignières s'occupe pieusement de classer les innombrables papiers de son mari et de son illustre père. Elle a recherché et su retrouver (non sans peine) les manuscrits de Galois : ceux-ci, ainsi que d'autres papiers importants, seront donnés à l'Académie des Sciences : Mme de Blignières a bien voulu, en attendant, m'autoriser à examiner les manuscrits de Galois et à en publier des extraits : je lui exprime ici ma profonde reconnaissance.

Je dois aussi des remercîments à M. Paul Dupuy, dont tous les géomètres connaissent la belle Notice sur la vie d'Évariste Galois, publiée dans les *Annales scientifiques de l'École Normale* [2]. M. Dupuy a bien voulu procéder à un premier classement des manuscrits qui m'avaient été remis et en séparer ceux qui appartiennent incontestablement à Galois, dont il connaît bien l'écriture.

Les lignes qui suivront, les quelques fragments ou notes que je pourrai publier n'ajouteront rien à la gloire de Galois : elles ne sont qu'un hommage rendu à cette gloire dont l'éclat n'a fait que grandir depuis la publication de Liouville.

Cette publication a été faite de la façon la plus judicieuse ; mais, soixante ans plus tard, on est tenu à moins de réserve. Les mathématiciens s'intéresseront toujours à Galois, à l'homme et à ses écrits : il est de ceux dont on voudrait tout savoir.

Je m'occuperai tout d'abord des œuvres posthumes et des papiers qui s'y rapportent. Pour la plupart de ces papiers, on possède la copie de Chevalier ; d'ailleurs l'écriture de Galois est, d'ordinaire, parfaitement lisible et même assez élégante ; mais elle est parfois abrégée, hâtive ; les ratures et les surcharges abondent ; j'aurai à signaler quelques mots et quelques phrases illisibles.

L'importance de l'œuvre de Galois sera mon excuse pour la minutie de certains détails, où j'ai cru devoir entrer, et qui va jusqu'au relevé de fautes d'impression, dont le lecteur attentif ne peut manquer de s'apercevoir. Je ne me dissimule pas ce que cette minutie, en elle-même, a de puéril.

Les œuvres posthumes occupent les pages 408-444 du Tome XI (1846) du *Journal de Mathématiques pures et appliquées* et les pages 25-61 des *Œuvres mathématiques d'Évariste Galois publiées sous les auspices de la Société mathématique de France* [3]. C'est, sauf avis contraire, à ce dernier Ouvrage que se rapportent tous les renvois.

Lettre à Auguste Chevalier

(pages : 25-32).

Dimensions du papier : 31×20. La lettre, datée deux fois, au commencement et à la fin (29 mai 1832), contient sept pages : le bas de la septième, au-dessous de la signature, a été coupé sur une longueur d'environ 8^{cm}.

Le verso de la dernière page contient le brouillon de deux lettres, d'ailleurs biffées, dont l'une porte une date, biffée aussi ; on lit 14 mai 83 ; il est vraisemblable que Galois a écrit sa lettre à Chevalier sur la première feuille venue, une feuille sur laquelle il avait griffonné une quinzaine de jours auparavant.

Ces brouillons sont disposés d'une façon assez singulière : ils comportent des phrases entières, puis des lignes, blanches au milieu avec un mot au commencement et un mot à la fin : ces mots sont souvent illisibles, tant parce qu'il est impossible de leur attribuer un sens que par suite des ratures : celles-ci vont de haut en bas ; il en est ainsi dans plusieurs des manuscrits de Galois ; ici, elles semblent faites avec une barbe de plume, ou un bout de bois, qu'il aurait trempé dans l'encre ; le premier brouillon de lettre est à gauche, le second à droite et se continue dans une autre direction ; Galois a fait tourner son papier d'un angle droit. Voici ce que j'ai pu lire :

brisons là sur cette affaire je vous prie
Je n'ai pas assez d'esprit pour suivre
une conversation de ce genre
mais je tâcherai d'en avoir assez pour
converser avec vous comme je le faisais
avant que rien soit arrivé. Voilà
Mr le *(illis.)*
en a qui
doit vous qu'à
moi et ne plus penser à des choses
qui ne (*illis.*) exister et qui
n'existeront jamais

14 mai 83

J'ai suivi votre conseil et j'ai réfléchi
à qui s'est
passé sous quelque
dénomination que ce puisse [4] être *(illis.)* par s'établir
entre nous. Au reste Mr soyez (?)
persuadé qu'il n'en aurait sans doute

jamais été davantage ; vous supposez
mal et vos regrets sont mal fondés.
La vraie amitié n'existe guère
qu'entre des personnes de même sexe
Surtout des
amis. Sans doute
le vide qu l'absence
de tout sentiment de ce genre....
(illis.) confiance... mais elle a été
très *(illis.)* [5] ..... vous m'avez
vu triste z demandé
le motif ; je vous ai répondu que
j'avais des peines ; qu'on m'avait fait
éprouver. J'ai pensé que vous prendriez
celà comme toute personne devant
laquelle on laisse tomber une parole
pour *(illis.)* on n'est
pas
le calme de mes idées me laisse
la liberté de juger avec beaucoup
de réflexion les personnes que je vois
habituellement ; c'est ce qui fait que
j'ai rarement le regret de m'être
trompé ou laissé influencer à leur égard.
Je ne suis pas de votre avis pour
les *(illis.)* plus que
les (?) exiger
ni se vous remercie
sincèrement de tous ceux ou vous
voudrez bien descendre en ma
faveur.

J'ai collationné le manuscrit avec le texte imprimé : il n'est guère utile de parler de quelques changements de notation, sans aucune importance, qui remontent à Liouville, de dire que Galois a écrit bulletin ferussac et non Bulletin de Férussac, ou encore de signaler, page 29 des Œuvres, ligne 24, la substitution du mot "équation" au mot "réduction" que le sens indique suffisamment et qu'on lit dans le manuscrit et

dans le texte de Liouville. Le point le plus intéressant est que le théorème de Legendre (page 30, ligne 31),

$$\mathrm{FE}' + \mathrm{EF}' - \mathrm{FF}' = \frac{\pi}{2}$$

est écrit par Galois non sous la forme qui précède, mais comme il suit :

$$\mathrm{E}'\mathrm{F}'' - \mathrm{E}''\mathrm{F}' = \frac{\pi}{2}\sqrt{-1}$$

Mémoire sur les conditions de résolubilité par radicaux

(pages 33-50) [6].

Dans les quelques lignes d'introduction au Mémoire sur les conditions de résolubilité des équations par radicaux que Galois avait biffées (d'ailleurs très légèrement) et que Chevalier a conservées avec raison, Galois dit que le Mémoire est extrait d'un Ouvrage qu'il a présenté à l'Académie il y a un an. Le manuscrit de Galois n'est pas un extrait, c'est le texte même qui a été remis à l'Académie. Qu'il en soit ainsi, c'est ce que Chevalier avait signalé dans une note (page 33 des Œuvres, note 2) ainsi conçue :

> J'ai jugé convenable de placer en tête de ce Mémoire la préface qu'on va lire, bien que je l'aie trouvée biffée dans le manuscrit. Ce manuscrit est précisément celui que l'auteur présenta à l'Académie.

La dernière phrase de cette note, qui figure dans la copie de Chevalier et sur l'épreuve dont j'ai parlé, a disparu du texte définitif. Liouville a-t-il voulu effacer la légère contradiction entre le texte et la note, a-t-il cru devoir se conformer au désir de Galois, qui semble avoir souhaité qu'on ignorât que ce Mémoire était celui-là même qu'il avait présenté à l'Académie ; a-t-il jugé lui-même que, pour des raisons de convenance envers l'Académie, cette ignorance était préférable ? C'est là, en vérité, des questions dont la réponse importe bien peu, non plus que la petite inexactitude du mot extrait. Il importe beaucoup plus que le texte du Mémoire de Galois ne se soit pas égaré, comme le précédent, et qu'il ait pu être remis à l'auteur, qui y a fait plusieurs remaniements : ceux-ci, le plus souvent, peuvent se distinguer par l'écriture. La conjecture de Chevalier, à savoir que "Galois a relu son Mémoire pour le corriger avant d'aller sur le terrain" (note de la page 40), est tout à fait vraisemblable.

La première page de la couverture, qui subsiste, est fort sale, tachée d'encre, couverte de gribouillages, de bouts de calcul, à l'encre ou au crayon, au recto et au verso, dans tous les sens ; quelques-unes des formules laissent supposer que Galois, en les traçant, pensait à quelque point de la théorie des fonctions elliptiques ; d'autres se rapportent à une suite récurrente.

En haut et à droite du recto on lit (écriture de Liouville) "Rapport du 4 juillet 1831" ; puis, en titre, d'une écriture qu'il serait probablement possible d'identifier :

MM. Lacroix

Poisson

commissaires

le 17 j^{er} 1831

le tout suivi d'un paraphe ; en face du nom de Poisson, il y a le mot *vu*, d'une grosse écriture, celle de Poisson sans doute.

Au verso, entre des taches et des calculs, Galois a écrit

> Oh ! chérubins.

On peut bien supposer que cette apostrophe s'adresse à MM. Lacroix et Poisson.

Le manuscrit contient onze pages (38 × 25) ; la marge occupe la moitié de chaque page ; elle contient plusieurs notes et additions, dont les unes remontent peut-être à la première rédaction, dont les autres ont été sans doute ajoutées par Galois, lorsqu'il a revu son travail pour la dernière fois telle est assurément celle qu'a signalée Chevalier, le tragique "je n'ai pas le temps".

En marge de la seconde page, on trouve ces quatre noms :

V. Delaunay,
N. Lebon,
F. Gervais,
A. Chevalier

et une liste de onze noms, soigneusement biffés.

Je dois, en passant, signaler, page 34 des *Œuvres*, l'omission de deux lignes, qui figurent dans le manuscrit et dans le texte de Liouville ; elles devraient terminer l'avant-dernier alinéa :

..., en général par quantité rationnelle une quantité qui s'exprime en fonction rationnelle des coefficients de la proposée.

Dans la marge de la troisième page du manuscrit, en face du lemme III (page 36), se trouve la note an crayon que voici :

La démonstration de ce lemme n'est pas suffisante ; mais il est vrai, d'après le n° 100 du Mémoire de Lagrange, Berlin, 1775.

Au-dessous, Galois a écrit :

Nous avons transcrit textuellement la démonstration que nous avons donnée de ce lemme dans un Mémoire présenté en 1830. Nous y joignons comme document historique la note suivante qu'a cru devoir y apposer M. Poisson.

On jugera.

Puis, plus bas :

Note de l'auteur.

Galois voulait évidemment que la note de Poisson [7] et son propre commentaire fussent publiés. Au surplus, les notes de Poisson et de Galois figurent dans la copie de Chevalier et dans l'épreuve. Liouville les a supprimées finalement, pour des raisons évidentes.

La note de la page 37 des *Œuvres* est en face du lemme IV et semble d'une encre différente de celle du texte; mais il ne me paraît nullement certain que ce soit une addition de la dernière heure : je crois que Galois a dû, à cette dernière heure, remanier et développer hâtivement la démonstration de ce lemme IV ; elle ne comportait probablement, dans le texte primitif, que quatre ou cinq lignes ; elle est maintenant écrite, partie dans la marge, partie dans le blanc qui restait au bas de la page, d'une écriture serrée, nerveuse : au reste, un mot injurieux, biffé, et qui est de la même encre que le "chérubins" de la couverture ne laisse guère de doute sur l'impatience que ce passage a fait éprouver à l'auteur.

La note de la page 38 des *Œuvres* est en marge, en face de la proposition I. À la suite de cette note, avec l'indication "à reporter dans les définitions", se trouve ce qui est imprimé pages 35 et 36, à partir de la ligne 22 (Les substitutions sont) jusqu'à la ligne 3 (la substitution ST) ; ce passage est en face du texte imprimé du milieu de la page 38 au milieu de la page 39.

En marge de la page suivante (cinquième) du manuscrit, le scholie II [8] (page 40) est immédiatement précédé de ces indications, qui sont biffées :

Ce qui caractérise un groupe. On peut partir d'une des permutations quelconques du groupe.

Vraisemblablement, c'est après avoir écrit et biffé ces lignes que Galois s'est décidé à écrire le passage "à reporter dans les définitions". Un peu plus bas est la note "je n'ai pas le temps", puis cinq lignes biffées, mais qui sont d'une écriture calme et remontent peut-être à la première rédaction, les voici :

Car si l'on élimine $f(V,r)=0$ et $F(r)=0, F(r)$ étant du degré premier p, il ne peut arriver que de deux choses l'une : ou le résultat de l'élimination sera de même degré en V que $f(V,r)$ ou il sera d'un degré p fois plus grand.

Ce passage biffé doit évidemment être rapproché des indications données dans le premier alinéa de la note de la page 40. Ces indications sont de Liouville ; la note de Chevalier était ainsi conçue :

Vis-à-vis la démonstration de ce théorème, dans le manuscrit j'ai trouvé ceci

"Il y a quelque chose..."

C'est ainsi qu'elle figure dans l'épreuve. Les six premières lignes de la note de la page 40 sont donc de Liouville.

Au reste, Liouville a été visiblement préoccupé de cet endroit (proposition II) du texte de Galois : il a jugé un moment convenable de reprendre l'hypothèse primitive de Galois (p premier) et d'éclaircir

complètement la démonstration dans ce cas, par une note que je crois devoir transcrire, non pas qu'elle puisse apprendre quelque chose au lecteur, mais parce qu'elle me semble une trace touchante des soins et des scrupules que Liouville apportait dans sa publication ; le renvoi correspondrait à la ligne 20 de la page 40 des *Œuvres* :

Ceci mérite d'être expliqué avec quelque détail.

Désignons par, $\psi(V) = 0$ l'équation dont l'auteur parle, et soient $f(V,r), f_1(V,r), \ldots, f_{i-1}(V,r)$ les facteurs irréductibles dans lesquels, $\psi(V)$ devient décomposable par l'adjonction de r, en sorte que,

$$\psi(V) = f(V,r)f_1(V,r)\ldots f_{i-1}(V,r).$$

Comme r est racine d'une équation irréductible, on pourra dans le second membre remplacer r par $r', r'', \ldots, r^{\mu-1}$. Ainsi $\psi(V)^\mu$ est le produit des i quantités suivantes

$$\begin{array}{ccc} f(V,r) & f(V,r')\ldots f(V,r^{(\mu-1)}) \\ f_1(V,r) & f_1(V,r')\ldots f_1(V,r^{(\mu-1)}) \\ f_{i-1}(V,r) & f_{i-1}(V,r')\ldots f_{i-1}(V,r^{(\mu-1)}) \end{array},$$

dont chacune, symétrique en $r, r', \ldots, r^{(p-1)}$ et par suite exprimable en fonction rationnelle de V indépendamment de toute adjonction, doit diviser $\psi(V)^\mu$ et se réduire en conséquence a une simple puissance du polynôme $\psi(V)$ qui cesse de se résoudre en facteurs lorsqu'on n'adjoint pas les auxiliaires r, r', etc. J'ajoute que le degré de la puissance est le même pour toutes. En effet, les équations $f(V,r') = 0, \quad f_1(V,r) = 0, \ldots, f_{i-1}(V,r) = 0$ qui dérivent de $\psi(V) = 0$ et dont les racines sont fonctions rationnelles les unes des autres ne peuvent manquer d'être du même degré. En faisant donc

$$f(V,r)f(V,r')\ldots f(V,r^{(p-1)}) = \psi(V)^\mu,$$

on en conclura $p = i\mu$. Mais p est premier et $i > 1$; donc on a $i = p$, d'où $\mu = t$, et enfin

$$\psi(V) = f(V,r)f(V,r')\ldots f(V,r^{(p-1)}).$$

Ce qu'il fallait démontrer.

J. Liouville.

Assurément, en rédigeant cette note, Liouville se conformait au précepte d'être "transcendantalement clair" qu'il a rappelé dans l'avertissement aux Œuvres mathématiques de Galois. Il s'est aperçu ensuite en réfléchissant davantage, que la proposition II n'impliquait pas que le nombre p fût premier et il a soigneusement noté les différences essentielles entre les deux rédactions successives de l'auteur. Qu'il ait reculé devant les explications nécessaires pour donner à la pensée de Galois toute la clarté qu'il faudrait, cela, aujourd'hui, n'a aucun inconvénient.

Page 41 des Œuvres, les lettres μ, ν remplacent les lettres p, n dont s'est servi Galois ; pareil changement a été fait dans la lettre à Chevalier ; ces petites modifications, destinées à éviter des confusions possibles, sont de Liouville : les lettres p, n figurent encore dans l'épreuve.

Les lignes 7, 8, 9 de la même page sont une addition marginale, mais qui ne semble pas de la dernière heure. Cette addition est suivie de la nouvelle rédaction de la proposition III, datée de 1832, sur laquelle l'attention est appelée dans la note qui est au bas de la page qui nous occupe. Ici encore, Liouville est intervenu ; la note de Chevalier était ainsi conçue.

Dans le manuscrit de Galois l'énoncé du théorème qu'on vient de lire se trouve en marge et vis-à-vis de la démonstration qu'il en avait écrite d'abord. Celle-ci est effacée avec soin ; l'énoncé précédent porte la date 1832 et montre par la manière dont il est écrit que l'auteur était extrêmement pressé : ce qui confirme l'assertion que j'ai avancée dans la note précédente.

C'est donc Liouville qui a déchiffré et intercalé le texte primitif de la proposition III.

La phrase (il suffit ... substitutions), placée entre parenthèses au bas de la page 43 des *Œuvres* et en haut de la page 44, est une note marginale.

Page 46, ligne 24, Galois a simplement écrit *"Journal de l'École, XVII"*.

Il y a dans les manuscrits de Galois une feuille (double) qui est une sorte de brouillon de la proposition V ; ce brouillon a passé en grande partie dans la rédaction du Mémoire [9].

Avant de parler du manuscrit contenant le fragment imprimé dans les dernières pages des *Œuvres*, je dois dire un mot d'une feuille détachée [10] en partie déchirée, qui, par le format du papier, la couleur de l'encre et la forme de l'écriture, paraît avoir appartenu au cahier dont ce manuscrit faisait partie. Elle contient une rédaction antérieure de la proposition I et de sa démonstration, rédaction qui semble avoir été écrite au moment même où Galois venait de trouver cette démonstration : l'énoncé de la proposition fondamentale est, presque textuellement, le même que dans le Mémoire sur des conditions de résolubilité, puis viennent seize lignes barrées que je reproduis :

Considérons d'abord un cas particulier. Supposons que l'équation donnée n'ait aucun diviseur rationnel et que toutes ses racines se déduisent rationnellement de l'une quelconque d'entre elles. La proposition sera facile à démontrer.

En effet, dans notre hypothèse, toute fonction des racines s'exprimera en fonction d'une seule racine et sera de la forme $\phi x, x$ étant une racine. Soient

$$x \quad x_1 = f_1 x \quad x_2 = f_2 x \ldots x_{m-1} = f_{m-1} x$$

les m racines. Écrivons les m permutations

$$\begin{array}{cccc} x & f_1 x & f_2 x \ldots & f_{m-1} x \\ x_1 & f_1 x_1 & f_2 x_1 \ldots & f_{m-1} x_1 \\ x_2 & f_1 x_2 & f_2 x_2 \ldots & f_{m-1} x_2 \\ & & \text{— — — —} & \\ x_{m-1} & f_1 x_{m-1} & f_2 x_{m-1} \ldots & f_{m-1} x_{m-1} \end{array}$$

Le reste de la démonstration suivait, contenu dans une douzaine de lignes qui sont devenues les lignes 13-26 de la page 39 des *Œuvres* : on distingue assez bien les x surcharges des V de la rédaction définitive ; ces douze lignes sont d'ailleurs réunies en marge par un trait, avec l'indication : *à reporter plus loin*. Galois a changé d'idée ; il trouve *maintenant* inutile de s'arrêter au cas particulier ; mais il semble que ce cas particulier lui ait été d'abord nécessaire, car les douze lignes que je viens de dire sont suivies de celles-ci :

Le théorème est donc démontré dans l'hypothèse particulière que nous avons établie.

Revenons au cas général.

Ces trois lignes sont biffées avec un soin particulier, Galois est en possession de la démonstration générale, sous la forme simple et définitive ; il est joyeux ; il couvre de hachures les seize lignes puis les trois lignes dont il n'a plus besoin. Vient ensuite la vraie démonstration, les deux dernières lignes de la page 38 des *Œuvres* et le commencement de la page 39, jusqu'à : "je dis que ce groupe de permutations jouit de la propriété énoncée". Puis l'indication, en marge, à demi déchirée : *mettre ici la partie sautée*, et les lignes 24, 25 de la page 39 des *Œuvres*.

Ne semble-t-il pas qu'on assiste à un moment essentiel dans le développement de la pensée de Galois ? L'émotion s'accroît encore à la lecture des lignes du bas de la feuille, couvertes de ratures et de surcharges, et où le nom propre a disparu dans un trou, produit d'une tache et de l'usure :

Je dois observer que j'avais d'abord démontré le théorème autrement, sans penser à me servir de cette propriété très simple des équations, propriété que je regardais comme une conséquence du théorème. C'est la lecture d'un Mémoire
qui m'a suggéré

La fin de la ligne est indéchiffrable : après *suggéré*, il y a des mots, l'un au-dessus de l'autre, qui sont biffés, peut-être *cette* surmonté de *la pensée*, puis, dans la partie la plus usée du papier, *assertion* ou *analyse*, ou autre chose, et enfin, plus bas, je crois lire *que je dois*. Quant au nom propre, les quelques traits qui subsistent, à côté du trou, ne confirment pas la supposition qui vient de suite à l'esprit (page 37, ligne 11), que ce nom est celui d'Abel.

Sur la marge de cette curieuse feuille, se trouvent encore quelques formules, à demi effacées, qui correspondent visiblement aux lemmes II et III.

---

1. Célestin de Blignières (1823-1905), ancien Élève de l'École Polytechnique, a été l'un des disciples directs d'Auguste Comte, l'un des plus distingués sans doute et vraiment capable, par l'étendue de son esprit et de son savoir, de comprendre pleinement la doctrine du maître. Mais l'indépendance de son caractère et l'originalité de son esprit l'ont empêché de s'enrôler dans l'un ou l'autre des partis du Positivisme. Il plaisantait parfois de son isolement et se

qualifiait de bligniériste : on lui doit une intéressante Exposition de la Philosophie et de la Religion positives (Paris, Chamerot, 1857).

Pendant neuf ans (1874-1883), un commerce de pensée, très actif, s'établit entre Liouville et M. de Blignières. De ce commerce, dont l'un et l'autre ont beaucoup joui, M. de Blignières a gardé jusqu'à sa mort un souvenir singulièrement vif et présent.

2. Tome XIII (1896) de la 3^{e} série. Cette Notice a été reproduite, avec le portrait de Galois, dans les *Cahiers de la quinzaine* [2^{e} cahier de la 5^{e} série (1903)].
3. Paris, Gauthier-Villars, 1897.
4. La lecture des quatre premiers mots de cette ligne est douteuse.
5. Il y a une tache d'encre sur le mot ; on distingue nettement les deux dernières lettres *ée*.
6. J'ai eu à ma disposition le manuscrit de Galois, la copie de Chevalier et une épreuve, corrigée de la main de Liouville, mais ou ne figurent pas toutes les modifications apportées aux notes : j'aurai l'occasion de parler plusieurs fois de cette épreuve.
7. Grâce à l'obligeance de Mme de Blignières, j'ai pu comparer l'écriture de cette note avec celle de Poisson, dans une lettre à Liouville; aucun doute ne peut subsister.
8. Les numéros I, II des scholies (p. 39 et 40) ne sont pas dans le manuscrit.
9. Je ne pense pas qu'il y ait intérêt à publier ce brouillon.
10. C'est M. P. Dupuy qui a appelé mon attention sur cette feuille. Quelques autres débris apportent un peu de lueur sur la suite des idées de Galois : ils seront publiés dans un second article.

wikisource Manuscrits de Galois, édition Tannery 1908, Papiers inédits de Galois

Étant donnée une équation algébrique, à coefficients quelconques, numériques ou littéraux, reconnaître si ses racines peuvent s'exprimer en radicaux, telle est la question dont nous offrons une solution complète.

Si maintenant vous me donnez une équation que vous aurez choisie à votre gré et que vous désiriez connaître si elle est ou non soluble par radicaux, je n'aurai rien à y faire que de vous indiquer le moyen de répondre à votre question, sans vouloir charger ni moi ni personne de le faire. En un mot les calculs sont impraticables.

Il paraîtrait d'après cela qu'il n'y a aucun fruit à tirer de la solution que nous proposons.

En effet, il en serait ainsi si la question se présentait ordinairement sous ce point de vue. Mais, la plupart du temps, dans les applications de l'analyse algébrique, on est conduit à des équations dont on connaît d'avance toutes les propriétés : propriétés au moyen desquelles il sera toujours aisé de répondre à la question par les règles que nous exposerons. Il existe, en effet, pour ces sortes d'équations, un certain ordre de considérations métaphysiques qui planent sur tous les calculs, et qui souvent les rendent inutiles. Je citerai, par exemple, les équations qui donnent la division des fonctions elliptiques et que le célèbre Abel a résolues. Ce n'est certainement pas d'après leur forme numérique que ce géomètre y est parvenu. Tout ce qui fait la beauté et à la fois la difficulté de cette théorie, c'est qu'on a sans cesse à indiquer la marche des calculs et à prévoir les résultats sans jamais pouvoir les effectuer. Je citerai encore les équations modulaires.

| Première page.|

Deux Mémoires d'Analyse pure suivis d'une dissertation sur la classification des problèmes par Évariste Galois.

| Deuxième page.|

Table des matières.

Mémoire sur les conditions pour qu'une équation soit soluble par radicaux.

Mémoire sur les fonctions de la forme $\int X dx$, X étant une fonction de x.

Dissertation sur la classification des problèmes de Mathématiques et sur la nature des quantités et des fonctions transcendantes.

| Troisième page ([1]).|

Ampère

Cauchy

Gauss

Hachette

Jacobi

Lacroix

Legendre

Poinsot

Poisson

Sturm

Vernier

Richard

Bulletin des Sciences

École normale

École Polytechnique

Institut. [24]

| Quatrième page.|

Abel paraît être l'auteur qui s'est le plus occupé de cette théorie. On sait qu'après avoir cru trouver la résolution des équations (générales) du cinquième degré ([2]), ce géomètre a démontré l'impossibilité de cette résolution. Mais, dans le mémoire allemand publié à cet effet, l'impossibilité en question n'est prouvée que par des raisonnements relatifs au degré des équations auxiliaires et à l'époque de cette publication, il est certain qu'Abel ignorait les circonstances particulières de la résolution par radicaux. Je n'ai donc parlé de ce mémoire qu'afin de déclarer qu'il n'a aucun rapport avec ma théorie.

[*Passage biffé* : Depuis, une lettre particulière adressée par Abel à M. Legendre annonçait qu'il avait eu le bonheur de découvrir une règle pour reconnaître si une équation est [ou était] résoluble par radicaux ; mais la mort anticipée de ce géomètre ayant privé la science de ses recherches, promises dans cette lettre, il n'en était pas moins nécessaire de donner une solution de ce problème qu'il m'est bien pénible de posséder, puisque je dois cette possession à une des plus grandes pertes qu'aura (?) faites la science.

Dans tous les cas, il me serait aisé de prouver que j'ignorais même le nom d'Abel, quand j'ai présenté à l'Institut mes premières recherches sur la théorie des équations et que la solution d'Abel n'aurait pu paraître avant la mienne.]

Deux Mémoires d'Analyse pure par E. Galois

Préface.

Cecy est un livre de bonne foy.
Montaigne.

Les calculs algébriques ont d'abord été peu nécessaires au progrès des Mathématiques, les théorèmes fort simples gagnaient à peine à être traduits dans la langue de l'analyse. Ce n'est guère que depuis Euler que cette langue plus brève est devenue indispensable à la nouvelle extension que ce grand géomètre a donnée à la Science. Depuis Euler les calculs sont devenus de plus en plus nécessaires et aussi ([3]) de plus en plus difficiles à mesure qu'ils s'appliquaient à des objets de science plus avancés. Dès le commencement de ce siècle, l'algorithme avait atteint un degré de complication tel que tout progrès était devenu impossible par ce moyen, sans l'élégance que les géomètres modernes ont d'imprimer à leurs recherches et au moyen de laquelle l'esprit saisit promptement et d'un seul coup un grand nombre d'opérations.

Il est évident que l'élégance si vantée et à si juste titre n'a pas d'autre but.

Du fait bien constaté que les efforts des géomètres les plus avancés ont pour objet l'élégance on peut donc conclure avec certitude qu'il devient de plus en plus nécessaire d'embrasser plusieurs opérations à la fois, parce que l'esprit n'a plus le temps de s'arrêter aux détails.

Or je crois que les simplifications produites par l'élégance des calculs (simplifications intellectuelles, s'entend ; de matérielles il n'y en a pas) ont leur limite ; je crois que le moment arrivera où les transformations algébriques prévues par les spéculations des analystes ne trouveront plus ni le temps ni la place de se reproduire ; à tel point qu'il faudra se contenter de les avoir prévues : je ne veux pas dire qu'il n'y a plus rien de nouveau pour l'analyse sans ce secours : mais je crois qu'un jour, sans cela, tout serait épuisé.

Sauter à pieds joints sur les calculs ; grouper les opérations, les classer suivant leurs difficultés et non suivant leurs formes ; telle est, suivant moi, la mission des géomètres futurs ; telle est la voie où je suis entré dans cet ouvrage.

Il ne faut pas confondre l'opinion que j'émets ici, avec l'affectation que certaines personnes ont d'éviter en apparence toute espèce de calcul, en traduisant par des phrases fort longues ce qui s'exprime très brièvement par l'algèbre, et ajoutant ainsi à la longueur des opérations, les longueurs d'un langage qui n'est pas fait pour les exprimer. Ces personnes sont en arrière de cent ans.

Ici rien de semblable ([4]) ; ici l'on fait l'analyse de l'analyse : ici les calculs les plus élevés [les fonctions elliptiques ([5])] exécutés jusqu'à présent sont considérés comme des cas particuliers, qu'il a été utile, indispensable de traiter, mais qu'il serait funeste de ne pas abandonner pour des recherches plus larges. Il sera temps d'effectuer des calculs prévus par cette haute analyse et classés suivant leurs difficultés, mais non spécifiés dans leur forme, quand la spécialité d'une question les réclamera.

La thèse générale que j'avance ne pourra être bien comprise que quand on lira attentivement mon ouvrage qui en est une application, non que le point de vue théorique ait précédé l'application ; mais je

me suis demandé, mon livre terminé, ce qui le rendait si étrange à la plupart des lecteurs, et rentrant en moi-même, j'ai cru observer celle tendance de mon esprit à éviter les calculs dans les sujets que je traitais, et qui plus est, j'ai reconnu une difficulté insurmontable à qui voudrait les effectuer généralement dans les matières que j'ai traitées.

On doit prévoir que, traitant des sujets aussi nouveaux, hasardé dans une voie aussi insolite, bien souvent des difficultés se sont présentées que je n'ai pu vaincre. Aussi, dans ces deux mémoires et surtout dans le second qui est le plus récent, trouvera-t-on souvent la formule "je ne sais pas". La classe des lecteurs dont j'ai parlé au commencement ([6]), ne manquera pas d'y trouver à rire. C'est que, malheureusement, on ne se doute pas que le livre le plus précieux du plus savant serait celui où il dirait tout ce qu'il ne sait pas, c'est qu'on ne se doute pas qu'un auteur ne nuit ([7]) jamais tant à ses lecteurs que quand il dissimule une difficulté. Quand la concurrence c'est-à-dire l'égoïsme ne régnera plus dans les sciences, quand on s'associera pour étudier, au lieu d'envoyer aux académies des paquets cachetés, on s'empressera de publier les moindres observations, pour peu qu'elles soient nouvelles, et en ajoutant "je ne sais pas le reste".

De S^{te} Pélagie X^{bre} 1831
Evariste Galois.

Sciences mathématiques
Discussions sur les progrès de l'analyse pure

De toutes les connaissances humaines, on sait que l'Analyse pure est la plus immatérielle, la plus éminemment logique, la seule qui n'emprunte rien aux manifestations des sens. Beaucoup en concluent qu'elle est, dans son ensemble, la plus méthodique et la mieux coordonnée. Mais c'est erreur. Prenez un livre d'Algèbre, soit didactique, soit d'invention, et vous n'y verrez qu'un amas confus de propositions dont la régularité contraste bizarrement avec le désordre du tout. Il semble que les idées coûtent déjà trop à l'auteur pour qu'il se donne la peine de les lier et que son esprit épuisé par les conceptions qui sont la base de son ouvrage, ne puisse enfanter une même pensée qui préside à leur ensemble.

Que si vous rencontrez une méthode, une liaison, une coordination, tout cela est faux et artificiel. Ce sont des divisions sans fondement, des rapprochements arbitraires, un arrangement tout de convention. Ce défaut pire que l'absence de toute méthode arrive surtout dans les ouvrages didactiques, la plupart composés par des hommes qui n'ont pas l'intelligence de la science qu'ils professent.

Tout cela étonnera fort les gens du monde, qui en général ont pris le mot Mathématique pour synonyme de régulier.

Toutefois, on sera étonné si l'on réfléchit qu'ici comme ailleurs la science est l'œuvre de l'esprit humain ([8]), qui est plutôt destiné à étudier qu'à connaître, à chercher qu'à trouver la vérité. En effet on conçoit qu'un esprit qui aurait puissance pour percevoir d'un seul coup l'ensemble des vérités mathématiques non pas à nous connues, mais toutes les vérités possibles, pourrait les ([9]) déduire régulièrement et comme machinalement de quelques principes combinés par des méthodes uniformes ; alors plus d'obstacles, plus de ces difficultés que le savant rencontre dans ses explorations ([10]). Mais il n'en est pas ainsi ; si ([11]) la tâche du savant est plus pénible et partant plus belle, la marche de la science est moins régulière : la science progresse par une série de combinaisons où le hasard ne joue pas le moindre rôle ; sa vie est brute et ressemble à celle des minéraux qui croissent par juxtaposition. Cela s'applique non seulement à la science telle qu'elle résulte des travaux d'une série de savants, mais aussi aux recherches particulières à chacun d'eux. En vain les analystes voudraient-ils se le dissimuler ([12]) : ils ne déduisent pas, ils combinent, ils comparent ([13]) ; quand ils arrivent à la vérité, c'est en heurtant de côté et d'autre qu'ils y sont tombés.

Les ouvrages didactiques doivent partager avec les ouvrages d'invention ce défaut d'une marche sûre toutes les fois que le sujet qu'ils traitent ([14]) n'est pas autrement soumis à nos lumières. Ils ne pourraient donc prendre une forme vraiment méthodique que sur un bien petit nombre de matières. Pour la leur donner, il faudrait une profonde intelligence de l'analyse et l'inutilité de l'entreprise dégoûte ceux qui pourraient en supporter la difficulté.

Il serait en dehors de la gravité de cet écrit d'entrer dans une pareille lutte avec des sentiments personnels d'indulgence ou d'animosité à l'égard des savants. L'auteur des articles évitera également ces deux écueils. Si un passé pénible le garantit du premier, un amour profond de la science, qui la lui fait respecter dans ceux qui la cultivent, assurera contre le second son impartialité.

Il est pénible dans les sciences de se borner au rôle de critique : nous ne le ferons que contraint et forcé. Quand nos forces nous le permettront, après avoir blâmé, nous indiquerons ce qui à nos yeux sera

mieux. Nous aurons souvent ainsi l'occasion d'appeler l'attention du lecteur sur les idées nouvelles qui nous ont conduit dans l'étude de l'analyse. Nous nous permettrons donc de l'occuper de ces idées, dans nos premiers articles, afin de n'avoir point à y revenir.

Dans des sujets moins abstraits, dans les objets d'art, il y aurait un profond ridicule à faire précéder un ouvrage de critique par ses propres œuvres : ce serait avouer par trop naïvement ce qui est presque toujours vrai au fond, que l'on se prend pour le type auquel on rapporte les objets pour les juger : mais ici, il ne s'agit pas d'exécution, il s'agit des idées les plus abstraites qu'il soit donné à l'homme de concevoir ; ici critique et discussion deviennent synonymes, et discuter, c'est mettre aux prises ses idées avec celles des autres.

Nous exposerons donc, dans quelques articles, ce qu'il y a de plus général, de plus philosophique, dans des recherches que mille circonstances ont empêché de publier plus tôt. Nous les présenterons seules, sans complications d'exemples et de hors-d'œuvre, qui chez les analystes noyent d'ordinaire les conceptions générales. Nous les exposerons surtout avec bonne foi, indiquant sans détour la voie qui nous y a conduit, et les obstacles qui nous ont arrêté. Car nous voulons que le lecteur soit aussi instruit que nous des matières que nous aurons traitées. Quand ce but aura été rempli, nous aurons conscience d'avoir bien fait, sinon par le profit qu'en retirera directement la science, du moins par l'exemple donné, d'une bonne loi qu'on n'a pas trouvée jusqu'à ce jour.

Ici comme dans toutes les sciences chaque époque a en quelque sorte ses questions du moment : il y a des questions vivantes qui fixent à la fois les esprits les plus éclairés comme malgré eux et sans que [*illis.*] ait présidé à ce concours. Il semble souvent que les mêmes idées apparaissent à plusieurs comme une révélation. Si l'on en cherche la cause il est aisé de la trouver dans les ouvrages de ceux qui nous ont précédés où ces idées sont présentes à l'insu de leurs auteurs.

La science n'a pas tiré, jusqu'à ce jour, grand parti de cette coïncidence observée si souvent dans les recherches des savants. Une concurrence fâcheuse, une rivalité dégradante en ont été les principaux fruits. Il n'est pourtant pas difficile de reconnaître dans ce fait la preuve que les savants ne sont pas plus que d'autres faits pour l'isolement, qu'eux aussi appartiennent à leur époque et que tôt ou tard ils décupleront leurs forces par l'association. Alors que de temps épargné pour la science !

Beaucoup de questions d'un genre nouveau occupent maintenant les analystes. C'est à découvrir un lien entre ces questions que nous nous attacherons ([15]).

Tout voir, tout entendre, ne perdre aucune idée.
29 7$^{\text{bre}}$ 1831

Sciences.
Hiérarchie. Ecoles

La hiérarchie est un moyen même pour l'inférieur.

Quiconque n'est pas envieux ou a de l'ambition a besoin d'une hiérarchie factice pour vaincre l'envie ou les obstacles.

Jusqu'à ce qu'un homme ait dit : la science c'est moi, il doit avoir un nom à opposer à ceux qu'il combat. Si non, son ambition passera pour de l'envie.

Avant d'être roi il faut être aristocrate. Machiavel.

L'intrigue est un jeu. Si l'on mérite ce qu'on brigue, on y gagne tout. Si non, on perd la partie.

On combat les professeurs par l'institut, l'institut par le passé, un passé par un autre passé.

Voici la [*illis.*] de Victor Hugo. Renaissance, moyen âge, enfin, moi.

C'est à ce besoin de combattre un homme par un autre homme, un siècle par un autre siècle, qu'on doit attribuer les réactions littéraires ou scientifiques, qui ne sont pas de longue durée, Aristote, Ptolémée, Descartes, Laplace.

[*Une ligne illisible.*]

Ce jeu use celui qui s'en sert. Un homme qui n'est pas dévoué se fait éclectique.

Un homme qui a une idée peut choisir entre, avoir, sa vie durant, une réputation colossale d'homme savant, ou bien se faire une école, se taire et laisser un grand nom dans l'avenir. Le premier cas a lieu s'il

pratique son idée sans remettre, le second s'il la publie. Il y a un troisième moyen juste milieu entre les deux autres. C'est de publier et de pratiquer, alors on est ridicule.

---

1. Cette liste se trouve à droite ; à gauche est une autre liste de noms, à peu près les mêmes : tous ces noms sont biffés, sauf ceux de Sturm, de Richard et un autre que je n'ai pu déchiffrer. Parmi les noms de cette première liste, qui ne figurent pas dans la seconde, je distingue ceux de :
Blanchet, Leroy, Poullet de l'Isle, Francœur.
2. Même erreur est arrivée en 1828 à l'auteur (il avait seize ans). Ce n'est pas la seule analogie frappante entre le géomètre norvégien mort de faim, et le géomètre français condamné à vivre ou à mourir, comme on voudra, sous les verrous d'une prison.
(Note de l'éditeur.)
3. Je suis le texte de Chevalier ; il y a dans le manuscrit de Galois un mot illisible.
4. Chevalier, dans sa copie, a supprimé cette phrase : "Ici rien de semblable" et a placé cet alinéa avant le précédent. C'est ainsi qu'il est, en effet, placé dans le texte de Galois ; mais, d'une part, les mots "Ici rien de semblable" ne sont nullement biffés dans le manuscrit ; ils ont, au contraire, été ajoutés en interligne ; d'autre part, ils sont précédés d'un astérisque suivi d'un trait (assez peu distinct) dont l'extrémité indique sans doute la place où l'alinéa doit être placé ; à cette place, les mots supprimés par Chevalier ont un sens très clair ; ils n'en ont pas quand on laisse le second alinéa avant le premier : c'est évidemment la raison pour laquelle Chevalier les a supprimés.
5. On sait assez que le second Mémoire est perdu : toutefois, il subsiste un morceau (non daté) où Galois traite de la division de l'argument dans les fonctions elliptiques et dont le contenu correspond assez bien à l'indication du texte ; on peut donc supposer que ce morceau pouvait rentrer dans l'ensemble que Galois voulait publier. Il sera publié dans un second article.
6. Voici la phrase à laquelle Galois fait allusion : "Tout ce qui précède, je l'ai dit pour prouver que c'est sciemment que je m'expose à la risée des sots."
7. Texte de Chevalier ; on ne distingue que la lettre n ; le reste du mot est un trou.
8. Mot peu lisible, omis par Chevalier.
9. Un mot illisible, je suis le texte de Chevalier.
10. C'est le texte de Chevalier. Le passage est illisible ; je ne puis lire "rencontre" ; après "explorations" qui est douteux, il y a les mots, douteux aussi : "et qui souvent sont imaginaires" et ceux-ci, bien nets : "Mais aussi plus de rôle au savant". Chevalier a supprimé ce qui ne s'accordait pas avec son texte.
11. Chevalier a écrit : "et la. . . ".
12. Je suis le texte de Chevalier ; il y a ici, en interligne, une phrase dont le copiste n'a pas tenu compte, malgré son intérêt ; malheureusement, elle est en partie illisible : j'y distingue à peu près ce qui suit : "toute immatérielle qu'elle [*illis.*] l'analyse n'est pas plus en notre pouvoir que d'autre [*illis.*]."
13. Autre addition, en interligne, supprimée par Chevalier : "il faut l'épier, la sonder, la solliciter [la vérité]".
14. Dans le manuscrit : "qu'il traite".
15. Passage biffé.

ÉCRITS MATHÉMATIQUES INÉDITS.

En dehors des quelques fragments que l'on trouvera plus loin, les écrits mathématiques de Galois que Liouville n'a pas publiés contiennent une cinquantaine de feuilles détachées ([1]) pleines de calculs qui, pour la plupart, concernent la théorie des fonctions elliptiques et remontent sans doute à un moment où Galois étudiait les Mémoires de Jacobi ([2]), quatre pages sur les équations aux dérivées partielles du premier ordre, quelques calculs, avec un commencement de rédaction, sur les intégrales eulériennes ([3]), huit lignes, dont plusieurs mots sont déchirés, qui paraissent se rapporter au groupe alterné et n'avoir pas grand intérêt, un cahier dont la plupart des pages sont blanches et dont je dirai tout à l'heure deux mots, enfin une vingtaine de lignes sur le théorème d'Abel.

Ces vingt lignes peuvent être regardées comme un résumé de la célèbre "Démonstration d'une propriété générale d'une certaine classe de fonctions transcendantes" ([4]), qui est datée de 1829 ; elles occupent les deux tiers de la première page d'une feuille double de même format (30 x 15) que la lettre à Chevalier. On lit en haut de la page :

Théorie des fonctions de la forme $\int X\,\mathrm{d}x$, X étant une fonction algébrique de x.

Les mots "fonctions de la...", jusqu'à la fin, sont biffés et Galois a écrit au-dessus

intégrales dont les différentielles est algébrique.

Le premier titre est presque identique à ceux qui ont été signalés précédemment (p. 17 et p. 23). dont l'un porte la mention "septembre 1831". L'énoncé du théorème d'Abel (qui n'est pas nommé) est précédé des mots "Lemme fondamental". Après la démonstration on lit

Remarque. Dans le cas où

Le reste de la page, les deux pages qui suivent sont en blanc ([5]). Ces quelques lignes sont-elles tout ce qui reste du troisième *Mémoire qui concerne les intégrales*, que Galois résume dans la lettre à Chevalier ? Ce troisième Mémoire a-t-il été rédigé ? Je rappelle quelques termes de la lettre

On pourra faire avec tout cela trois Mémoires.

Le premier est écrit, et... je le maintiens... . . . tout ce que j'ai écrit là est depuis bientôt un an dans ma tête.

Le premier est écrit semble indiquer que les autres ne sont pas rédigés. *On pourra faire avec tout cela trois Mémoires* porte à penser que Galois laissait des notes, dont on ne peut plus espérer aujourd'hui qu'elles soient retrouvées. Une seule chose est certaine, c'est que, la veille de sa mort, *il avait tout cela dans la tête.*

Le cahier est du format 20 x 15 ; on lit sur la couverture : Notes de mathématiques, quatorze pages, seulement, sont utilisées. On trouve dans ce cahier et, parfois, sur la même page, deux sortes d'écriture : pour l'une, il n'y a pas de doute, c'est bien celle de Galois, avec son allure habituelle. L'autre, beaucoup moins lisible, est droite. Je me suis demandé si Galois ne s'était pas amusé à déformer son écriture ; mais M. Paul Dupuy, après un examen attentif des deux écritures, a constaté qu'elles révélaient des habitudes très différentes : elles ne sont pas de la même personne.

Au reste, ce cahier, par son contenu, n'offre qu'un intérêt médiocre. Les pages qui sont de Galois contiennent quelques remarques sur les asymptotes des courbes algébriques et un court essai sur les principes de l'Analyse, dont je citerai quelques lignes ; elles caractérisent un état d'esprit qui résultait sans doute de l'enseignement que Galois avait reçu ; on n'oubliera pas qu'il n'était sans doute alors qu'un écolier, un écolier qui, peut-être, avait approfondi déjà des problèmes singulièrement difficiles.

Après avoir expliqué comment il juge la méthode de Lagrange, où le développement de Taylor tient le rôle essentiel, préférable à la méthode qui consiste à partir de la notion de dérivée considérée comme la limité de l'expression

$$\frac{f(X)-f(x)}{X-x},$$

limite qui ne peut être constamment nulle ou infinie, et comment le raisonnement de Lagrange ne tient pas debout, il propose de lui substituer le suivant :

Considérons d'abord une fonction $\phi(z)$ qui devienne nulle pour la valeur 0 de la variable. Je dis que l'on pourra toujours déterminer un seul nombre positif et fini n de manière que $\frac{\phi(z)}{z^n}$ ne soit ni nulle ni infinie, à moins que $\frac{\phi(z)}{z^n}$ ne soit nul quand $z = 0$, pour toute valeur finie de n.

Car si $\frac{\phi(z)}{z^n}$ n'est pas nul quand $z = 0$ pour toute valeur finie de n, soit m une valeur telle que $\frac{\phi(z)}{z^m}$ ne soit pas nul quand $z = 0$. Si $\frac{\phi(z)}{z^m}$ acquiert alors une valeur finie, la proposition est démontrée. Sinon $\frac{\phi(z)}{z^m}$ étant infini et $\phi(z)$ nul pour $z = 0$, en faisant croître n depuis $n = 0$ jusqu'à $n = m$, les valeurs de $\frac{\phi(z)}{z^m}$ pour $z = 0$ devront être infinies à partir d'une certaine limite. Soit p cette limite. $\frac{\phi(z)}{z^p}$ ne sera pas infini pour $z = 0$ mais $\frac{\phi(z)}{z^{p+\mu}}$ le sera, quelque petite que soit la quantité μ. Donc $\frac{\phi(z)}{z^\mu}$ ne saurait être nul pour $z = 0$. La proposition est donc démontrée.

De cette proposition ainsi "démontrée", Galois conclut qu'une fonction $\phi(s)$, qui ne devient pas infinie pour $z = 0$, peut se mettre sous la forme

$$\phi(z) = A + Bz^n + Cz^m + \ldots + Pz^p + z^k\Psi(z),$$

où les exposants positifs $n, m, \ldots, p, k$ vont en croissant, l'exposant k étant aussi grand qu'on veut et la fonction $\Psi(z)$ n'étant ni nulle ni infinie pour $z = 0$.

De la formule du binôme il déduit ensuite le développement de Taylor.

Quant aux fragments qui suivent, j'ai cru devoir les reproduire tels quels, avec une exactitude minutieuse, en conservant l'orthographe, la ponctuation ou l'absence de ponctuation, sans les quelques corrections qui se présentent naturellement à l'esprit. Cette minutie m'était imposée pour les quelques passages où la pensée de Galois n'était pas claire pour moi ; sur cette pensée, les fragments informes que je publie jetteront peut-être quelque lueur. Je me suis efforcé de donner au lecteur une photographie sans retouche.

J. T.

[Première feuille] ([6]).

Permutations. Nombres de lettres m.

Substitutions. Notation.

Période. Substitutions inverses. Substitutions semblables. Substitutions circulaires. Ordre. Autres substitutions.

Groupes. Groupes semblables. Notation.

Théorème I. Les Permutations communes à deux groupes forment un groupe.

Théorème II. Si un groupe est contenu dans un autre, celui-ci sera la somme d'un certain nombre de groupes semblables au premier, qui en sera dit un *diviseur*.

Théorème III. Si le nombre des permutations d'un groupe est divisible par p (p étant premier), ce groupe contiendra une substitution dont la période sera de p termes.

Réduction des groupes, dépendants ou indépendants. Groupes irréductibles.

Des groupes irréductibles en général.

Théorème. Parmi les permutations d'un groupe, il y en a toujours une où une lettre donnée occupe une place donnée, et, si l'on ne considère dans un groupe irréductible que les permutations où une même lettre occupe une même place et qu'on fasse abstraction de cette lettre, les permutations qu'on obtiendra ainsi formeront un groupe. Soit n le nombre des permutations de ce dernier mn ([7]).

Nouvelle démonstration du théorème relatif aux groupes alternes.

Théorème. Si un groupe contient une substitution complète de l'ordre m et une de l'ordre $m - 1$, il sera irréductible.

Discussion des groupes irréductibles. Groupes, primitif et non primitif. Propriété des racines ([8]).

On peut supposer que le groupe ne contienne que des substitutions paires.

Il y aura toujours un système conjugué complet de m permutations quand $m = 4n$ et $4n + 1$, un système conjugué complet de $\frac{m}{2}$ permutations quand $m = 4n + 2$.

Donc $t = m - 2$ dans le premier cas, $t = (m - 2)/2$ dans le second ([9]).

[Deuxième feuille.]

Application à la théorie des fonctions et des équations algébriques. Fonctions semblables. Combien il peut y avoir de fonctions semblables entre elles. M$^{\text{r}}$ Cauchy. Groupes appartenant aux fonctions. Théorème plus général, quand $m > 4$. Quelles sont les fonctions qui n'ont que m valeurs, ou qui ne contenant que des substitutions paires, n'ont que $2m$ valeurs.

Théorème. Si une fonction de m indéterminées est donnée par une équation de degré inférieur à m dont tous les coefficients soient des fonctions symétriques permanentes ou alternées de ces indéterminées, cette fonction sera elle même symétrique, quand $m > 4$.

Théorème. Si une fonction de m indéterminées est donnée par une équation de degré m dont tous les coefficients, etc. ; cette fonction sera symétrique permanente ou alternée par rapport à toutes les lettres ou du moins par rapport $m - 1$ d'entre elles.

Théorème. Aucune équation algébrique de degré supérieur à 4 ne saurait se résoudre ni s'abaisser.

Du cas où une fonction des racines de l'équation dont le groupe est G est connue.

Théorème. Soit H le groupe d'une fonction ϕ des racines, G est

un diviseur de H, ϕ ne dépendra plus que d'une ([10]) équation du $n^{ième}$ degré.

On peut ramener à ce cas celui où on supposerait plusieurs fonctions connues.

Premier cas. Quand le groupe appartenant à la fonction connue est réductible. Cas où une seule permutation lui appartient.

2$^{\text{e}}$ cas. Quand le groupe appartenant à la fonction est irréductible non primitif.

3$^{\text{e}}$ cas. Quand le groupe appartenant à la fonction est primitif m étant premier ([11]).

4$^{\text{e}}$ cas. Quand le groupe appartenant à la fonction est primitif et que $m = p^2$.

5$^{\text{e}}$ cas. Quand le groupe est primitif $m - 1$ étant premier ou le carré d'un nombre premier ([12]).

Note sur les équations numériques.

Ce qu'on entend par l'ensemble des permutations d'une équation.

Du cas où cet ensemble constitue un groupe.

Il n'y a qu'une circonstance où nous ayons reconnu que cela doit nécessairement avoir lieu. C'est celui où toutes les racines sont des fonctions rationnelles d'une quelconque d'entre elles.

Démonstration.

C'est improprement, etc. Du reste, tout ce que nous avons dit est applicable à ce changement près. 1°. théorème. Si une équation jouit de la propriété énoncée, toute fonction des racines invariable par les $m - 1$ substitutions conjuguées sera connue, et réciproquement. 2° Théorème découlant de la réciproque précédente ([13]). Toute équation dont les racines seront des fonctions rationnelles de la première ; jouira de la même propriété. 3° Corollaire. Si a est une racine imaginaire d'une pareille équation et que fa en soit la conjuguée, fx sera en gén´ral la conjuguée d'une racine quelconque imaginaire, x.

On peut passer aisément de ce cas à celui où une racine étant connue, quelques unes en dépendent par des fonctions rationnelles. Car soient

$$x, \quad \phi_1 x, \quad \phi_2(x), \ldots$$

Ces racines, si l'on prend, etc.

Il est aisé de voir que la même méthode de décomposition s'applique au cas où dans l'ensemble des permutations d'une équation, n mêmes lettres occupent toujours n mêmes places (abstraction faite de l'ordre) quand une seule de ces lettres occupe une de ces places, et il n'est pas nécessaire pour cela que l'ensemble de ces permutations constitue un groupe.

([14])

On appelle groupe un système de permutations tel que etc. Nous représenterons cet ensemble par G.

GS est le groupe engendré lorsqu'on opère sur tout le groupe G la substitution S. Il sera dit semblable ;

Un groupe peut être fort différent d'un autre et avoir les mêmes substitutions. Ce groupe en général ne sera pas GS.

Groupe réductible est un groupe dans les permutations duquel n lettres ne sortent pas de n places fixes. Tel est le groupe

$$\begin{array}{ccc} abcde & abdec & abecd \\ bacde & badec & baecd \end{array}$$

Un groupe irréductible, etc.

Un groupe irréductible est tel qu'une lettre donnée occupe une place donnée. Car, supposons qu'une place ne puisse appartenir qu'à n lettres. Alors toute place occupée par l'une de ces lettres jouira de la même propriété. Donc etc.

Groupe irréductible non-primitif est celui où l'on a n places et n lettres telles que une des lettres ne puisse occuper une de ces places, sans que les n lettres n'occupent les n places.

On voit que les lettres se partageront en classes de n lettres telles que les n places en question ne puissent être occupées à la fois que par l'une de ces places ([15]). d'où

$$TS' = STS' = T - 1ST$$

Sur l'autre face du même fragment, on lit :

Si l'on représente les n lettres par n indices

$$1.2.3 \ldots n$$

toute permutation pourra être représentée

$$\phi 1 \quad \phi 2 \quad \phi 3 \ldots \phi n$$

ϕ étant une fonction convenablement choisie la substitution par laquelle on passe de la première perm. à l'autre sera $(k, \phi k)$, k désignant un indice quelconque.

Au lieu de représenter les lettres par des nombres on pourrait représenter les places par des nombres.

. . . . . .

équations ([16]). Nous nous contenterons donc d'avoir exposé les définitions indispensables pour l'intelligence de la suite et nous allons montrer la liaison qui existe entre les deux théories.

§ 2. Comment la théorie des Équations dépend de celle des Permutations.

6. Considérons une équation à coefficients quelconques et regardons comme rationnelle toute quantité qui s'exprime rationnellement au moyen des coefficients de l'équation, et même au moyen d'un certain nombre d'autres quantités irrationnelles adjointes que l'on peut supposer connues a priori.

Lorsqu'une fonction des racines ne change pas de valeur numérique par une certaine substitution opérée entre les racines, elle est dite invariable par cette substitution. On voit qu'une fonction peut très bien être invariable par telle ou telle substitution entre les racines, sans que sa forme l'indique. Ainsi, si $F(x) = 0$ est l'équation proposée, la fonction $\phi[F(a), F(b), \ldots]$, (ϕ étant une fonction quelconque, $a, b, c \ldots$ les racines) sera une fonction de ces racines invariable par toute substitution entre les racines, sans que sa forme l'indique généralement.

Or c'est une question dont il ne paraît pas qu'on ait encore la solution, de savoir si, étant donnée une fonction de plusieurs quantités numériques, on peut trouver un groupe qui contienne toutes les substitutions par lesquelles cette fonction est invariable, et qui n'en contienne pas d'autres.

Il est certain que cela a lieu pour des quantités littérales, puisqu'une fonction de plusieurs lettres invariables par deux substitutions est invariable par leur produit. Mais rien n'annonce que la même chose ait toujours lieu quand aux lettres on substitue des nombres.

On ne peut donc point traiter toutes les équations comme les équations littérales. Il faut avoir recours à des considérations fondées sur les propriétés particulières de chaque équation numérique. C'est ce que je vais tâcher de faire

Des cas particuliers des équations ([17])

Remarquons que tout ce qu'une équation numérique peut avoir de particulier, doit provenir de certaines relations entre les racines. Ces relations seront rationnelles dans le sens que nous l'avons entendu, c'est à dire qu'elles ne contiendront d'irrationnelles que les coefficients de l'équation et les quantités adjointes. De plus ces relations ne devront pas être invariables par toute substitution opérée sur les racines, sans quoi on n'aurait rien de plus que dans les équations littérales.

Ce qu'il importe donc de connaître, c'est par quelles substitutions peuvent être invariables des relations entre les racines, ou ce qui revient au même, des fonctions des racines dont la valeur numérique est déterminable rationnellement.

A ce sujet, nous allons démontrer un théorème de la dernière importance dans cette matière et dont l'énoncé suit : "*Étant donnée une équation avec un certain nombre de quantités adjointes, il existe toujours un certain groupe de permutations dont les substitutions sont telles* ([18]) que toute fonction des racines invariable par ces substitutions est rationnellement connue, et telle réciproquement qu'une fonction ne peut être rationnellement déterminable, à moins d'être invariable par ces substitutions que nous nommerons substitutions de l'équation." *(Dans le cas des équations littérales, ce groupe n'est autre chose que l'ensemble de toutes les permutations des racines, puisque les fonctions symmétriques sont seules connues).*

Pour plus de simplicité, nous supposerons dans la démonstration de notre théorème, qu'il ait été reconnu pour toutes les équations de degrés inférieurs ; ce qu'on peut toujours admettre puisqu'il est évident pour les équations du second degré.

Admettons donc la chose pour tous les degrés inférieurs à m ; pour la démontrer dans le $m^{ième}$, nous distinguerons quatre cas :

1er Cas. L'équation se décomposant en deux ou en un plus grand nombre de facteurs.

Soit $U = 0$ l'équation, $U = VT, V$ et T étant des fonctions dont les coefficients se déterminent rationnellement au moyen des coefficients de la proposée et des quantités adjointes.

Je vais faire voir que, dans l'hypothèse, on pourra trouver un groupe qui satisfasse à la condition énoncée.

Remarquons ici que dans ces sortes de questions, comme il ne s'agit que, des substitutions par lesquelles des fonctions sont invariables, si un groupe satisfait à la condition, tout groupe qui aurait les mêmes substitutions y satisfera aussi. Il convient donc de partir toujours d'une permutation arbitraire, mais fixe, afin de déterminer les groupes que l'on aura à considérer. De cette manière, on évitera toute ambiguïté.

Cela posé, dans le cas actuel, il est clair que si l'on adjoignait à l'équation $U = 0$, toutes les racines de l'équation $V = 0$, l'équation $U = 0$ se décomposerait en facteurs dont l'un serait $T = 0$, et les autres seraient les facteurs simples de V.

Soit H le groupe que l'on obtient en opérant sur une permutation arbitraire A des racines de l'équation $U = 0$, toutes les substitutions qui sont relatives à l'équation $T = 0$ quand on lui adjoint les racines de $V = 0$.

Soit K le groupe que l'on obtient en opérant sur toutes les substitutions qui sont relatives à $V = 0$ quand on ne lui adjoint que les quantités adjointes primitivement à la proposée.

Combinez en tous sens toutes les substitutions du groupe H avec celles du groupe K. Vous obtiendrez un groupe réductible que je dis jouir de la condition exigée relativement à la question proposée.

En effet toute fonction invariable par les substitutions du groupe K ([19] [20])

Soit donc $\phi(H)$ une certaine fonction invariable par les substitutions du groupe H et non par celles du groupe G. On aura donc

$$\phi(H) = f(r)$$

la fonction y ne contenant dans son expression que les quantités antérieurement connues.

Éliminons algébriquement r entre les équations

$$r^p = A \quad f(r) = z$$

On aura une équation irréductible du $p^{ième}$ degré en z. (Sinon z serait fonction de r^p : ce qui est contre l'hypothèse). Maintenant soit S une des substitutions du groupe G qui ne lui soient pas communes à H. On voit que $\phi(HS)$ sera encore racine de l'équation ci-dessus en z, puisque les coefficients de cette équation sont invariables par la substitution S.

On aura donc

$$\phi(HS) = f(\alpha r)$$

α étant une des racines de l'unité.

Ces deux équations

$$\phi(H) = f(r) \quad \phi(HS) = f(\alpha r)$$

donneront par l'élimination de r une relation entre

$$\phi(H) \quad \phi(HS) \quad \text{et } \alpha$$

indépendante de r, et la même relation aura par conséquent lieu entre

$$1 + \phi(H) \quad \text{et} \quad \phi(HS^2)$$

Donc : comme

$$\phi(HS) = f(\alpha r)$$

on en déduit

$$\phi(HS^2) = f(\alpha^2 r)$$

et ainsi de suite, jusqu'à

$$\phi(HS^p) = f(r) = \phi(H)$$

Ainsi la connaissance de la seule quantité r, donne à la fois toutes les fonctions correspondantes aux groupes

$$H, HS, HS^2, ...$$

la somme de ces groupes est évidemment G, puisque toute

Étant donnée ([21]) une équation avec tant de quantités adjointes que l'on voudra, on peut toujours trouver quelque fonction des racines qui soit numériquement invariable par toutes les substitutions d'un groupe donné et ne le soit pas par d'autres substitutions.

Si le groupe d'une équation se décompose en n groupes semblables H, HS, HS ([22]), et qu'une fonction $\phi(H)$ soit invariable par toutes les substitutions du groupe H par aucune autre substitution du groupe G, cette fonction est racine d'une équation irréductible du $n^{ième}$ degré dont les autres racines sont $\phi(HS)$, ...

Note ([23]).

On appelle équations non-primitives les équations qui, étant, par exemple du degré mn se décomposent en m facteurs du degré n au moyen d'une seule équation du degré m. Ce sont les Equations de M$^{\text{r}}$ Gauss. Les équations primitives sont celles qui ne jouissent pas d'une pareille simplification. Je suis, à l'égard des Equations primitives, parvenu aux résultats suivants :

1° Pour qu'une équation primitive de degré m soit résoluble par radicaux, il faut que $m = p^\nu, p$ étant un nombre premier

2° Si l'on excepte le cas de $m = 9$ et $m = p^p$, l'équation devra être telle que deux quelconques de ses racines étant connues, les autres s'en déduisent rationnellement.

3° Dans le cas de $m = p^p$, deux des racines étant connues, les autres doivent s'en déduire du moins par un seul radical du degré p.

4° Enfin dans le cas de $m = 9$, l'équation doit être du genre de celles qui déterminent la trisection des fonctions Elliptiques.

La démonstration de ces propositions est fondée sur la théorie des permutations. ([24])

Addition au mémoire sur la résolution des équations.

Lemme I. Soit un groupe G de $mt.n$ permutations, qui se décompose en n groupes semblables à H. Supposons que le groupe H se décompose en t groupes de m permutations, et semblables à K.

Si, parmi toutes les substitutions du groupe G, celles du groupe H sont les seules qui puissent transformer l'une dans l'autre quelques substitutions du groupe K, on aura $n \equiv 1 \pmod m$ ou $tn \equiv t \pmod m$.

Lemme II. Si μ est un nombre premier, et p un entier quelconque on aura

$$(x-p)(x-p^2)(x-p^3)\dots(x-p^{\mu-1}) \equiv \frac{x^\mu - 1}{x-1} \left(\text{mod } \frac{p^\mu - 1}{p-1}\right).$$

Ces deux lemmes permettent de voir dans quel cas un groupe primitif de degré p^ν (où p est premier) peut appartenir à une équation résoluble par radicaux.

En effet, appelons G un groupe qui contient toutes les substitutions linéaires possibles par les $\frac{p^\nu - 1}{p-1}$ lettres. (Voyez le mémoire cité.) Soit, s'il est possible, L un groupe qui divise G et qui se partage lui-même en p groupes semblables à K, K ne comprenant pas deux permutations où une lettre occupe la même place. On peut prouver 1° que s'il y a dans le groupe G et hors du groupe L, quelque substitution S qui transforme l'une dans l'autre quelques substitutions du groupe K, cette substitution sera de r termes, r étant un diviseur de $p-1$.

D'après cela, comme le nombre de permutations du groupe G est $\frac{p^\nu - 1}{p-1}.(p^\nu - p^{\nu-1})(p^\nu - p^{\nu-2})\dots(p^\nu - p^2)(p^\nu - p)$

d'après le lemme I, on devra avoir ([25])

$$(p^\nu - p^{\nu-1})(p^\nu - p^{\nu-2})\dots(p^\nu - p^2)(p^\nu - p) \equiv p^k r \left(mod\ \frac{p^\nu - 1}{p-1}\right)$$

D'où l'on voit que ν doit être un nombre premier ([26]). (Lemme II)

$$pr \equiv \nu \left(mod\ \frac{p^\nu - 1}{p-1}\right)$$

On en déduit quand $\nu > 2 \quad pr = \mu$, savoir $p = \nu$, puisque p et μ sont premiers.

Ainsi, le théorème que j'avais énoncé dans mon mémoire sera vrai dans tout autre cas que dans celui où p serait élevé à la puissance p.

Toujours devra-t-on avoir $r = 1$, et $L = H$. Ainsi même dans le $p^{p^{ième}}$ degré le groupe de l'équation réduite du degré $\frac{p^p - 1}{p-1} =$ devra être de $\frac{p^p - 1}{p-1} p$ permutations. La règle est donc encore fort simple dans ce cas.

il faut comme on voit 1° que $\nu = 1$; 2° que le groupe de la réduite soit de $\frac{p^p - 1}{p-1} p =$ permutations

([27])

Dans un mémoire sur la théorie des Equations, j'ai fait voir comment on peut résoudre une équation algébrique de degré premier m, dont les racines sont $x_0, x_1, x_2, \ldots, x_{m-1}$, quand on suppose connue la valeur d'une fonction des racines qui ne demeure invariable que par les substitutions de la forme (x_h, x_{ak+b}). Or il arrive, par un hasard que nous n'avions pas prévu, que la Méthode proposée dans ce mémoire s'applique avec succès à la division d'une fonction elliptique de première classe en un nombre premier de parties égales. Nous pourrions, à la rigueur, nous contenter de donner cette division, et le problème de la section des fonctions de première classe pourrait être considéré comme résolu.

Mais, afin de rendre cette solution plus générale, nous nous proposerons de diviser une fonction elliptique de première classe en m parties égales, m étant $= p^n$ et p premier.

Pour cela nous étendons d'abord la méthode exposée dans le mémoire cité, au cas où le degré de l'équation serait une puissance de nombre premier. Nous supposerons toujours que les racines soient $x_0, x_1, x_2, \ldots, x_{m-1}$, et que l'on connaisse la valeur d'une fonction de ces racines qui ne demeure invariable que pour des substitutions de la forme $(k, ak + b)$.

Dans cette expression, k et $ak + b$ signifieront les restes minima de ces quantités par rapport à m. Parmi les substitutions de cette forme, que, pour abréger, nous appelerons substitutions linéaires, il est clair que l'on ne peut admettre que celles où a est premier avec m, sans quoi une même $ak+b$ remplacerait à la fois plusieurs k.

Cela posé, passons à la resolution de la classe d'équations indiquée.

§ 1. *Résolution de l'équation algébrique de degré p^n en y supposant connue la valeur d'une fonction qui n'est invariable que par des substitutions linéaires.*

La congruence $k = ak+b$ n'étant pas soluble pour plus d'une seule valeur, on voit clairement que la fonction qu'on suppose connue n'est invariable par aucune substitution dans laquelle deux lettres garderaient un même rang.

Si donc, mutatis mutandis, on applique à ce cas les raisonnements employés dans le mémoire cité, on vérifiera l'énoncé de la proposition qui suit :

"Étant supposée connue la valeur de la fonction en question, une racine s'exprimera toujours au moyen de deux autres, et l'égalité qu'on obtiendra ainsi sera invariable par les substitutions telles que $(k, ak+b)$."

Soit donc $x_2 = f(x_1, x_0)$ on en déduira en général,

$$x_{2a+b} = f(x_{a+b}, x_b),$$

équation qui, appliquée de toutes manières, donnera l'expression d'une quelconque des racines de deux autres quelconques, si l'on a soin d'y substituer successivement les expressions des racines qui entrent dans cette équation.

Cela posé, prennons une fonction symmétrique Φ des racines $x_0, x_p, x_{2p}, x_{3p}, \ldots, x_{(p^{n-1}-1)p}$; il vient

$$\Phi(x_0, x_p, x_{2p}, \ldots) = \Phi_0$$

$$\Phi(x_1, x_{p+1}, x_{2p+1}, \ldots) = \Phi_1$$

$$\Phi(x_2, x_{p+2}, x_{2p+2}, \ldots) = \Phi_2$$

$$- - - - - - - -$$

$$\Phi(x_{p-1}, x_{2p-1}, \ldots) = \Phi_{p-1}$$

et supposons qu'en général $\Phi_{k+p} = \Phi_{p-1}$ Toute fonction des quantités Φ, qui sera invariable par les substitutions linéaires de ces quantités, sera évidemment une fonction invariable par les substitutions linéaires

de $x_0, x_1, x_2, \ldots, x_{m-1}$. Ainsi l'on connaitra à priori toute fonction des quantités, $\Phi_0, \Phi_1, \ldots, \Phi_{p-1}$, invariable par les substitutions linéaires de ces quantités. On pourra donc 1° former l'équation dont ces quantités sont racines (puisque toute fonction symmétrique est à plus forte raison invariable par les substitutions) ; 2° résoudre cette équation.

Il suit de là, qu'on pourra toujours, au moyen d'une équation de degré p, algébriquement soluble, diviser l'équation proposée en facteurs dont les racines seront respectivement

$$x_0, x_p, x_{2p}, x_{3p}, \ldots$$

$$x_1, x_{p+1}, x_{2p+1}, x_{3p+1}, \ldots$$

$$- - - - - - - - - -$$

Comme dans chaque facteur on aura l'expression d'une racine au moyen de deux autres, par exemple, dans le premier,

$$f(x_p, x_0) = x_{2p}$$

et que cette expression sera invariable par toute substitution linéaire, on voit que chaque facteur pourra se traiter comme l'équation donnée, et que le problème, s'abaissant successivement, sera enfin résolu.

On peut en conséquence regarder comme solubles les équations dans lesquelles on connaîtrait la valeur d'une fonction des racines qui ne serait invariable que par des substitutions linéaires, quand le degré de l'équation est une puissance de nombre premier.

Nous pouvons donc passer à la solution du problème général de la section des transcendantes de première classe, puisque, toute fraction étant la somme de fractions dont les dénominateurs sont des puissances de nombres premiers, il suffit d'apprendre à diviser ces transcendantes en p^n parties égales.

§ 2. *Division des transcendantes de première espèce en $m = p^n$ parties égales.*

Nous déterminerons chaque transcendante par le sinus de son amplitude. On pourrait de la même manière prendre le cosinus ou la tangente, et il n'y aurait rien à changer à ce que nous allons dire.

Nous désignerons par (x, y) le sinus de la transcendante somme des transcendantes dont les sinus sont x et y. Si x est le sinus d'une transcendante, $(x)^k$ désignera celui d'une transcendante k fois plus grande.

Il est clair que $(x, -y)$ sera le sinus de la différence des transcendantes qui ont pour sinus, d'après la notation indiquée pour les sommes.

Cela posé, nous commencerons par une remarque sur la nature des quantités qui satisfont à l'équation $(x)^m = 0$.

Si l'on désigne par p l'une de ses racines, il est clair que $(p)^k$ en sera une autre. L'on aura donc une suite de racines exprimée par $p, (p)^2, (p)^3, \ldots, (p)^{m-1}$. Le nombre des racines étant $> m$, soit q une des racines qui ne sont pas comprises dans cette suite, $(q)^l$ sera une autre racine différente de q et des premières. Car, si l'on avait $(p)^k = (q)^t$ on en déduirait $q = (q)^g, g$ étant un nombre entier.

Prenant donc les deux suites $p, (p)^2, \ldots$ et $q, (q)^2, \ldots$ on trouvera pour la formule générale des racines de l'équation $(x)^m = 0$, cette expression

$$((p)^k, (q)^l)$$

Cela posé, supposons que l'on donne à résoudre l'équation $(x)^m = \sin A$, m étant impair et toujours de la forme p^n. Si x est une des racines, il est clair que toutes les autres seront

$$(x, (p)^k, (q)^l)$$

Posons donc en général

$$(x, (p)^k, (q)^l) = x_{k,l}$$

en faisant $x = x_{00}$ nous en déduirons généralement

$$(x_{2a+b,2c+d} - x_{a+b,c+d}) = (x_{a+b,c+d} - x_{b,d})$$

d'où

$$(x_{2a+b,2c+d} = ((x_{a+b,c+d})^2, x_{b,d})$$

Or il est aisé de tirer de cette égalité une expression rationnelle de $x_{2a+b,2c+d}$ en fonction de $x_{a+b,c+d}$ et de $x_{b,d}$. Car si ϕ est l'arc correspondant à l'un quelconque des sinus qui satisfont à l'équation $(x)^m = \sin A$ pour avoir $\cos\phi$ en fonction de $\sin\phi$, il suffit de chercher le plus grand commun diviseur entre les équations $x^2 + y^2 = 1$ et $f(y) = \cos A$, $f(y)$ étant le cosinus de la transcendante m fois plus grande que celle dont le cosinus est y. On trouverait de même $\Delta\varphi$ en fonction rationnelle de $\sin\varphi$.

Ou pourra donc, par les formules connues, exprimer

$$x_{2a+b,2c+d} = f(x_{a+b,c+d}, x_{b,d})$$

en fonction rationnelle de $x_{a+b,c+d}$ et de $x_{b,d}$

Ce principe posé, démontrons la proposition suivante :

"Toute fonction rationnelle de $x_{0,0}, x_{1,0}, x_{0,1}, \ldots$ invariable par les substitutions de la forme $(x_{k,l}, x_{ak+b,cl+d})$ immédiatement connue."

En effet, on pourra d'abord rendre cette fonction fonction de $x_{0,0}, x_{1,0}, x_{0,1}$ seuls, par l'élimination des autres racines. Cette fonction ne changerait pas de valeur si à la place de $x_{0,0}, x_{1,0}, x_{0,1}, \ldots$ on mettait $x_{0,0}, x_{1,0}, x_{k,l}$, k n'étant pas nul.

Or, comme toute racine de la forme $x_{0,1}$ s'exprime en fonction rationnelle de $x_{0,0}$, et $x_{0,l}$, il s'ensuit que toute fonction symmétrique des racines dans lesquelles le premier indice n'est pas nul sera connue en fonction rationnelle et entière de $x_{0,0}$ et de $x_{0,l}$. Donc la fonction que nous considérions tout à l'heure ne variant pas quand on met pour $x_{1,0}$ l'une quelconque des racines dont le premier indice n'est pas nul, cette fonction sera une fonction de $x_{0,0}$, et de $x_{0,l}$, seuls. On éliminera encore $x_{0,1}$ de cette fonction qui deviendra fonction de $x_{0,0}$ et enfin une quantité connue.

Le principe est donc démontré.

Cela posé soit F une fonction symmétrique de certaines racines de l'équation proposée. Posons

$$F(x_{0,0}, x_{0,1}, x_{0,2}, \ldots) = y_0$$

$$F(x_{1,0}, x_{1,1}, x_{1,2}, \ldots) = y_1$$

$$F(x_{2,0}, x_{2,1}, x_{2,2}, \ldots) = y_2$$

Prenons une fonction de $y_0, y_1, y_2 \ldots$ invariable par les substitutions linéaires de ces quantités. Il est clair que cette fonction sera une fonction des racines x invariable par toute substitution telle que ([28]) $(x_{k,l,ak+b,ck+d})$. Cette fonction sera donc connue. On pourra donc, par la méthode que j'ai indiquée, trouver les valeurs de $y_0, y_1, y_2 \ldots$ et par conséquent décomposer l'équation proposée en facteurs dont l'un ait pour racines $x_{0,0}, x_{0,1}, x_{0,2}, \ldots$

On trouverait de même un facteur de la même équation dont les racines seraient $x_{0,0}, x_{1,0}, x_{2,0}, \ldots$. On pourra donc en cherchant le plus grand commun diviseur de ces deux facteurs avoir $x_{0,0}$, qui est l'une des solutions cherchées. Il en serait de même des autres racines. ([29])

Note 1. sur l'intégration des équations linéaires.

Soit l'équation linéaire à coefficients variables

$$\frac{d^n y}{dx^n} + P\frac{d^{n-1}y}{dx^{n-1}} + Q\frac{d^{n-2}y}{dx^{n-2}} \ldots + S\frac{dy}{dx} + Ty = V$$

Pour l'intégrer supposons que nous connaissions n solutions

$$y = u_1 \quad , = u, \ldots, = u_n$$

de cette équation privée de second membre. La solution complète

$$y = \alpha_1 u_1 + \alpha_2 u_2 + \alpha_3 u_3 + \ldots + \alpha_n u_n$$

qui convient à l'équation privée de second membre, satisfera encore quand on supposera ce second membre, si au lieu de regarder $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ comme constantes, on les considère comme déterminées par les équations suivantes en $\frac{dx_1}{dx}, \frac{dx_2}{dx}, \ldots \frac{dx_n}{dx}$

$$(1)\begin{cases} u_1\frac{d\alpha_1}{dx}+u_2\frac{d\alpha_2}{dx}+u_3\frac{d\alpha_3}{dx}+\ldots+u_n\frac{d\alpha_n}{dx}=0 \\ \frac{du_1}{dx}\frac{d\alpha_1}{dx}+\frac{du_2}{dx}\frac{d\alpha_2}{dx}+\frac{du_3}{dx}\frac{d\alpha_3}{dx}+\ldots+\frac{du_n}{dx}\frac{d\alpha_n}{dx}=0 \\ \frac{d^2u_1}{dx^2}\frac{d\alpha_1}{dx}+\frac{d^2u_2}{dx^2}\frac{d\alpha_1}{dx}+\frac{d^2u_3}{dx^2}\frac{d\alpha_3}{dx}+\ldots+\frac{d^2u_n}{dx^2}\frac{d\alpha_n}{dx} \\ \ldots \\ \frac{d^{n-1}u_1}{dx^{n-1}}\frac{d\alpha_1}{dx}+\frac{d^{n-1}u_2}{dx^{n-1}}\frac{d\alpha_1}{dx}+\frac{d^{n-1}u_3}{dx^{n-1}}\frac{d\alpha_3}{dx}+\ldots+\frac{d^2u_n}{dx^{n-1}}\frac{d\alpha_n}{dx}=V \end{cases}$$

Il importe d'abord de reconnaître si le dénominateur commun aux valeurs tirées de ces équations peut ou non être nul.

Pour cela j'observe que ce dénominateur est le même que celui des n équations suivantes résolues par rapport à $PQ\ldots ST$

$$(2)\quad\begin{cases} \frac{d^nu_1}{dx^n}+P\frac{d^{n-1}u_1}{dx^{n-1}}+Q\frac{d^{n-2}u_1}{dx^{n-2}}+\ldots+S\frac{du_1}{dx}+Tu_1=0 \\ \frac{d^nu_2}{dx^n}+P\frac{d^{n-1}u_2}{dx^{n-1}}+Q\frac{d^{n-2}u_2}{dx^{n-2}}+\ldots+S\frac{du_2}{dx}+Tu_2=0 \\ \frac{d^nu_3}{dx^n}+P\frac{d^{n-1}u_3}{dx^{n-1}}+Q\frac{d^{n-2}u_3}{dx^{n-2}}+\ldots+S\frac{du_3}{dx}+Tu_3=0 \\ \ldots \\ \frac{d^nu_n}{dx^n}+P\frac{d^{n-1}u_n}{dx^{n-1}}+Q\frac{d^{n-2}u_n}{dx^{n-2}}+\ldots+S\frac{du_n}{dx}+Tu_n=0 \end{cases}$$

Or ces équations doivent être parfaitement déterminées, puisque la forme d'une équation différentielle dépend uniquement de celle de l'équation intégrale.

Donc le dénominateur en question n'est jamais nul.

Mais on peut de plus le calculer d'avance. Soit D le dénominateur. Il est aisé de voir que l'on aura

$$\frac{dD}{dx}=D_n+D_{n-1}+D_{n-2}+D_{n-3}+\ldots+D_1$$

$D1$ étant ce que devient D quand on y substitue partout $\frac{d^nu}{dx^n}$ à la place de $\frac{d^{n-1}u}{dx^{n-1}}$, $Dn-1$ ce que devient D quand on y met $\frac{d^{n-1}u}{dx^{n-1}}$ au lieu de $\frac{d^{n-2}u}{dx^{n-2}}$ et ainsi de suite enfin $D1$ ce que devient D par la substitution de $\frac{du}{dx}$ la place de u

Et comme toutes les parties sont nulles excepté D_n il reste

$$\frac{dD}{dx}=D_n$$

Mais on a d'ailleurs

$$P=-\frac{D_n}{D}$$

Puisque $-Dn$ est le numérateur de l'expression de P tirée de (2).

Donc $D=e^{-\int Pdx}$ valeur cherchée du dénominateur.

On pourrait de cette dernière formule déduire celle que nous avons trouvée plus haut, en considérant une équation linéaire de l'ordre n, comme remplaçant n équations simultanées seulement du premier ordre. Quant à la détermination des numérateurs des quantités inconnues, et à l'examen du cas où l'on n'aurait qu'une partie des solutions de la question, nous n'entrerons pas dans ces détails auxquels le lecteur suppléera au moyen des principes émis plus haut.

RECHERCHE SUR LES SURFACES DU 2$^{\text{d}}$ DEGRÉ ([30]).

Problème ([31]). Étant données dans un parallélépipède les trois arêtes m, m', m'', et les angles $\theta, \theta', \theta''$, que font entre elles respectivement m' et m'', m et m'', trouver l'expression des angles de la diagonale avec les arêtes.

Soit $m = OM, m' = OM', m" = OM"$. Si l'on cherche l'angle POM que la diagonale OP forme avec OM, on aura dans le triangle OPM

$$\cos POM = \frac{m^2 + OP^2 - \overline{PM}^2}{2m.OP}$$

Mais on a par la géométrie

$$\overline{OP}^2 = m^2 + m'^2 + 2m'm'' \cos\theta + 2mm'' \cos\theta' + 2mm' \cos\theta'$$
$$\overline{PM}^2 = m'^2 + m''^2 + 2m'm'' \cos\theta$$

d'où l'on tire

$$m^2 + \overline{OP}^2 - \overline{PM}^2 = 2m(m + m'' \cos\theta' + m'' \cos\theta'')$$

et enfin

$$\cos POM = \frac{m + m'' \cos\theta' + m' \cos\theta''}{OP}$$

On trouvera de même pour les cosinus des angles $M'OP$ et $M"OP$

$$\frac{m + m'' \cos\theta + m \cos\theta''}{OP} \qquad \text{et} \qquad \frac{m'' + m' \cos\theta + m \cos\theta'}{OP}$$

Le problème est donc résolu.

Problème. Trouver pour des axes quelconques la condition de perpendicularité d'une droite et d'un plan.

Prenons à partir de l'origine et suivant certaine direction $OP = 1$. Appelons $m, m', m"$ les coordonnées du point P. Les équations de toute droite parallèle à OP, seront de la forme

$$\frac{x - a}{m} = \frac{y - b}{m'} = \frac{z - c}{m''}$$

Les quantités $m, m', m"$ étant liées par la relation

$$1 = m^2 + m'^2 + m''^2 + 2m'm'' \cos\theta + 2mm' \cos\theta''$$

Cherchons de même l'équation d'un plan perpendiculaire à OP.

Il est évident que si on appelé x, y, z les coordonnées de ce plan, et que l'on projette orthogonalement sur OP ces coordonnées la somme des projections devra être constante. Or on connaît, par le problème précédent, les cosinus des angles de la droite OP avec les axes. L'équation du plan sera donc.

$$(m + m' \cos\theta'' + m'' \cos\theta')x + (m' + m \cos\theta'' + m'' \cos\theta)y + (m'' + m \cos\theta' + m' \cos\theta)z + p = 0$$

Et il est remarquable que le premier membre de cette équation exprime aussi la distance à ce plan d'un point quelconque dont les coordonnées sont x, y, z. Ce qui est évident puisque ce premier membre n'est autre chose que la somme des projections des coordonnées d'un point sur la droite OP, augmentée de la distance du plan à l'origine.

Cela posé, soit l'équation d'une surface du second degré rapportée à des axes obliques

$$Ax^2 + A'y^2 + A''z^2 + 2Byz + 2B'xz + 2B''xy + 2Cx + 2C'y + 2C''z + D = \phi(x, y, z) = 0$$

Lorsqu'on cherche l'équation du plan qui divise également toutes les cordes parallèles à une droite donnée, on substitue l'équation $\phi(x, y, z) = 0$ à la place de x, y, z,

$$x + \rho m \quad y + \rho m' \quad z + \rho m''$$

et les racines de l'équation en ρ qu'on obtient ainsi, expriment les distances du point (x, y, z) aux deux points où une corde parallèle à la droite $\frac{x}{m} = \frac{y}{m'} = \frac{z}{m''}$ menée par le point (x, y, z) coupe la surface du

second degré. Ces deux distances devant être égales et de signe contraire, il suffira de faire dans l'équation en ρ le second terme nul pour avoir l'équation du plan diamétral.

Or l'équation en ρ est en faisant

$$M = \phi(m, m', m'')$$

$$\begin{aligned} MP = (Am + B''m' + B'm'')x \quad & +(A'm' + b''m + Bm'')y \\ & +(A''m'' + B'm + Bm')z + Cm + C'm' + C''m'' \end{aligned}$$

de la forme

$$\rho^2 + 2P\rho + Q = 0$$

Si l'on cherche l'équation d'un plan principal, il faudra de plus que le plan représenté par $P = 0$ soit perpendiculaire à la droite $\frac{x}{m} = \frac{y}{m'} = \frac{z}{m''}$ et par conséquent que son équation soit de la forme

$$\begin{aligned} (m + m'\cos\theta'' + m''\cos\theta')x + (m' + m\,\cos\theta'' + m''\cos\theta)y \\ + (m'' + m\,\cos\theta' + m''\cos\theta)z + p = S = 0 \end{aligned}$$

Il faudra donc que les coefficients de MP et ceux de S soient proportionnels et que l'on ait

$$\frac{MP}{S} = \text{const} = s$$

La quantité étant telle que l'on ait

$$\begin{aligned} (A - s)m + (B'' - s\,\cos\theta'')m' + (B' - s\,\cos\theta')m'' = 0 \\ (A' - s)m' + (B'' - s\,\cos\theta'')m + (B - s\,\cos\theta)m'' = 0 \\ (A'' - s)m'' + (B' - s\,\cos\theta')m + (B - s\,\cos\theta)m'' = 0 \end{aligned}$$

On en déduit l'équation en s,

$$\begin{aligned} 0 =& (A - s)(B - s\,\cos\theta)^2 + (A' - s)(B' - s\,\cos\theta')^2 + (A'' - s)(B'' - s\,\cos\theta'')^2 \\ & - (A - s)(A' - s)(A'' - s) - 2(B - s\,\cos\theta)(B' - s\,\cos\theta'') \end{aligned}$$

qui est du troisième degré parce qu'en effet il existe trois plans principaux.

Mais la quantité s et l'équation qui la détermine jouissent d'une propriété fort remarquable que personne jusqu'ici ne paraît avoir observée.

Supposons que l'on transforme les coordonnées en exprimant les anciennes coordonnées d'un point en fonction des nouvelles. Si on substitue les valeurs de x, y, z en x', y', z' dans la fonction $\varphi(x, y, z)$ on obtient une fonction $\varphi'(x', y', z')$ d'une autre forme, et qui est telle que dans la fonction φ on substitue les anciennes coordonnées d'un point déterminé, et dans la fonction φ' les nouvelles, les deux résultats ainsi obtenus sont égaux.

Cela posé reprenons l'expression de s, $s = \frac{MP}{S}$ la quantité M étant le résultat de la substitution des coordonnées du point pris sur une droite fixe à une distance $= 1$ de l'origine c'est à dire d'un point fixe, dans l'équation de la surface, ne variera pas quand on transformera les coordonnées.

La quantité P exprimant la demi-somme des distances d'un point (x, y, z) à la surface distances comptées suivant une droite fixe, est aussi invariable par la transformation des coordonnées. Enfin la quantité S exprimant la distance d'un point à un plan déterminé, ne saurait non plus varier.

La quantité s est donc elle même invariable pour un même plan principal, et l'équation qui donne ses trois valeurs aura des coefficients invariables. Or en la développant, on a

$$\begin{aligned} & (1 - \cos^2\theta - \cos^2\theta' - \cos^2\theta'' + 2\cos\theta\cos\theta\cos\theta'')s^3 \\ & - s^2[A\,\sin^2\theta + A'\,\sin^2\theta' + A''\sin^2\theta'' + 2b(\cos\theta'\,\cos\theta'' - \cos\theta) \\ & + 2B'(\cos\theta\,\cos\theta'' - \cos\theta') + 2B''(\cos\theta\,\cos\theta' - cos\theta'')] \\ & + s(A'A'' + AA'' + AA' - 2AB\,\cos\theta 2A'B'\cos\theta' - 2A''B''\cos\theta'' \\ & - B^2 - B'^2 - B''^2 + 2B'B''\cos\theta \\ & + 2BB''\cos\theta' + 2BB'\cos\theta'') + AB^2 + A'B'^2 + A''B''^2 - AA'A'' - 2BB'B'' = 0 \end{aligned}$$

Divisant tous les coefficients par le premier ou par le dernier on aura trois fonctions des constantes qui entrent dans l'équation de la surface, invariables par la transformation des coordonnées. Si l'on suppose cos $\theta, \cos\ \theta'$ et cos θ" nuls on aura pour tous les systèmes d'axes où cela peut être c'est à dire d'axes rectangulaires,les équations

$$A + A' + A'' = \text{const}$$

$$B^2 + B'^2 + B''^2 - A'A'' - AA''AA' = \text{const}$$

$$AB^2 + A'B'^2 + A''B''^2 - AA'A'' - 2BB'B'' = \text{const}$$

Également si l'on suppose encore dans l'équation en s, B, B', B" nuls, c'est à dire qu'on suppose la surface rapportée à des diamètres conjugués, en divisant toute l'équation par le dernier terme, on trouvera pour tous les systèmes semblables

$$\frac{1 - \cos^2\theta - \cos^2\theta' - \cos^2\theta'' + 2\cos\theta\cos\theta'\cos\theta''}{AA'A''} = \text{const}$$

$$\frac{\sin^2\theta}{A'A''} + \frac{\sin^2\theta'}{AA''} + \frac{\sin^2\theta''}{AA'} = \text{const}$$

$$\frac{1}{A} + \frac{1}{A'} + \frac{1}{A''} = \text{const}$$

Et comme $\frac{1}{A}, \frac{1}{A'}, \frac{1}{A''}$ expriment dans ce cas les carrés des diamètres, on retrouve ici les théorèmes connus.

FIN.

---

1. Trois de ces feuilles comportent du texte ; une se rapporte à la théorie de la transformation, une autre au théorème d'addition pour la fonction sin am, déduit de la formule fondamentale de trigonométrie sphérique, la troisième au théorème d'addition pour la fonction $\Pi(u, a)$.

2. Les papiers que m'a remis Mme de Blignières contiennent un brouillon, couvert de ratures et de corrections, qui est de la main de Liouville, et qui porte en tête : Lettre d'Alfred Galois à M. Jacobi, 17 novembre 1847. Voici cette lettre :
   Monsieur,
   J'ai l'honneur de vous envoyer, en vous priant d'en agréer l'hommage, un exemplaire de la première Partie des Œuvres mathématiques de mon frère. Il y a près d'un an qu'elle a paru dans le Journal de M. Liouville, et, si je ne vous l'ai pas adressée plus tôt, c'est que, sans cesse, j'espérais pouvoir vous faire remettre d'un jour à l'autre l'Ouvrage complet, dont la publication s'est trouvée retardée par diverses circonstances. Au reste, cette première Partie renferme ce que mon pauvre Évariste a laissé de plus important et nous n'avons guère à y ajouter que quelques fragments arrachés au désordre de ses papiers. Ainsi on n'a rien retrouvé concernant la théorie des fonctions elliptiques et abéliennes ; on voit seulement qu'il s'était livré la plume à la main à une étude approfondie de vos Ouvrages. Quant à la théorie des équations, M. Liouville et d'autres géomètres que j'ai consultés affirment que son Mémoire, si durement repoussé par M. Poisson, contient les bases d'une doctrine très féconde et une première application importante de cette doctrine. "Ce travail, me disent-ils, assure pour toujours une place à votre frère dans l'histoire des Mathématiques." Malheureusement étranger à ces matières, j'écoute avec plaisir de telles paroles : si votre précieux suffrage, qu'Évariste aurait ambitionné par-dessus tout, venait les confirmer, ce serait pour ma mère et pour moi une bien grande consolation ; il deviendrait pour notre Évariste un gage d'immortalité, et je croirais que mon frère n'est pas entré tout entier dans la tombe. Etc., etc.

3. En posant
   $$[m, n] = \int_0^1 (1 - x)^{m-1} x^{m-1}\, \mathrm{d}x,$$
   Galois part de la relation $[m + 1, n] = \frac{m}{m + n}[m, n]$;
   il en déduit, en désignant par p un nombre entier positif quelconque,
   $$[m, n] = \frac{[p, m]}{[p, m + n]}[m + p, n],$$
   puis
   $$[m, n] = \lim_{p \to \infty} \frac{[p, m] \times [p, n]}{[p, m + n]};$$

remplaçant $[p,n]$ par $\dfrac{1}{p^n}\displaystyle\int_0^p (1-\int xp)^{\mu-1}x^{n-1}\,\mathrm{d}x$, et en passant à la limite, il obtient $[m,n]=\dfrac{\Gamma m\Gamma n}{\Gamma(m+n)}$.
Il établit ensuite la relation

$$\int_0^1 \frac{x^{n-1}-1}{x-1}\,\mathrm{d}x=\phi(n)-\phi(1),$$

où

$$\phi(n)=\frac{d\log\Gamma(n)}{dn},$$

en partant de ce que l'on a, pour $m=1$,

$$\frac{d\log[m,n]}{dm}=\frac{\int_0^1\log(1-x)x^{n-1}\,\mathrm{d}x}{\int_0^1 x^{n-1}\,\mathrm{d}x}=\int_0^1\log(1-x)nx^{n-1}\,\mathrm{d}x,$$

d'où, en intégrant le dernier membre par parties,

$$\phi(1)-\phi(n+1)=-\int_0^1\frac{x^n-1}{x-1}dx.$$

4. Œuvres d'Abel, édition Sylow, t. I, p. 515.
5. La feuille a été pliée ; sur la moitié de la quatrième page, on trouve quelques calculs relatifs à l'intégrale

$$\int\frac{dx}{\sqrt{x(x^2-2\alpha x+\gamma^2)(x^2-2\beta x+\gamma^2)}}$$

où Galois fait la substitution

$$x+\frac{\gamma^2}{x}=2z$$

6. Ce fragment occupe deux feuilles, écrites sur les deux faces, du format 23 x 18.
7. Cette phrase elliptique a été ajoutée dans une fin de ligne et dans l'interligne au-dessous.
8. La première page finit ici ; les six lignes qui suivent sont au verso.
9. Un peu plus bas, on lit : Discussion des groupes irréductibles ; le texte de la page est couvert de calculs, écrits en renversant la page de haut en bas.
10. Les mots mis ici entre crochets sont barrés ; au reste tout ce passage, à partir de "Du cas ou" jusqu'à "plusieurs fonctions connues" est couvert de ratures et de surcharges ; on lit, par exemple, sous une rature : "Si D est le commun diviseur à ce groupe et à celui de la fonction supposée" ; tout ce passage est un renvoi placé au bas de la page, de façon à être substitué à trois lignes qui sont barrées, et dont voici le texte :
Du cas où une fonction des racines est censée connue. Remarque. On peut réduire à ce cas celui où on supposerait plusieurs connues.
11. Au-dessous en interligne :
Jusqu'ici on avait cru
12. Les deux fragments qui suivent sont sur l'autre face de la feuille ; ils sont séparés par un blanc laissé au milieu de la page ; au-dessus de l'avant-dernière ligne du premier passage et dans le blanc, on trouve les mots suivants dont le premier est couvert d'une rature et dont les autres sont bâtonnés ; la lecture du mot Présenté est douteuse.

Mémoire
la théorie des fonctions et sur celle
des équations littérales.
Présenté à l'Institut par
E. Galois.
Octobre 1829.

13. Mots placés en interligne et presque illisibles ; on pourrait aussi bien lire *remarque* que *réciproque*.
14. Une feuille du format 23 x 17, écrite sur les deux faces.
15. En renversant la page, on trouve quelques lignes relatives à la décomposition d'un groupe, que l'absence de contexte rend inintelligibles, puis le commencement d'une question, qu'on retrouve en entier sur un petit fragment de papier, comme il suit :
Étant donnée une substitution S et deux permutations A et A' on demande une substitution S' telle que la lettre située au k$^{\text{ième}}$ rang dans A' prenne le $\phi k^{\text{ième}}$ rang dans AS, la lettre située au $k^{ième}$ rang dans A' prenne le $\phi k^{\text{ième}}$ dans $A'S'$.
Supposons le problème résolu. Soit $A'=AT$, on aura évidemment

$$A'S'=AST$$

16. Ce fragment comporte trois feuilles du format 20×15, du même papier que le fragment M ; la troisième feuille, dont il est question dans une note ultérieure, est intacte ; les deux autres sont déchirées, à droite, de haut en bas ; il manque quelques lettres et, parfois, des mots entiers ; d'où les crochets que l'on trouvera dans le texte imprimé. La déchirure a pu se faire en détachant les trois feuilles d'un cahier pareil à celui qui porte le titre "Notes de mathématiques" et dont j'ai parlé plus haut.
Cet essai est sans doute antérieur à la rédaction du Mémoire sur les conditions de résolubilité des équations par radicaux, et de la feuille relative à la proposition I de ce Mémoire, dont j'ai parlé précédemment (p. 11) ; les deux rédactions sont interrompues ; pour l'une et l'autre, la fin de la page reste blanche ; l'essai n'a pas été achevé.

17. Ces mots sont mis en marge.

18. La page se termine au mot “telles”, le reste se continue sur deux feuilles distinctes ; l’une de ces deux feuilles est écrite sur le recto et le verso, c’est celle dont le texte est imprimé ci-dessus ; l’autre feuille n’est écrite que sur le recto, jusqu’au milieu de la page : le verso contient quelques calculs relatifs à la résolution algébrique de l’équation du troisième degré. Les deux feuilles contiennent le même texte jusqu’à la fin de l’alinéa “sont seules connues”. A partir de ces mots, on lit dans la seconde feuille :
Mais, avant de développer la démonstration complète de cette proposition, nous ferons voir qu’il suffit de la donner dans le cas où l’équation proposée ne se décompose pas en facteurs dont les coefficients se déduisent rationnellement de ses coefficients et des quantités qui lui sont adjointes, plus brièvement, dans le cas où l’équation n’a pas de diviseurs rationnels. Admettons en effet que la chose ait été démontrée dans ce cas, et supposons qu’une équation se décompose en deux facteurs qui n’aient eux-mêmes aucun diviseur rationnel.

19. Un fragment qui semble un morceau déchiré (hauteur, 9") d’une feuille de papier du même format contient le texte suivant, d’un côté : Soit G un groupe correspondant à l’équation $\psi = 0$ et $A, B, C...$ les permutations du groupe G. Pour obtenir un pareil groupe, il faut opérer sur une permutation A toutes les substitutions de l’équation ψ. Nous supposons que la permutation A contienne toutes les racines de $F(x) = 0$. Prenons une fonction $\Phi(A\Sigma)$ invariable par les substitutions Σ relatives aux racines de ϕ,
et de l’autre côté :
qui correspondent aux substitutions indiquées quand aux racines de l’équation ϕ on substitue leurs expressions en fonction de celles de ψ. Je dis qu’il viendra un groupe de permutations qui relativement à la proposée $F(x) = 0$ satisfera à la condition exigée. En effet, toute fonction des racines invariable par les substitutions de ce groupe pourra d’abord s’exprimer en fonction des seules racines de l’équation ψ. De plus, comme cette fonction transformée sera encore invariable par les substitutions de l’équation ψ on voit que sa valeur numérique

20. Feuille déchirée (18 x 17), écrite sur les deux faces.

21. Cet énoncé est écrit sur un morceau de papier (10 x 18) ; l’écriture, parfois malaisée à déchiffrer en raison des ratures et des surcharges, trahit une certaine nervosité ; au-dessous, Galois a mis son nom, écrit à main posée, avec une certaine complaisance.

22. Il n’est guère utile de dire qu’il faut lire HS' ; ce passage est à demi effacé.

23. Une seule page de format 20 x 15. Ce fragment et le suivant doivent être rapprochés de l’*Analyse d’un Mémoire sur la résolution algébrique des équations*, qui a été publiée dans le *Bulletin de Férussac (Œuvres*, p. 11), et dont les premières lignes sont identiques à celles du fragment M.

24. Une feuille (18 x 15), écrite des deux côtés.

25. Relativement au premier membre de la congruence qui suit, je dois signaler l’énoncé que voici, écrit sur la première page d’une feuille double (22 x 18) : Le produit
$$(p^\nu - p)(p^\nu - p^2)(p^\nu - p^3)\dots(p^\nu - p^{\nu-1})$$
n’admet point de facteur premier $\dfrac{p^\nu - 1}{\partial(p-1)}$, ∂ étant le plus grand commun diviseur entre ν et $p-1$, à moins que $\nu = 2$.
Cet énoncé est placé au milieu de calculs dont quelques-uns concernent la transformation des fonctions elliptiques. Sur les autres pages, d’autres formules se rapportent à l’équation $\dfrac{du}{dx} = \dfrac{d'u}{dt'}$ aux fonctions trigonométriques, à la résolution des équations binômes, à la décomposition des fonctions trigonométriques en produits ou en fractions simples, etc.

26. Dans la ligne qui suit et, un peu plus loin, dans l’égalité $p = \nu$, la lettre ν a été mise en surcharge sur la lettre μ ; ensuite, la correction n’a pas été faite. Au reste, la lecture de ce fragment est, par endroits, assez difficile.

27. Trois feuilles (20 x 15) écrites sur les deux faces.

28. Il faut lire sans doute
$$(x_{k,l,ak+b,cl+d}).$$

29. Deux pages et demie d’une feuille double (23 x 18).

30. Malgré son caractère élémentaire, j’ai cru devoir publier cette note, qui n’est pas sans intérêt pour l’histoire de la Géométrie analytique et de la théorie des invariants. En raison de son contenu, on peut supposer qu’elle remonte au temps où Galois était élève de M. Richard, dans la classe de Mathématiques spéciales, ou au moment où il sortait de cette classe pour entrer à l’École Normale. Toutefois, la première supposition semble devoir être écartée : s’il en avait eu connaissance, M. Richard aurait sans doute fait pénétrer dans son enseignement les idées de son élève, qui se seraient diffusées immédiatement. Quoi qu’il en soit, cette note a, comme le morceau précédent, l’aspect d’une copie d’écolier, avec la signature en haut et à gauche ; elle ressemble tout à fait à quelques-unes des copies de Galois, que M. Richard avait conservées et données à Hermite. M. Émile Picard a retrouvé ces copies de Galois dans les papiers d’Hermite ; il a bien voulu me les remettre pour qu’elles soient jointes au précieux trésor que Mme de Blignières donne à l’Académie des Sciences. L’une de ces copies contient un petit travail, que Galois a sans doute fait librement et remis à son maître, et où son esprit philosophique se manifeste déjà ; j’en extrais cette curieuse réflexion :
Un auteur me dit : “l’arithmétique est la base de toutes les parties des Mathématiques, puisque c’est toujours aux nombres qu’il faut ramener les résultats des calculs.” D’après la dernière phrase de l’auteur, il serait plus naturel de croire que l’arithmétique est le terme et le complément de l’Analyse ; et c’est ce qui a lieu.
Toutes ces copies, comme la présente note, sont sur du papier de format 23 x 18.

31. Il y a une figure en marge, dans le texte de Galois.

Géométrie modulaire et quantique (Denise Vella-Chemla, 12.8.2017)

Du fait de recherches récentes, on cherche à distinguer d'un point de vue géométrique (sur le cercle unité) les résidus quadratiques des résidus de puissances plus grandes que les puissances 2^{des} (les carrés) des nombres.

On constate que *la somme des résidus quadratiques du double* $2p$ *d'un nombre premier* p *de la forme* $4k+1$ *vaut* p^2 *et donc que* p *la divise.* On constate également que p un nombre premier impair de la forme $4k+3$ divise la somme des résidus quadratiques de son double $2p$.

On a pris l'habitude de représenter les résidus quadratiques dans des petits tableaux, par exemple modulo 11 :

10	9	8	7	6
1	2	3	4	5
1	4	9	5	3

On constate que la somme des restes $1 + 4 + 9 + 5 + 3 = 22$ est divisible par 11. Ce fait semble vérifié pour tout nombre p premier supérieur ou égal à 5 :

$$p \text{ est un nombre premier } \implies \left(\sum_{x=1}^{\frac{p-1}{2}} x^2 \right) \equiv 0 \ (mod\ p)$$

Malheureusement, ce fait est aussi vérifié pour 14 et pour de nombreux autres nombres. Il ne permet donc pas de discriminer les nombres premiers des nombres composés.

On cherche un élément discriminant certaines classes de nombres, on observe le fait suivant, qu'il faudrait démontrer, et qui permet de distinguer parmi les nombres pairs les doubles des nombres premiers des autres :

$$2p \text{ est le double d'un nombre premier de la forme } 4k+3 \implies \left(\sum_{x=1}^{\frac{2p-1}{2}} x^2 \right) \equiv 0 \ (mod\ 2p)$$

et

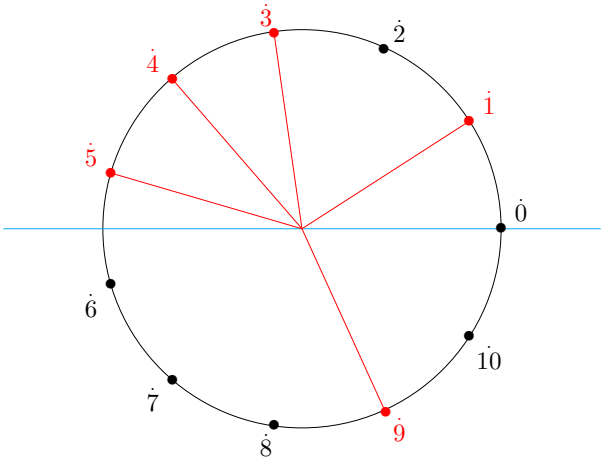
$$2p \text{ est le double d'un nombre premier de la forme } 4k+1 \iff \left(\sum_{x=1}^{\frac{2p-1}{2}} x^2 \right) \equiv p \ (mod\ 2p)$$

La première propriété ne permet pas de discriminer les nombres doubles de nombres premiers des nombres doubles de nombres composés (70 la vérifie par exemple).

Illustrons la propriété ci-dessus géométriquement : on positionne les classes modulaires selon le module $m = 11$ sur le cercle unité. On note en rouge les résidus quadratiques et on laisse les non-résidus en noir.

La somme des angles au centre entre l'axe des abscisses et les droites qui relient les points correspondant aux résidus à l'origine est un multiple entier du tour complet. Le même phénomène semble avoir lieu pour tout module pair $m = 2p$ double d'un nombre premier $p = 4k+3$ mais ne pas avoir lieu pour tout nombre pair autre que ceux-là.

Cette idée de *nombre entier de tours complets* justifie l'emploi du mot *quantique* dans le titre de cette note.



La propriété pour les doubles de premiers ($4k+1$ ou $4k+3$) est également vérifiée pour d'autres résidus que les résidus quadratiques (les résidus cubiques et quintiques par exemple) mais pour les résidus en question, elle est aussi vérifiée par d'autres nombres pairs et n'est donc pas discriminative de ces pairs particuliers (les doubles de nombres premiers). On fournit en annexe les calculs effectués pour de petites valeurs qui illustrent cela.

Annexe 1 : Résidus quadratiques pour les modules $m \leqslant 20$ des nombres $x \leqslant \frac{m-1}{2}$ et leur somme

Remarque : on ne note ni les restes nuls, ni le fait que certains restes sont images de plusieurs nombres (multiplicités), la somme n'est donc pas toujours celle des nombres apparaissant sur chaque ligne.

2 :	1	$\sum = 1$
3 :	1	$\sum = 1$
4 :	1	$\sum = 1$
5 :	1 4	$\sum = 5\ (\equiv 0)$
6 :	1 3 4	$\sum = 8\ (\equiv 2)$
7 :	1 2 4	$\sum = 7\ (\equiv 0)$
8 :	1 4	$\sum = 6$
9 :	1 4 7	$\sum = 12\ (\equiv 3)$
10 :	1 4 5 6 9	$\sum = 25\ (\equiv 5)$
11 :	1 3 4 5 9	$\sum = 22\ (\equiv 0)$
12 :	1 4 9	$\sum = 19\ (\equiv 7)$
13 :	1 3 4 9 10 12	$\sum = 39\ (\equiv 0)$
14 :	1 2 4 7 8 9 11	$\sum = 42\ (\equiv 0)$
15 :	1 4 6 9 10	$\sum = 35\ (\equiv 5)$
16 :	1 4 9	$\sum = 28\ (\equiv 12)$
17 :	1 2 4 8 9 13 15 16	$\sum = 68\ (\equiv 0)$
18 :	1 4 7 9 10 13 16	$\sum = 69\ (\equiv 15)$
19 :	1 4 5 6 7 9 11 16 17	$\sum = 76\ (\equiv 0)$
20 :	1 4 5 9 16	$\sum = 65\ (\equiv 5)$

Annexe 2 : Résidus cubiques pour les modules $m \leqslant 20$ des nombres $x \leqslant \frac{m-1}{2}$ et leur somme

2 :	1	$\sum = 1$
3 :	1	$\sum\sum = 1$
4 :	1	$\sum\sum\sum = 1$
5 :	1 3	$\sum\sum\sum = 4$
6 :	1 2 3	$\sum\sum\sum = 6\ (\equiv 0)$
7 :	1 6	$\sum\sum\sum = 8\ (\equiv 1)$
8 :	1 3	$\sum\sum\sum = 4$
9 :	1 8	$\sum\sum\sum = 10\ (\equiv 1)$
10 :	1 4 5 7 8	$\sum\sum\sum = 25\ (\equiv 5)$
11 :	1 4 5 8 9	$\sum\sum\sum = 27\ (\equiv 5)$
12 :	1 3 4 5 8	$\sum\sum\sum = 21\ (\equiv 9)$
13 :	1 8 12	$\sum\sum\sum = 38\ (\equiv 12)$
14 :	1 6 7 8 13	$\sum\sum\sum = 56\ (\equiv 0)$
15 :	1 4 5 6 8 12 13	$\sum\sum\sum = 49\ (\equiv 4)$
16 :	1 7 8 11 13	$\sum\sum\sum = 48\ (\equiv 0)$
17 :	1 2 3 6 8 10 12 13	$\sum\sum\sum = 55\ (\equiv 4)$
18 :	1 8 9 10 17	$\sum\sum\sum = 63\ (\equiv 9)$
19 :	1 7 8 11 18	$\sum\sum\sum = 68\ (\equiv 11)$
20 :	1 3 4 5 7 8 9 12 16	$\sum = 65\ (\equiv 5)$

Annexe 3 : résultats d'exécution (résidus quadratiques, cubiques, quintiques) jusqu'à 100 ; pour les nombres jusqu'à 20, détails des puissances ; en résultat global, la somme des résidus, puis son reste modulo le nombre considéré, après les ":"

quadratiques

$1^2 = 1\ (mod\ 3)$.
$3 -> 1 : 1$

$1^2 = 1\ (mod\ 4)$.
$2^2 = 0\ (mod\ 4)$.
$4 -> 1 : 1$

$1^2 = 1\ (mod\ 5)$.
$2^2 = 4\ (mod\ 5)$.
$5 -> 5 : 0$

$1^2 = 1\ (mod\ 6)$.
$2^2 = 4\ (mod\ 6)$.
$3^2 = 3\ (mod\ 6)$.
$6 -> 8 : 2$

$1^2 = 1\ (mod\ 7)$.
$2^2 = 4\ (mod\ 7)$.
$3^2 = 2\ (mod\ 7)$.
$7 -> 7 : 0$

$1^2 = 1\ (mod\ 8)$.
$2^2 = 4\ (mod\ 8)$.
$3^2 = 1\ (mod\ 8)$.
$4^2 = 0\ (mod\ 8)$.
$8 -> 6 : 6$

$1^2 = 1\ (mod\ 9)$.
$2^2 = 4\ (mod\ 9)$.
$3^2 = 0\ (mod\ 9)$.
$4^2 = 7\ (mod\ 9)$.
$9 -> 12 : 3$

$1^2 = 1\ (mod\ 10)$.
$2^2 = 4\ (mod\ 10)$.
$3^2 = 9\ (mod\ 10)$.
$4^2 = 6\ (mod\ 10)$.

$5^2 = 5\ (mod\ 10)$.
$10 -> 25 : 5$

$1^2 = 1\ (mod\ 11)$.
$2^2 = 4\ (mod\ 11)$.
$3^2 = 9\ (mod\ 11)$.
$4^2 = 5\ (mod\ 11)$.
$5^2 = 3\ (mod\ 11)$.
$11 -> 22 : 0$

$1^2 = 1\ (mod\ 12)$.
$2^2 = 4\ (mod\ 12)$.
$3^2 = 9\ (mod\ 12)$.
$4^2 = 4\ (mod\ 12)$.
$5^2 = 1\ (mod\ 12)$.
$6^2 = 0\ (mod\ 12)$.
$12 -> 19 : 7$

$1^2 = 1\ (mod\ 13)$.
$2^2 = 4\ (mod\ 13)$.
$3^2 = 9\ (mod\ 13)$.
$4^2 = 3\ (mod\ 13)$.
$5^2 = 12\ (mod\ 13)$.
$6^2 = 10\ (mod\ 13)$.
$13 -> 39 : 0$

$1^2 = 1\ (mod\ 14)$.
$2^2 = 4\ (mod\ 14)$.
$3^2 = 9\ (mod\ 14)$.
$4^2 = 2\ (mod\ 14)$.
$5^2 = 11\ (mod\ 14)$.
$6^2 = 8\ (mod\ 14)$.
$7^2 = 7\ (mod\ 14)$.
$14 -> 42 : 0$

$1^2 = 1\ (mod\ 15)$.
$2^2 = 4\ (mod\ 15)$.
$3^2 = 9\ (mod\ 15)$.
$4^2 = 1\ (mod\ 15)$.
$5^2 = 10\ (mod\ 15)$.
$6^2 = 6\ (mod\ 15)$.
$7^2 = 4\ (mod\ 15)$.
$15 -> 35 : 5$

$1^2 = 1\ (mod\ 16)$.
$2^2 = 4\ (mod\ 16)$.
$3^2 = 9\ (mod\ 16)$.
$4^2 = 0\ (mod\ 16)$.
$5^2 = 9\ (mod\ 16)$.
$6^2 = 4\ (mod\ 16)$.
$7^2 = 1\ (mod\ 16)$.
$8^2 = 0\ (mod\ 16)$.
$16 -> 28 : 12$

$1^2 = 1\ (mod\ 17)$.
$2^2 = 4\ (mod\ 17)$.
$3^2 = 9\ (mod\ 17)$.
$4^2 = 16\ (mod\ 17)$.
$5^2 = 8\ (mod\ 17)$.
$6^2 = 2\ (mod\ 17)$.
$7^2 = 15\ (mod\ 17)$.
$8^2 = 13\ (mod\ 17)$.
$17 -> 68 : 0$

$1^2 = 1\ (mod\ 18)$.
$2^2 = 4\ (mod\ 18)$.
$3^2 = 9\ (mod\ 18)$.
$4^2 = 16\ (mod\ 18)$.
$5^2 = 7\ (mod\ 18)$.
$6^2 = 0\ (mod\ 18)$.
$7^2 = 13\ (mod\ 18)$.
$8^2 = 10\ (mod\ 18)$.
$9^2 = 9\ (mod\ 18)$.
$18 -> 69 : 15$

$1^2 = 1\ (mod\ 19)$.
$2^2 = 4\ (mod\ 19)$.
$3^2 = 9\ (mod\ 19)$.
$4^2 = 16\ (mod\ 19)$.
$5^2 = 6\ (mod\ 19)$.
$6^2 = 17\ (mod\ 19)$.
$7^2 = 11\ (mod\ 19)$.
$8^2 = 7\ (mod\ 19)$.
$9^2 = 5\ (mod\ 19)$.
$19 -> 76 : 0$

$1^2 = 1\ (mod\ 20)$.
$2^2 = 4\ (mod\ 20)$.
$3^2 = 9\ (mod\ 20)$.
$4^2 = 16\ (mod\ 20)$.
$5^2 = 5\ (mod\ 20)$.
$6^2 = 16\ (mod\ 20)$.
$7^2 = 9\ (mod\ 20)$.
$8^2 = 4\ (mod\ 20)$.
$9^2 = 1\ (mod\ 20)$.
$10^2 = 0\ (mod\ 20)$.
$20 -> 65 : 5$

21 -> 91 : 7
22 -> 110 : 0
23 -> 92 : 0
24 -> 74 : 2
25 -> 125 : 0
26 -> 169 : 13
27 -> 144 : 9
28 -> 147 : 7
29 -> 203 : 0
30 -> 190 : 10
31 -> 186 : 0
32 -> 152 : 24
33 -> 242 : 11
34 -> 289 : 17
35 -> 245 : 0
36 -> 201 : 21
37 -> 333 : 0
38 -> 342 : 0
39 -> 286 : 13
40 -> 270 : 30
41 -> 410 : 0
42 -> 413 : 35
43 -> 430 : 0
44 -> 363 : 11
45 -> 420 : 15
46 -> 460 : 0
47 -> 423 : 0

48 -> 340 : 4
49 -> 490 : 0
50 -> 575 : 25
51 -> 578 : 17
52 -> 585 : 13
53 -> 689 : 0
54 -> 666 : 18
55 -> 605 : 0
56 -> 546 : 42
57 -> 760 : 19
58 -> 841 : 29
59 -> 767 : 0
60 -> 635 : 35
61 -> 915 : 0
62 -> 868 : 0
63 -> 777 : 21
64 -> 688 : 48
65 -> 1040 : 0
66 -> 1045 : 55
67 -> 1072 : 0
68 -> 969 : 17
69 -> 1058 : 23
70 -> 1120 : 0
71 -> 994 : 0
72 -> 870 : 6
73 -> 1314 : 0
74 -> 1369 : 37
75 -> 1150 : 25
76 -> 1235 : 19
77 -> 1386 : 0
78 -> 1352 : 26
79 -> 1343 : 0
80 -> 1100 : 60
81 -> 1404 : 27
82 -> 1681 : 41
83 -> 1577 : 0
84 -> 1393 : 49
85 -> 1785 : 0
86 -> 1806 : 0
87 -> 1595 : 29
88 -> 1562 : 66
89 -> 1958 : 0
90 -> 1875 : 75
91 -> 1911 : 0
92 -> 1771 : 23
93 -> 1984 : 31
94 -> 1974 : 0
95 -> 1805 : 0
96 -> 1544 : 8
97 -> 2328 : 0
98 -> 2205 : 49
99 -> 2211 : 33
100 -> 2025 : 25

cubiques

$1^3 = 1\ (mod\ 3)$.
$3 -> 1 : 1$

$1^3 = 1\ (mod\ 4)$.
$2^3 = 0\ (mod\ 4)$.
$4 -> 1 : 1$

$1^3 = 1\ (mod\ 5)$.
$2^3 = 3\ (mod\ 5)$.
$5 -> 4 : 4$

$1^3 = 1\ (mod\ 6)$.
$2^3 = 2\ (mod\ 6)$.
$3^3 = 3\ (mod\ 6)$.
$6 -> 6 : 0$

$1^3 = 1\ (mod\ 7)$.
$2^3 = 1\ (mod\ 7)$.
$3^3 = 6\ (mod\ 7)$.
$7 -> 8 : 1$

$1^3 = 1\ (mod\ 8)$.
$2^3 = 0\ (mod\ 8)$.
$3^3 = 3\ (mod\ 8)$.
$4^3 = 0\ (mod\ 8)$.
$8 -> 4 : 4$

$1^3 = 1\ (mod\ 9)$.
$2^3 = 8\ (mod\ 9)$.
$3^3 = 0\ (mod\ 9)$.
$4^3 = 1\ (mod\ 9)$.
$9 -> 10 : 1$

$1^3 = 1\ (mod\ 10)$.
$2^3 = 8\ (mod\ 10)$.
$3^3 = 7\ (mod\ 10)$.
$4^3 = 4\ (mod\ 10)$.
$5^3 = 5\ (mod\ 10)$.
$10 -> 25 : 5$

$1^3 = 1\ (mod\ 11)$.
$2^3 = 8\ (mod\ 11)$.
$3^3 = 5\ (mod\ 11)$.
$4^3 = 9\ (mod\ 11)$.
$5^3 = 4\ (mod\ 11)$.
$11 -> 27 : 5$

$1^3 = 1\ (mod\ 12)$.
$2^3 = 8\ (mod\ 12)$.
$3^3 = 3\ (mod\ 12)$.
$4^3 = 4\ (mod\ 12)$.
$5^3 = 5\ (mod\ 12)$.
$6^3 = 0\ (mod\ 12)$.
$12 -> 21 : 9$

$1^3 = 1\ (mod\ 13)$.
$2^3 = 8\ (mod\ 13)$.
$3^3 = 1\ (mod\ 13)$.
$4^3 = 12\ (mod\ 13)$.
$5^3 = 8\ (mod\ 13)$.
$6^3 = 8\ (mod\ 13)$.
$13 -> 38 : 12$

$1^3 = 1\ (mod\ 14)$.
$2^3 = 8\ (mod\ 14)$.
$3^3 = 13\ (mod\ 14)$.
$4^3 = 8\ (mod\ 14)$.
$5^3 = 13\ (mod\ 14)$.
$6^3 = 6\ (mod\ 14)$.
$7^3 = 7\ (mod\ 14)$.
$14- > 56 : 0$

$1^3 = 1\ (mod\ 15)$.
$2^3 = 8\ (mod\ 15)$.
$3^3 = 12\ (mod\ 15)$.
$4^3 = 4\ (mod\ 15)$.
$5^3 = 5\ (mod\ 15)$.
$6^3 = 6\ (mod\ 15)$.
$7^3 = 13\ (mod\ 15)$.
$15- > 49 : 4$

$1^3 = 1\ (mod\ 16)$.
$2^3 = 8\ (mod\ 16)$.
$3^3 = 11\ (mod\ 16)$.
$4^3 = 0\ (mod\ 16)$.
$5^3 = 13\ (mod\ 16)$.
$6^3 = 8\ (mod\ 16)$.
$7^3 = 7\ (mod\ 16)$.
$8^3 = 0\ (mod\ 16)$.
$16- > 48 : 0$

$1^3 = 1\ (mod\ 17)$.
$2^3 = 8\ (mod\ 17)$.
$3^3 = 10\ (mod\ 17)$.
$4^3 = 13\ (mod\ 17)$.
$5^3 = 6\ (mod\ 17)$.
$6^3 = 12\ (mod\ 17)$.
$7^3 = 3\ (mod\ 17)$.
$8^3 = 2\ (mod\ 17)$.
$17- > 55 : 4$

$1^3 = 1\ (mod\ 18)$.
$2^3 = 8\ (mod\ 18)$.
$3^3 = 9\ (mod\ 18)$.
$4^3 = 10\ (mod\ 18)$.
$5^3 = 17\ (mod\ 18)$.
$6^3 = 0\ (mod\ 18)$.
$7^3 = 1\ (mod\ 18)$.
$8^3 = 8\ (mod\ 18)$.
$9^3 = 9\ (mod\ 18)$.
$18- > 63 : 9$

$1^3 = 1\ (mod\ 19)$.
$2^3 = 8\ (mod\ 19)$.
$3^3 = 8\ (mod\ 19)$.
$4^3 = 7\ (mod\ 19)$.
$5^3 = 11\ (mod\ 19)$.
$6^3 = 7\ (mod\ 19)$.
$7^3 = 1\ (mod\ 19)$.
$8^3 = 18\ (mod\ 19)$.
$9^3 = 7\ (mod\ 19)$.
$19- > 68 : 11$

$1^3 = 1\ (mod\ 20)$.
$2^3 = 8\ (mod\ 20)$.

$3^3 = 7\ (mod\ 20)$.
$4^3 = 4\ (mod\ 20)$.
$5^3 = 5\ (mod\ 20)$.
$6^3 = 16\ (mod\ 20)$.
$7^3 = 3\ (mod\ 20)$.
$8^3 = 12\ (mod\ 20)$.
$9^3 = 9\ (mod\ 20)$.
$10^3 = 0\ (mod\ 20)$.
$20- > 65 : 5$

21 -> 85 : 1
22 -> 110 : 0
23 -> 124 : 9
24 -> 84 : 12
25 -> 84 : 9
26 -> 117 : 13
27 -> 100 : 19
28 -> 161 : 21
29 -> 208 : 5
30 -> 150 : 0
31 -> 233 : 16
32 -> 224 : 0
33 -> 214 : 16
34 -> 255 : 17
35 -> 274 : 29
36 -> 261 : 9
37 -> 344 : 11
38 -> 304 : 0
39 -> 337 : 25
40 -> 340 : 20
41 -> 353 : 25
42 -> 399 : 21
43 -> 428 : 41
44 -> 517 : 33
45 -> 469 : 19
46 -> 552 : 0
47 -> 506 : 36
48 -> 528 : 0
49 -> 428 : 36
50 -> 575 : 25
51 -> 514 : 4
52 -> 637 : 13
53 -> 718 : 29
54 -> 540 : 0
55 -> 599 : 49
56 -> 588 : 28
57 -> 619 : 49
58 -> 841 : 29
59 -> 779 : 12
60 -> 765 : 45
61 -> 834 : 41
62 -> 682 : 0
63 -> 883 : 1
64 -> 704 : 0
65 -> 974 : 64
66 -> 825 : 33
67 -> 1094 : 22
68 -> 1105 : 17
69 -> 1159 : 55
70 -> 980 : 0

71 -> 1146 : 10
72 -> 1044 : 36
73 -> 1322 : 8
74 -> 1517 : 37
75 -> 1234 : 34
76 -> 1501 : 57
77 -> 1611 : 71
78 -> 1482 : 0
79 -> 1759 : 21
80 -> 1360 : 0
81 -> 1315 : 19
82 -> 1599 : 41
83 -> 1459 : 48
84 -> 1533 : 21
85 -> 1959 : 4
86 -> 1892 : 0
87 -> 1861 : 34
88 -> 1716 : 44
89 -> 1723 : 32
90 -> 1845 : 45
91 -> 1884 : 64
92 -> 2093 : 69
93 -> 2062 : 16
94 -> 1880 : 0
95 -> 1854 : 49
96 -> 2016 : 0
97 -> 2084 : 47
98 -> 2009 : 49
99 -> 2062 : 82
100 -> 2125 : 25

quintiques

$1^5 = 1\ (mod\ 3)$.
$3 -> 1 : 1$

$1^5 = 1\ (mod\ 4)$.
$2^5 = 0\ (mod\ 4)$.
$4 -> 1 : 1$

$1^5 = 1\ (mod\ 5)$.
$2^5 = 2\ (mod\ 5)$.
$5 -> 3 : 3$

$1^5 = 1\ (mod\ 6)$.
$2^5 = 2\ (mod\ 6)$.
$3^5 = 3\ (mod\ 6)$.
$6 -> 6 : 0$

$1^5 = 1\ (mod\ 7)$.
$2^5 = 4\ (mod\ 7)$.
$3^5 = 5\ (mod\ 7)$.
$7 -> 10 : 3$

$1^5 = 1\ (mod\ 8)$.
$2^5 = 0\ (mod\ 8)$.
$3^5 = 3\ (mod\ 8)$.
$4^5 = 0\ (mod\ 8)$.
$8 -> 4 : 4$

$1^5 = 1\ (mod\ 9)$.
$2^5 = 5\ (mod\ 9)$.
$3^5 = 0\ (mod\ 9)$.

$4^5 = 7\ (mod\ 9)$.
$9- > 13 : 4$

$1^5 = 1\ (mod\ 10)$.
$2^5 = 2\ (mod\ 10)$.
$3^5 = 3\ (mod\ 10)$.
$4^5 = 4\ (mod\ 10)$.
$5^5 = 5\ (mod\ 10)$.
$10- > 15 : 5$

$1^5 = 1\ (mod\ 11)$.
$2^5 = 10\ (mod\ 11)$.
$3^5 = 1\ (mod\ 11)$.
$4^5 = 1\ (mod\ 11)$.
$5^5 = 1\ (mod\ 11)$.
$11- > 14 : 3$

$1^5 = 1\ (mod\ 12)$.
$2^5 = 8\ (mod\ 12)$.
$3^5 = 3\ (mod\ 12)$.
$4^5 = 4\ (mod\ 12)$.
$5^5 = 5\ (mod\ 12)$.
$6^5 = 0\ (mod\ 12)$.
$12- > 21 : 9$

$1^5 = 1\ (mod\ 13)$.
$2^5 = 6\ (mod\ 13)$.
$3^5 = 9\ (mod\ 13)$.
$4^5 = 10\ (mod\ 13)$.
$5^5 = 5\ (mod\ 13)$.
$6^5 = 2\ (mod\ 13)$.
$13- > 33 : 7$

$1^5 = 1\ (mod\ 14)$.
$2^5 = 4\ (mod\ 14)$.
$3^5 = 5\ (mod\ 14)$.
$4^5 = 2\ (mod\ 14)$.
$5^5 = 3\ (mod\ 14)$.
$6^5 = 6\ (mod\ 14)$.
$7^5 = 7\ (mod\ 14)$.
$14- > 28 : 0$

$1^5 = 1\ (mod\ 15)$.
$2^5 = 2\ (mod\ 15)$.
$3^5 = 3\ (mod\ 15)$.
$4^5 = 4\ (mod\ 15)$.
$5^5 = 5\ (mod\ 15)$.
$6^5 = 6\ (mod\ 15)$.
$7^5 = 7\ (mod\ 15)$.
$15- > 28 : 13$

$1^5 = 1\ (mod\ 16)$.
$2^5 = 0\ (mod\ 16)$.
$3^5 = 3\ (mod\ 16)$.
$4^5 = 0\ (mod\ 16)$.
$5^5 = 5\ (mod\ 16)$.
$6^5 = 0\ (mod\ 16)$.
$7^5 = 7\ (mod\ 16)$.
$8^5 = 0\ (mod\ 16)$.
$16- > 16 : 0$

$1^5 = 1\ (mod\ 17)$.
$2^5 = 15\ (mod\ 17)$.

$3^5 = 5\ (mod\ 17)$.
$4^5 = 4\ (mod\ 17)$.
$5^5 = 14\ (mod\ 17)$.
$6^5 = 7\ (mod\ 17)$.
$7^5 = 11\ (mod\ 17)$.
$8^5 = 9\ (mod\ 17)$.
$17 -> 66 : 15$

$1^5 = 1\ (mod\ 18)$.
$2^5 = 14\ (mod\ 18)$.
$3^5 = 9\ (mod\ 18)$.
$4^5 = 16\ (mod\ 18)$.
$5^5 = 11\ (mod\ 18)$.
$6^5 = 0\ (mod\ 18)$.
$7^5 = 13\ (mod\ 18)$.
$8^5 = 8\ (mod\ 18)$.
$9^5 = 9\ (mod\ 18)$.
$18 -> 81 : 9$

$1^5 = 1\ (mod\ 19)$.
$2^5 = 13\ (mod\ 19)$.
$3^5 = 15\ (mod\ 19)$.
$4^5 = 17\ (mod\ 19)$.
$5^5 = 9\ (mod\ 19)$.
$6^5 = 5\ (mod\ 19)$.
$7^5 = 11\ (mod\ 19)$.
$8^5 = 12\ (mod\ 19)$.
$9^5 = 16\ (mod\ 19)$.
$19 -> 99 : 4$

$1^5 = 1\ (mod\ 20)$.
$2^5 = 12\ (mod\ 20)$.
$3^5 = 3\ (mod\ 20)$.
$4^5 = 4\ (mod\ 20)$.
$5^5 = 5\ (mod\ 20)$.
$6^5 = 16\ (mod\ 20)$.
$7^5 = 7\ (mod\ 20)$.
$8^5 = 8\ (mod\ 20)$.
$9^5 = 9\ (mod\ 20)$.
$10^5 = 0\ (mod\ 20)$.
$20 -> 65 : 5$

21 -> 115 : 10
22 -> 88 : 0
23 -> 122 : 7
24 -> 84 : 12
25 -> 108 : 8
26 -> 91 : 13
27 -> 139 : 4
28 -> 189 : 21
29 -> 157 : 12
30 -> 120 : 0
31 -> 209 : 23
32 -> 128 : 0
33 -> 223 : 25
34 -> 289 : 17
35 -> 213 : 3
36 -> 297 : 9
37 -> 383 : 13
38 -> 342 : 0
39 -> 280 : 7

40 -> 260 : 20
41 -> 377 : 8
42 -> 399 : 21
43 -> 517 : 1
44 -> 429 : 33
45 -> 463 : 13
46 -> 460 : 0
47 -> 546 : 29
48 -> 336 : 0
49 -> 570 : 31
50 -> 575 : 25
51 -> 661 : 49
52 -> 585 : 13
53 -> 701 : 12
54 -> 702 : 0
55 -> 773 : 3
56 -> 644 : 28
57 -> 802 : 4
58 -> 899 : 29
59 -> 879 : 53
60 -> 645 : 45
61 -> 925 : 10
62 -> 1054 : 0
63 -> 913 : 31
64 -> 768 : 0
65 -> 1008 : 33
66 -> 1155 : 33
67 -> 1195 : 56
68 -> 969 : 17
69 -> 1111 : 7
70 -> 1190 : 0
71 -> 1273 : 66
72 -> 972 : 36
73 -> 1164 : 69
74 -> 1295 : 37
75 -> 1258 : 58
76 -> 1197 : 57
77 -> 1466 : 3
78 -> 1092 : 0
79 -> 1846 : 29
80 -> 1040 : 0
81 -> 841 : 31
82 -> 1763 : 41
83 -> 1719 : 59
84 -> 1449 : 21
85 -> 1783 : 83
86 -> 1978 : 0
87 -> 1810 : 70
88 -> 1716 : 44
89 -> 1942 : 73
90 -> 1845 : 45
91 -> 1879 : 59
92 -> 2093 : 69
93 -> 2224 : 85
94 -> 2444 : 0
95 -> 2208 : 23
96 -> 1920 : 0
97 -> 2256 : 25
98 -> 1813 : 49

99 -> 2335 : 58
100 -> 2125 : 25

Valuations p-adiques des nombres dans les factorielles (Denise Vella-Chemla, 12.8.2017)

Dans la table suivante, on fournit dans la case (i, j) la valuation i-adique de i dans la factorielle de j (ou $val_i(j!)$, pour $i \geqslant 2$). On la note $<$ si elle est inférieure à 1, 1 si elle vaut 1 et $>$ si elle est supérieure à 1.

$val_3(4!) = val_3(4.3.2.1) = val_3(2.2.3.2.1) = 1$.

$val_9(6!) = val_9(6.5.4.3.2.1) = val_9(3.2.5.2.2.3.2.1) = 1$.

$val_i(j!)$	1	2	3	4	5	6	7	8	9	10
2	$<$	1	1	$>$	$>$	$>$	$>$	$>$	$>$	$>$
3	$<$	$<$	1	1	1	$>$	$>$	$>$	$>$	$>$
4	$<$	$<$	$<$	1	1	1	1	$>$	$>$	$>$
5	$<$	$<$	$<$	$<$	1	1	1	1	1	$>$
6	$<$	$<$	1	1	1	1	1	1	$>$	$>$
7	$<$	$<$	$<$	$<$	$<$	$<$	1	1	1	1
8	$<$	$<$	$<$	1	1	1	1	1	1	1
9	$<$	$<$	$<$	$<$	$<$	1	1	1	$>$	$>$
10	$<$	$<$	$<$	$<$	1	1	1	1	1	$>$

On note que $val_{p^2}((2p)!) = 1$.

On simplifie à l'extrême en n'utilisant que 3 images. On aurait pu utiliser une fonction val' qui aurait associé aux nombres des images rationnelles ; par exemple,

$$val'_9(12!) = val_9(12.11.10.9.8.7.6.5.4.3.2) = val'_9(2.2.3.11.2.5.3.3.2.2.2.7.2.3.5.2.2.3.2) = \frac{5}{2}.$$

Les seuls nombres tels que $val_x(x!) = 1$ sont les nombres premiers.

Sommes de résidus modulaires (Denise Vella-Chemla, 14.8.2017)

Il s'agit ici de présenter des constats[1] induits de suites de résultats calculés par programme pour les entiers inférieurs à 100 concernant les sommes de résidus quadratiques, cubiques et quintiques des entiers.

Les résidus (quadratiques, cubiques, etc) sont les solutions d'équations et on effectue donc des sommes de solutions modulaires.

Résidus quadratiques

La somme des résidus quadratiques calculée ici est $q(n) = \sum_{k=1}^{milieu} k^2 \ (mod\ n)$ avec $milieu$ qui vaut $\frac{n}{2}$ si n est pair et $\frac{n-1}{2}$ sinon.

1) $n = 8k$

Dans la suite $\{8 \rightarrow 6,\ 16 \rightarrow 12,\ 24 \rightarrow 2,\ 32 \rightarrow 24,\ 40 \rightarrow 30,\ 48 \rightarrow 4,\ 56 \rightarrow 42,\ 64 \rightarrow 48,\ 72 \rightarrow 6,\ 80 \rightarrow 60,\ 88 \rightarrow 66,\ 96 \rightarrow 8\}$, on repère les nombres 6, 12,..., 24, 30,..., 42, 48,... 60, 66, on infère : parmi les $8k$, les $n = 24k'$ ont leur somme qui vaut $\frac{n}{12}$ tandis que les $24k' + 8$ et les $24k' + 16$ ont pour somme des résidus quadratiques $\frac{3n}{4}$;

2) $n = 8k + 1$

De la suite $\{17 \rightarrow 0,\ 25 \rightarrow 0,\ 33 \rightarrow 11,\ 41 \rightarrow 0,\ 49 \rightarrow 0,\ 57 \rightarrow 19\}$, on infère que les $n = 8k + 1$ divisibles par 3 (les $24k' + 9$) ont pour somme des résidus quadratiques $\frac{n}{3}$ tandis que ceux qui ne sont pas divisibles par 3 (les $24k' + 1$ et les $24k' + 17$) ont une somme des résidus quadratiques qui est nulle ;

3) $n = 8k + 2$

Dans la suite $\{10 \rightarrow 5,\ 18 \rightarrow 15,\ 26 \rightarrow 13,\ 34 \rightarrow 17,\ 42 \rightarrow 35,\ 50 \rightarrow 25,\ 58 \rightarrow 29,\ 66 \rightarrow 55,\ 74 \rightarrow 37,\ 82 \rightarrow 41,\ 90 \rightarrow 75,\ 98 \rightarrow 49\}$, on repère les nombres 13,17,...,25,29,...,37,41, on infère que les $24k' + 18$ ont pour somme des résidus quadratiques $\frac{5n}{6}$ tandis que les $n = 24k' + 2$ et les $n = 24k' + 10$ ont pour somme des résidus quadratique $\frac{n}{2}$;

4) $n = 8k + 3$

De la suite $\{11 \rightarrow 0,\ 19 \rightarrow 0,\ 27 \rightarrow 9,\ 35 \rightarrow 0,\ 43 \rightarrow 0,\ 51 \rightarrow 17,\ 59 \rightarrow 0,\ 67 \rightarrow 0,\ 75 \rightarrow 25,\ 83 \rightarrow 0,\ 91 \rightarrow 0\}$, on infère que les $24k' + 3$ ont pour somme des résidus quadratiques $\frac{n}{3}$ tandis que les $n = 24k' + 11$ et les $n = 24k' + 19$ ont leur somme des résidus quadratiques qui est nulle ;

5) $n = 8k + 4$

Dans la suite $\{4 \rightarrow 1,\ 12 \rightarrow 7,\ 20 \rightarrow 5,\ 28 \rightarrow 7,\ 36 \rightarrow 21,\ 44 \rightarrow 11,\ 52 \rightarrow 13,\ 60 \rightarrow 35,\ 68 \rightarrow 17,\ 76 \rightarrow 19,\ 84 \rightarrow 49,\ 92 \rightarrow 23,\ 100 \rightarrow 25\}$, on repère les nombres 5, 7,..., 11, 13, ..., 17, 19, ..., 23, 25, on infère que les $24k' + 12 = 12(2k' + 1)$ ont pour somme des résidus quadratiques $\frac{7n}{12}$ tandis que les $n = 24k + 4$ et les $n = 24k + 20$ ont leur somme des résidus quadratiques qui vaut $\frac{n}{4}$;

6) $n = 8k + 5$

De la suite $\{5 \rightarrow 0,\ 13 \rightarrow 0,\ 21 \rightarrow 7,\ 29 \rightarrow 0,\ 37 \rightarrow 0,\ 45 \rightarrow 15,\ 53 \rightarrow 0,\ 61 \rightarrow 0\}$, on infère que les $24k' + 21$ ont pour somme des résidus quadratiques $\frac{n}{3}$ tandis que les $n = 24k' + 5$ et les $n = 24k' + 13$ ont leur somme des résidus quadratique qui est nulle ;

7) $n = 8k + 6$

De la suite $\{22 \rightarrow 0,\ 30 \rightarrow 10,\ 38 \rightarrow 0,\ 46 \rightarrow 0,\ 54 \rightarrow 18,\ 62 \rightarrow 0,\ 70 \rightarrow 0,\ 78 \rightarrow 26,\ 86 \rightarrow 0,\ 94 \rightarrow 0\}$, on infère que les $24k' + 6$ ont pour somme des résidus quadratiques $\frac{n}{3}$ tandis que les $n = 24k' + 14$ et les $n = 24k' + 22$ ont leur somme des résidus quadratiques qui est nulle ;

8) $n = 8k + 7$

[1] à démontrer si c'est possible.

De la suite $\{7 \to 0,\ 15 \to 5,\ 23 \to 0,\ 31 \to 0,\ 39 \to 13,\ 47 \to 0,\ 55 \to 0,\ 63 \to 21\}$, on infère que les $24k'+15$ ont pour somme des résidus quadratiques $\frac{n}{3}$ tandis que les $n = 24k'+7$ et les $n = 24k'+23$ ont leur somme des résidus quadratiques qui est nulle.

Résidus cubiques

Pour les résidus cubiques, on infère :

1) parmi les $8k$, les $16k'$ ont pour somme des résidus cubiques 0 tandis que les $n = 16k'+8$ ont leur somme qui vaut $\frac{n}{2}$;

2) les $8k+1$ ont leur somme de résidus cubiques qui vaut k^2 ;

3) les $n = 8k+2$ ont leur somme de résidus cubiques qui vaut $\frac{n}{2}$;

4) pour les $8k+3$ ont leur somme de résidus cubiques qui vaut k^2+3k+1 ;

5) parmi les $8k+4$, les $n = 16k'+4$ ont pour somme des résidus cubiques $\frac{n}{4}$ tandis que les $n = 16k'+12$ ont leur somme de résidus cubiques qui vaut $\frac{3n}{4}$;

6) les $8k+5$ ont leur somme de résidus cubiques qui vaut k^2-k-1 ;

7) les $8k+6$ ont leur somme de résidus cubiques qui est nulle ;

8) les $8k+7$ (ou $8k-1$) ont (comme les $8k+1$) leur somme de résidus cubiques qui vaut k^2.

Résidus quintiques

Pour les résidus quintiques, on infère :

1) parmi les $8k$, les $16k'$ ont pour somme des résidus quintiques 0 tandis que les $n = 16k'+8$ ont leur somme qui vaut $\frac{n}{2}$ (même chose que pour les résidus cubiques) ;

2) pour les $8k+1$, voir ci-après ;

3) les $8k+2$ ont leur somme de résidus quintiques qui vaut $\frac{n}{2}$ (même chose que pour les résidus cubiques) ;

4) pour les $8k+3$, dans la suite $\{19 \to 23,\ 27 \to 31,\ 35 \to 38,\ 43 \to 44,\ 51 \to 49,\ 59 \to 53,\ 67 \to 56\}$ (remarque : les premières sommes de restes sont avant équivalence modulaire), on remarque qu'on passe d'une somme de restes à la suivante en faisant +8, +7, +6, +5, +4, +3 ; voir ci-après ;

5) parmi les $8k+4$, les $n = 16k'+4$ ont pour somme des résidus quintiques $\frac{n}{4}$ tandis que les $n = 16k'+12$ ont leur somme de résidus quintiques qui vaut $\frac{3n}{4}$ (même chose que pour les résidus cubiques) ;

6) pour les $8k+5$, voir ci-après ;

7) les $8k+6$ ont leur somme de résidus quintiques qui est nulle ;

8) les $8k+7$ ont leur somme de résidus quintiques qui est nulle.

Pour les $8k+3$ et les $8k+5$, on comprend que les formules doivent être quadratiques en k.

En effet, en prenant la suite des sommes de restes quintiques suivante

$$\{14, 23, 31, 38, 44, 53, 56\}$$

(des entiers $11, 19, 27, \ldots$ de la forme $8k+3$), on voit qu'on passe d'une somme de restes à la suivante en faisant $+9, +8, +7, +6, +5, etc.$. La somme des restes quintiques d'un nombre est donc une somme $\sum(10-k)$ et est de second degré en k.

De la même manière, en prenant la suite des sommes de restes quintiques suivante

$$\{8, 20, 31, 41, 50, 58, 65, 71, 76, 80, 83, 85\}$$

(des entiers $5, 13, 21, \ldots$ de la forme $8k+5$), on voit qu'on passe d'une somme de restes à la suivante en faisant $+12, +11, +10, +9, +8, etc.$. La somme des restes quintiques d'un nombre est donc une somme $\sum(12-k)$ et est de second degré en k.

On ne parvient pas à trouver la règle pour les $8k+1$.

Résumé

forme de n	*sum quadrat.*	*sum cubic.*	*sum quintic.*
$24k$	$n/12$	$48k \to 0$ $48k+24 \to n/2$	$48k \to 0$ $48k+24 \to n/2$
$24k+1$	0	k^2	
$24k+2$	$n/2$	$n/2$	$n/2$
$24k+3$	$n/3$	k^2+3k+1	
$24k+4$	$n/4$	$48k+4 \to n/4$ $48k+28 \to 3n/4$	$48k+4 \to n/4$ $48k+28 \to 3n/4$
$24k+5$	0	k^2-k-1	
$24k+6$	$n/3$	0	0
$24k+7$	0	k^2	0
$24k+8$	$3n/4$	$48k+32 \to 0$ $48k+8 \to n/2$	$48k+32 \to 0$ $48k+8 \to n/2$
$24k+9$	$n/3$	k^2	
$24k+10$	$n/2$	$n/2$	$n/2$
$24k+11$	0	k^2+3k+1	
$24k+12$	$7n/12$	$48k+36 \to n/4$ $48k+12 \to 3n/4$	$48k+36 \to n/4$ $48k+12 \to 3n/4$
$24k+13$	0	k^2-k-1	
$24k+14$	0	0	0
$24k+15$	$n/3$	k^2	0
$24k+16$	$3n/4$	$48k+40 \to n/2$ $48k+16 \to 0$	$48k+40 \to n/2$ $48k+16 \to 0$
$24k+17$	0	k^2	
$24k+18$	$5n/6$	$n/2$	$n/2$
$24k+19$	0	k^2+3k+1	
$24k+20$	$n/4$	$48k+44 \to 3n/4$ $48k+20 \to n/4$	$48k+44 \to 3n/4$ $48k+20 \to n/4$
$24k+21$	$n/3$	k^2-k-1	
$24k+22$	0	0	0
$24k+23$	0	k^2	0

On voit que les sommes de restes, dans le cas de restes quadratiques, sont toujours linéairement proportionnelles à n, ce qui n'est pas le cas des restes pour les puissances supérieures impaires (quelques calculs pour les puissances biquadratiques montrent qu'il semblerait que la linéarité de la somme des restes advienne pour toutes les sommes de restes des puissances paires).

On constate également que les sommes de restes quadratiques sont systématiquement nulles pour les nombres premiers qui sont nécessairement de la forme $24k+1$, ou $24k+5$ ou $24k+7$ ou $24k+11$ ou $24k+13$ ou $24k+17$ ou $24k+19$ ou $24k+23$.

Cela serait-il lié à l'hypothèse de Riemann, l'appartenance des zéros de zêta à la droite des complexes de partie réelle $\frac{1}{2}$ pouvant être interprété comme le fait d'enrouler une spirale brisée dont les côtés seraient fonctions des racines carrées des entiers successifs autour du point origine ? On peut rêver.

On comprend en étudiant les restes cubiques et quintiques de 2 nombres $8k+4$ (20 et 28) pour quelle raison leur somme de restes de l'un ou l'autre degré sont égales : il y a pour le premier cas échange de certains restes (12 et 8 d'une part, 7 et 3 d'autre part par exemple, pour les restes de 20), les autres restes étant fixes, ce qui préserve la somme ; dans le second cas, la plupart des restes sont modifiées mais le résultat est invariant modulo 28.

Restes de 20

	1	2	3	4	5	6	7	8	9	10
restes cubiques	1	8	7	4	5	16	3	12	9	0
restes quintiques	1	12	3	4	5	16	7	8	9	0

Restes de 28

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
restes cubiques	1	8	27	8	13	20	7	8	1	20	15	20	13	0
restes quintiques	1	4	19	16	17	20	7	8	25	12	23	24	13	0

Sommes de résidus modulaires (Denise Vella-Chemla, 17.8.2017)

a) Somme des résidus quadratiques

On utilise la formule $1^2 + 2^2 + \ldots + k^2 = \dfrac{k(k+1)(2k+1)}{6}$.

1) $n = 24k$

$$\begin{aligned}\sum_{x=1}^{12k} x^2 &= \frac{12k(12k+1)(24k+1)}{6} \\ &= \frac{3456k^3 + 432k^2 + 12k}{6} \\ &= k(576k^2 + 72k + 2)\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k$, on divise le polynôme ci-dessus par $24k$, on trouve $24k + 3$ reste $2k$ qui est bien égal à $\dfrac{n}{12}$.

2) $n = 24k + 1$

$$\begin{aligned}\sum_{x=1}^{12k} x^2 &= \frac{12k(12k+1)(24k+1)}{6} \\ &= \frac{3456k^3 + 432k^2 + 12k}{6} \\ &= k(576k^2 + 72k + 2)\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 1$, on divise le polynôme ci-dessus par $24k + 1$, on trouve $24k + 2$ reste 0.

3) $n = 24k + 2$

$$\begin{aligned}\sum_{x=1}^{12k+1} x^2 &= \frac{(12k+1)(12k+2)(24k+3)}{6} \\ &= \frac{3456k^3 + 1296k^2 + 156k + 6}{6} \\ &= 576k^3 + 216k^2 + 26k + 1\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 2$, on divise le polynôme ci-dessus par $24k + 2$, on trouve $24k^2 + 7k$ reste $12k + 1$ qui est bien égal à $\dfrac{n}{2}$.

4) $n = 24k + 3$

$$\begin{aligned}\sum_{x=1}^{12k+1} x^2 &= \frac{(12k+1)(12k+2)(24k+3)}{6} \\ &= \frac{3456k^3 + 1296k^2 + 156k + 6}{6} \\ &= 576k^3 + 216k^2 + 26k + 1\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 3$, on divise le polynôme ci-dessus par $24k + 3$, on trouve $24k^2 + 6k$ reste $8k + 1$ qui est bien égal à $\dfrac{n}{3}$.

5) $n = 24k + 4$

$$\begin{aligned}\sum_{x=1}^{12k+2} x^2 &= \frac{(12k+2)(12k+3)(24k+5)}{6} \\ &= \frac{3456k^3 + 2160k^2 + 444k + 30}{6} \\ &= 576k^3 + 360k^2 + 74k + 5\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 4$, on divise le polynôme ci-dessus par $24k + 4$, on trouve $24k^2 + 11k + 1$ reste $6k + 1$ qui est bien égal à $\dfrac{n}{4}$.

6) $n = 24k + 5$

$$\begin{aligned}\sum_{x=1}^{12k+2} x^2 &= \frac{(12k+2)(12k+3)(24k+5)}{6} \\ &= \frac{3456k^3 + 2160k^2 + 444k + 30}{6} \\ &= 576k^3 + 360k^2 + 74k + 5\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 5$, on divise le polynôme ci-dessus par $24k + 5$, on trouve $24k^2 + 10k + 1$ reste 0.

7) $n = 24k + 6$

$$\begin{aligned}\sum_{x=1}^{12k+3} x^2 &= \frac{(12k+3)(12k+4)(24k+7)}{6} \\ &= \frac{3456k^3 + 3024k^2 + 876k + 84}{6} \\ &= 576k^3 + 504k^2 + 146k + 14\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 6$, on divise le polynôme ci-dessus par $24k + 6$, on trouve $24k^2 + 15k + 2$ reste $8k + 2$ qui est bien égal à $\frac{n}{3}$.

8) $n = 24k + 7$

$$\begin{aligned}\sum_{x=1}^{12k+3} x^2 &= \frac{(12k+3)(12k+4)(24k+7)}{6} \\ &= \frac{3456k^3 + 3024k^2 + 876k + 84}{6} \\ &= 576k^3 + 504k^2 + 146k + 14\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 7$, on divise le polynôme ci-dessus par $24k + 7$, on trouve $24k^2 + 14k$ reste 0.

9) $n = 24k + 8$

$$\begin{aligned}\sum_{x=1}^{12k+4} x^2 &= \frac{(12k+4)(12k+5)(24k+9)}{6} \\ &= \frac{3456k^3 + 3888k^2 + 1452k + 180}{6} \\ &= 576k^3 + 648k^2 + 242k + 30\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 8$, on divise le polynôme ci-dessus par $24k + 8$, on trouve $24k^2 + 19k + 3$ reste $18k + 6$ qui est bien égal à $\frac{3n}{4}$.

10) $n = 24k + 9$

$$\begin{aligned}\sum_{x=1}^{12k+4} x^2 &= \frac{(12k+4)(12k+5)(24k+9)}{6} \\ &= \frac{3456k^3 + 3888k^2 + 1452k + 180}{6} \\ &= 576k^3 + 648k^2 + 242k + 30\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 9$, on divise le polynôme ci-dessus par $24k + 9$, on trouve $24k^2 + 18k + 3$ reste $8k + 3$ qui est bien égal à $\frac{n}{3}$.

11) $n = 24k + 10$

$$\begin{aligned}\sum_{x=1}^{12k+5} x^2 &= \frac{(12k+5)(12k+6)(24k+11)}{6} \\ &= 576k^3 + 792k^2 + 362k + 55\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 10$, on divise le polynôme ci-dessus par $24k + 10$, on trouve $24k^2 + 23k + 5$ reste $12k + 5$ qui est bien égal à $\frac{n}{2}$.

12) $n = 24k + 11$

$$\begin{aligned}\sum_{x=1}^{12k+5} x^2 &= \frac{(12k+5)(12k+6)(24k+11)}{6} \\ &= 576k^3 + 792k^2 + 362k + 55\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 11$, on divise le polynôme ci-dessus par $24k + 11$, on trouve $24k^2 + 22k + 5$ reste 0.

13) $n = 24k + 12$

$$\begin{aligned}\sum_{x=1}^{12k+6} x^2 &= \frac{(12k+6)(12k+7)(24k+13)}{6} \\ &= 576k^3 + 936k^2 + 506k + 91\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 12$, on divise le polynôme ci-dessus par $24k + 12$, on trouve $24k^2 + 27k + 7$ reste $14k + 7$ qui est bien égal à $\frac{7n}{12}$.

14) $n = 24k + 13$

$$\begin{aligned}\sum_{x=1}^{12k+6} x^2 &= \frac{(12k+6)(12k+7)(24k+13)}{6} \\ &= 576k^3 + 936k^2 + 506k + 91\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 13$, on divise le polynôme ci-dessus par $24k + 13$, on trouve $24k^2 + 26k + 7$ reste 0.

15) $n = 24k + 14$

$$\begin{aligned}\sum_{x=1}^{12k+7} x^2 &= \frac{(12k+7)(12k+8)(24k+15)}{6} \\ &= 576k^3 + 1080k^2 + 674k + 140\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 14$, on divise le polynôme ci-dessus par $24k + 14$, on trouve $24k^2 + 31k + 10$ reste 0.

16) $n = 24k + 15$

$$\begin{aligned}\sum_{x=1}^{12k+7} x^2 &= \frac{(12k+7)(12k+8)(24k+15)}{6} \\ &= 576k^3 + 1080k^2 + 674k + 140\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 15$, on divise le polynôme ci-dessus par $24k + 15$, on trouve $24k^2 + 30k + 9$ reste $8k + 5$ qui est bien égal à $\frac{n}{3}$.

17) $n = 24k + 16$

$$\begin{aligned}\sum_{x=1}^{12k+8} x^2 &= \frac{(12k+8)(12k+9)(24k+17)}{6} \\ &= 576k^3 + 1224k^2 + 866k + 204\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 16$, on divise le polynôme ci-dessus par $24k + 16$, on trouve $24k^2 + 35k + 12$ reste $18k + 12$ qui est bien égal à $\frac{3n}{4}$.

18) $n = 24k + 17$

$$\begin{aligned}\sum_{x=1}^{12k+8} x^2 &= \frac{(12k+8)(12k+9)(24k+17)}{6} \\ &= 576k^3 + 1224k^2 + 866k + 204\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 17$, on divise le polynôme ci-dessus par $24k + 17$, on trouve $24k^2 + 34k + 12$ reste 0.

19) $n = 24k + 18$

$$\begin{aligned}\sum_{x=1}^{12k+9} x^2 &= \frac{(12k+9)(12k+10)(24k+19)}{6} \\ &= 576k^3 + 1368k^2 + 1082k + 285\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 18$, on divise le polynôme ci-dessus par $24k + 18$, on trouve $24k^2 + 39k + 15$ reste $20k + 15$ qui est bien égal à $\frac{5n}{6}$.

20) $n = 24k + 19$

$$\begin{aligned}\sum_{x=1}^{12k+9} x^2 &= \frac{(12k+9)(12k+10)(24k+19)}{6} \\ &= 576k^3 + 1368k^2 + 1082k + 285\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 19$, on divise le polynôme ci-dessus par $24k + 19$, on trouve $24k^2 + 38k + 15$ reste 0.

21) $n = 24k + 20$

$$\begin{aligned}\sum_{x=1}^{12k+10} x^2 &= \frac{(12k+10)(12k+11)(24k+21)}{6} \\ &= 576k^3 + 1512k^2 + 1322k + 385\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 20$, on divise le polynôme ci-dessus par $24k + 20$, on trouve $24k^2 + 43k + 19$ reste $6k + 5$ qui est bien égal à $\frac{n}{4}$.

22) $n = 24k + 21$

$$\begin{aligned}\sum_{x=1}^{12k+10} x^2 &= \frac{(12k+10)(12k+11)(24k+21)}{6} \\ &= 576k^3 + 1512k^2 + 1322k + 385\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 21$, on divise le polynôme ci-dessus par $24k + 21$, on trouve $24k^2 + 42k + 18$ reste $8k + 7$ qui est bien égal à $\frac{n}{3}$.

23) $n = 24k + 22$

$$\begin{aligned}\sum_{x=1}^{12k+11} x^2 &= \frac{(12k+11)(12k+12)(24k+23)}{6} \\ &= 576k^3 + 1656k^2 + 1586k + 506\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 22$, on divise le polynôme ci-dessus par $24k + 22$, on trouve $24k^2 + 47k + 23$ reste 0.

24) $n = 24k + 23$

$$\begin{aligned}\sum_{x=1}^{12k+11} x^2 &= \frac{(12k+11)(12k+12)(24k+23)}{6} \\ &= 576k^3 + 1656k^2 + 1586k + 506\end{aligned}$$

Pour trouver le reste quadratique modulo $n = 24k + 23$, on divise le polynôme ci-dessus par $24k + 23$, on trouve $24k^2 + 46k + 22$ reste 0.

Moyenne des résidus quadratiques et moitié des nombres (Denise Vella-Chemla, 21.8.2017)

On poursuit ici nos expérimentations numériques en programmant de nouveaux calculs sur les résidus quadratiques modulaires des entiers.

On calcule pour chaque nombre x entre 3 et 100 la moyenne des résidus quadratiques des nombres inférieurs à la moitié de x. Illustrons cela par deux exemples :

- pour $x = 11, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 5, 5^2 = 3$, la moyenne vaut $\frac{1+4+9+5+3}{5} = \frac{22}{5} = 4.4$;
- pour $x = 13, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 3, 5^2 = 12, 6^2 = 10$, la moyenne vaut $\frac{1+4+9+3+12+10}{6} = \frac{39}{6} = 6.5$;

Attention à l'ordre dans lequel les opérations doivent être effectuées : effectuer d'abord la somme des carrés, puis la réduction modulaire n'aboutit pas au même résultat qu'effectuer d'abord les réductions modulaires, puis sommer les résultats (pour 13, la somme des carrés aurait abouti au nombre $91 = 1+4+9+16+25+36$ *et la réduction modulaire sur le résultat 91 aurait abouti à 0 puisque* $91 = 13 \times 7$ *; les réductions modulaires effectuées d'abord sur chaque carré indépendamment n'ont permis de soustraire que* 4×13 *à 91 (*1×13 *soustraite de 16,* 1×13 *soustraite de 25 et* 2×13 *soustraites de 36) et sommer les réductions modulaires a alors comme résultat 39 (différent du 0 obtenu en effectuant les opérations dans l'ordre inverse).*

Le programme de calcul des moyennes en C++ est fourni en annexe.

Voici le résultat de ce programme (pour les nombres x inférieurs ou égaux à 20, on a détaillé entre parenthèses les calculs des résidus quadratiques des nombres inférieurs à $\frac{x-1}{2}$).

```
3 ->
   (1,1),
   1
4 ->
   (1,1),(2,0),
   0.5
5 ->
   (1,1),(2,4),
   2.5
6 ->
   (1,1),(2,4),(3,3),
   2.66667
7 ->
   (1,1),(2,4),(3,2),
   2.33333
8 ->
   (1,1),(2,4),(3,1),(4,0),
   1.5
9 ->
   (1,1),(2,4),(3,0),(4,7),
   3
10 ->
   (1,1),(2,4),(3,9),(4,6),(5,5),
   5
11 ->
   (1,1),(2,4),(3,9),(4,5),(5,3),
   4.4
12 ->
   (1,1),(2,4),(3,9),(4,4),(5,1),(6,0),
   3.16667
```

```
13 ->
   (1,1),(2,4),(3,9),(4,3),(5,12),(6,10),
   6.5
14 ->
   (1,1),(2,4),(3,9),(4,2),(5,11),(6,8),(7,7),
   6
15 ->
   (1,1),(2,4),(3,9),(4,1),(5,10),(6,6),(7,4),
   5
16 ->
   (1,1),(2,4),(3,9),(4,0),(5,9),(6,4),(7,1),(8,0),
   3.5
17 ->
   (1,1),(2,4),(3,9),(4,16),(5,8),(6,2),(7,15),(8,13),
   8.5
18 ->
   (1,1),(2,4),(3,9),(4,16),(5,7),(6,0),(7,13),(8,10),(9,9),
   7.66667
19 ->
   (1,1),(2,4),(3,9),(4,16),(5,6),(6,17),(7,11),(8,7),(9,5),
   8.44444
20 ->
   (1,1),(2,4),(3,9),(4,16),(5,5),(6,16),(7,9),(8,4),(9,1),(10,0),
   6.5
```

$21 \to 9.1$	$41 \to 20.5$	$61 \to 30.5$	$81 \to 35.1$
$22 \to 10$	$42 \to 19.6667$	$62 \to 28$	$82 \to 41$
$23 \to 8.36364$	$43 \to 20.4762$	$63 \to 25.0645$	$83 \to 38.4634$
$24 \to 6.16667$	$44 \to 16.5$	$64 \to 21.5$	$84 \to 33.1667$
$25 \to 10.4167$	$45 \to 19.0909$	$65 \to 32.5$	$85 \to 42.5$
$26 \to 13$	$46 \to 20$	$66 \to 31.6667$	$86 \to 42$
$27 \to 11.0769$	$47 \to 18.3913$	$67 \to 32.4848$	$87 \to 37.093$
$28 \to 10.5$	$48 \to 14.1667$	$68 \to 28.5$	$88 \to 35.5$
$29 \to 14.5$	$49 \to 20.4167$	$69 \to 31.1176$	$89 \to 44.5$
$30 \to 12.6667$	$50 \to 23$	$70 \to 32$	$90 \to 41.6667$
$31 \to 12.4$	$51 \to 23.12$	$71 \to 28.4$	$91 \to 42.4667$
$32 \to 9.5$	$52 \to 22.5$	$72 \to 24.1667$	$92 \to 38.5$
$33 \to 15.125$	$53 \to 26.5$	$73 \to 36.5$	$93 \to 43.1304$
$34 \to 17$	$54 \to 24.6667$	$74 \to 37$	$94 \to 42$
$35 \to 14.4118$	$55 \to 22.4074$	$75 \to 31.0811$	$95 \to 38.4043$
$36 \to 11.1667$	$56 \to 19.5$	$76 \to 32.5$	$96 \to 32.1667$
$37 \to 18.5$	$57 \to 27.1429$	$77 \to 36.4737$	$97 \to 48.5$
$38 \to 18$	$58 \to 29$	$78 \to 34.6667$	$98 \to 45$
$39 \to 15.0526$	$59 \to 26.4483$	$79 \to 34.4359$	$99 \to 45.1224$
$40 \to 13.5$	$60 \to 21.1667$	$80 \to 27.5$	$100 \to 40.5$

On constate que la moyenne des restes pour les nombres premiers de la forme $p = 4k + 1$ (que sont 5, 13, 17, 29, 37, 41, 53, 61, 73, 89 et 97) est égale à $\frac{n}{2}$. Cela reste à prouver.

On constate qu'il en est de même pour les doubles des nombres premiers en question que sont 10, 26, 34, 58, 74 et 82.

Cette propriété ne semble pas vérifiée par une grosse majorité des nombres de la forme $4k + 1$ qui ne sont pas premiers : 9, 21, 25, 33, 45, 49, 57, 65, 69, 77, 81, 93 ; elle est cependant vérifiée par les nombre 65 et 85 qui sont chacun produits de 2 nombres premiers de la forme $4k + 1$: $65 = 5 \times 13$ et $85 = 5 \times 17$. On confirme en exécutant "plus loin" que la moyenne des restes quadratiques pour les nombres n suivants vaut $n/2$: 130 ($= 2 \times 5 \times 13$), 145 ($= 5 \times 29$), 170 ($= 2 \times 5 \times 17$), 185 ($= 5 \times 37$) ou 205 ($= 5 \times 41$), les factorisations de tous ces nombres contenant exclusivement deux nombres premiers de la forme $4k+1$ (soit aucun premier de la forme $4k + 3$), et parfois un facteur 2. On le confirme encore en trouvant $n/2$ comme moyenne des résidus quadratiques pour les nombres 481 ($= 13 \times 37$), 485 ($= 5 \times 97$), 493 ($= 17 \times 29$), 505

$(= 5 \times 101)$, 533 $(= 13 \times 41)$, 545 $(= 5 \times 109)$, 565 $(= 5 \times 113)$, 629 $(= 17 \times 37)$, 685 $(= 5 \times 137)$, 689 $(= 13 \times 53)$, 697 $(= 17 \times 41)$, 745 $(= 5 \times 149)$, 785 $(= 5 \times 157)$, 793 $(= 13 \times 61)$, 865 $(= 5 \times 173)$, 901 $(= 17 \times 53)$, 905 $(= 5 \times 181)$, 949 $(= 13 \times 73)$, 965 $(= 5 \times 193)$, 985 $(= 5 \times 197)$ ou enfin $2 \times 965 = 1930$, ce qui semble ne pas pouvoir être fortuit.

A première vue, il aurait pu sembler que les $n = 20k + 11$ premiers que sont 11, 31, 71 ont leur moyenne des restes quadratiques égale à $\frac{2n}{5}$ alors que cela n'est pas le cas des $n = 20k + 11$ composés que sont 51 et 91 mais on infirme cette hypothèse pour $n = 131$.

Ainsi, aucune formule évidente ne semble se dégager pour les nombres premiers (ou pas) de la forme $4k+3$.

Annexe : programme de calcul des moyennes des résidus quadratiques modulaires

```
#include <iostream>
#include <stdio.h>
#include <cmath>

int prime(int atester) {
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve) {
    if ((k * k) > atester) return 1;
    else
      if ((atester % k) == 0) return 0 ;
      else k++;
  }
}

int puiss(int n,int k,int m) {
  int result ;

  if (k == 0) result = 1;
  else result = (n * puiss(n,k-1,m)) % m;
  return result;
}

int main (int argc, char* argv[])
{
  int n, x, sommeres, bout, tempo ;

  for (n = 3 ; n <= 100 ; ++n) {
    std::cout << n << " -> " ;
    if (n <= 20) std::cout << "\n " ;
    sommeres = 0 ;
    if ((n % 2) == 0) bout = n/2 ; else bout=(n-1)/2 ;
    for (x = 1 ; x <= bout ; ++x) {
      tempo = puiss(x,2,n) ;
      if (n <= 20) std::cout << "(" << x << "," << tempo << ")," ;
      sommeres = sommeres+tempo ;
    }
    if (n <= 20) std::cout << "\n " ;
    std::cout << (float) sommeres / (float) bout << "\n" ;
  }
}
```

Différence entre les fonctions f et F de l'article de Riemann concernant le nombre des nombres premiers inférieurs à une grandeur donnée (22.8.2017)

Dans son article si important, Riemann utilise deux fonctions $f(x)$ et $F(x)$ (cette dernière correspondant à $\pi(x)$, le nombre de nombres premiers inférieurs à x) dont on étudie ci-après ce qui les distingue lorsqu'on limite, comme préconisé dans la note de Riemann, ces sommes à un nombre fini de termes.

$\pi(x)$ étant nul lorsque $x < 2$, on prendra comme derniers éléments des sommes les logarithmes à base 2.

(1) $$f(x) = \sum_{k=1}^{\lfloor log_2\ x \rfloor} \frac{1}{k} F\left(x^{\frac{1}{k}}\right)$$

(2) $$F(x) = \sum_{k \geqslant 2} \frac{\mu(k)}{k} f\left(x^{\frac{1}{k}}\right)$$

(3) $$f(x^{\frac{1}{k}}) = \sum_{l=1}^{\left\lfloor \frac{1}{k}\ log_2\ x \right\rfloor} \frac{1}{l} F\left(x^{\frac{1}{kl}}\right)$$

(4) $$F(x^{\frac{1}{k}}) = \sum_{l \geqslant 2} \frac{\mu(l)}{l} f\left(x^{\frac{1}{kl}}\right)$$

(1) + (4) $$f(x) = \sum_{k=1}^{\lfloor log_2\ x \rfloor} \frac{1}{k} \sum_{l \geqslant 2} \frac{\mu(l)}{l} f\left(x^{\frac{1}{kl}}\right)$$

$$= \sum_{k=1, l \geqslant 2}^{k=\left\lfloor \frac{ln\ x}{ln\ 2} \right\rfloor} \frac{\mu(l)}{kl} f\left(x^{\frac{1}{kl}}\right)$$

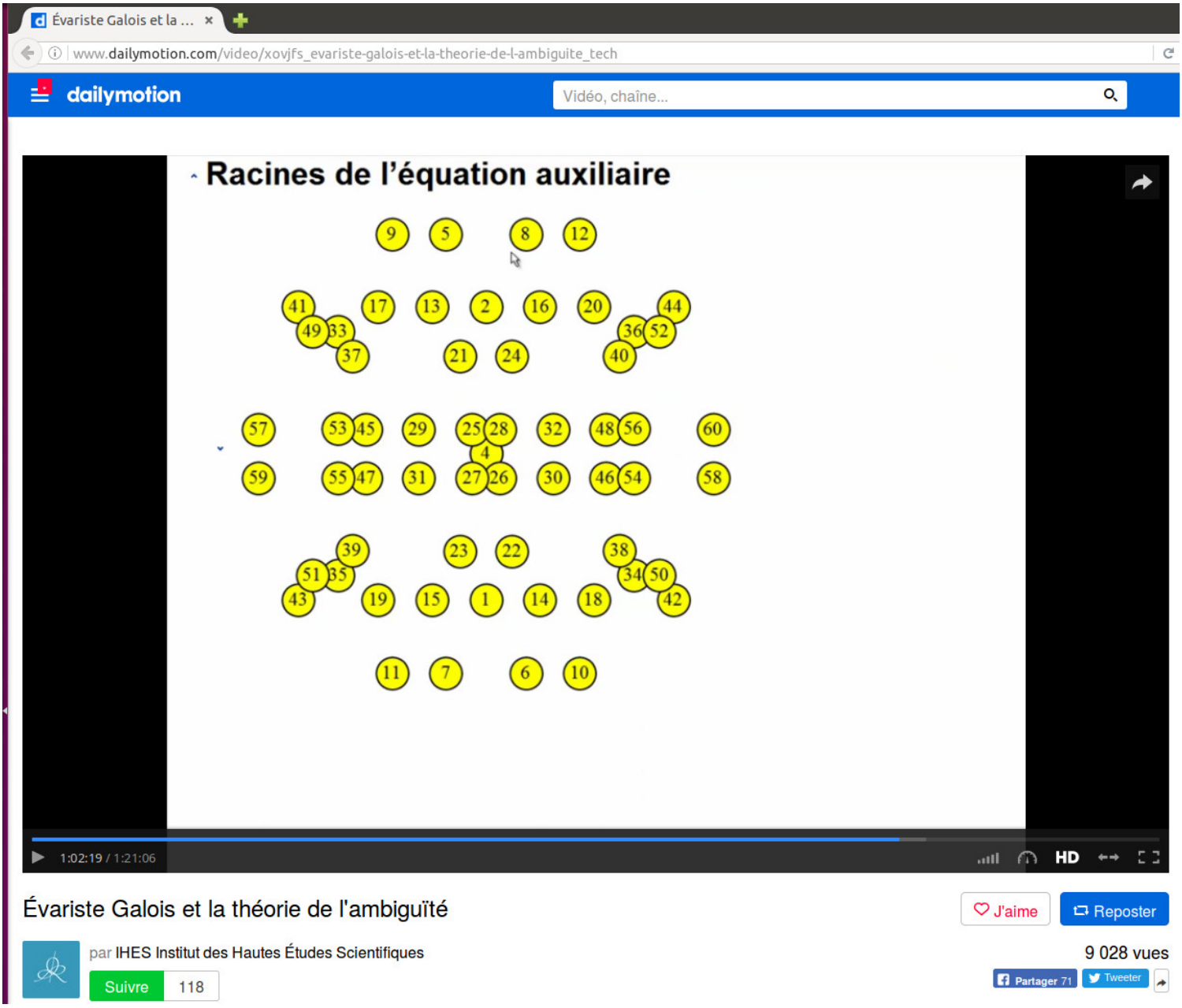
(2) + (3) $$F(x) = \sum_{k \geqslant 2} \frac{\mu(k)}{k} \sum_{l=1}^{\left\lfloor \frac{1}{k}\ \frac{ln\ x}{ln\ 2} \right\rfloor} \frac{1}{l} F\left(x^{\frac{1}{kl}}\right)$$

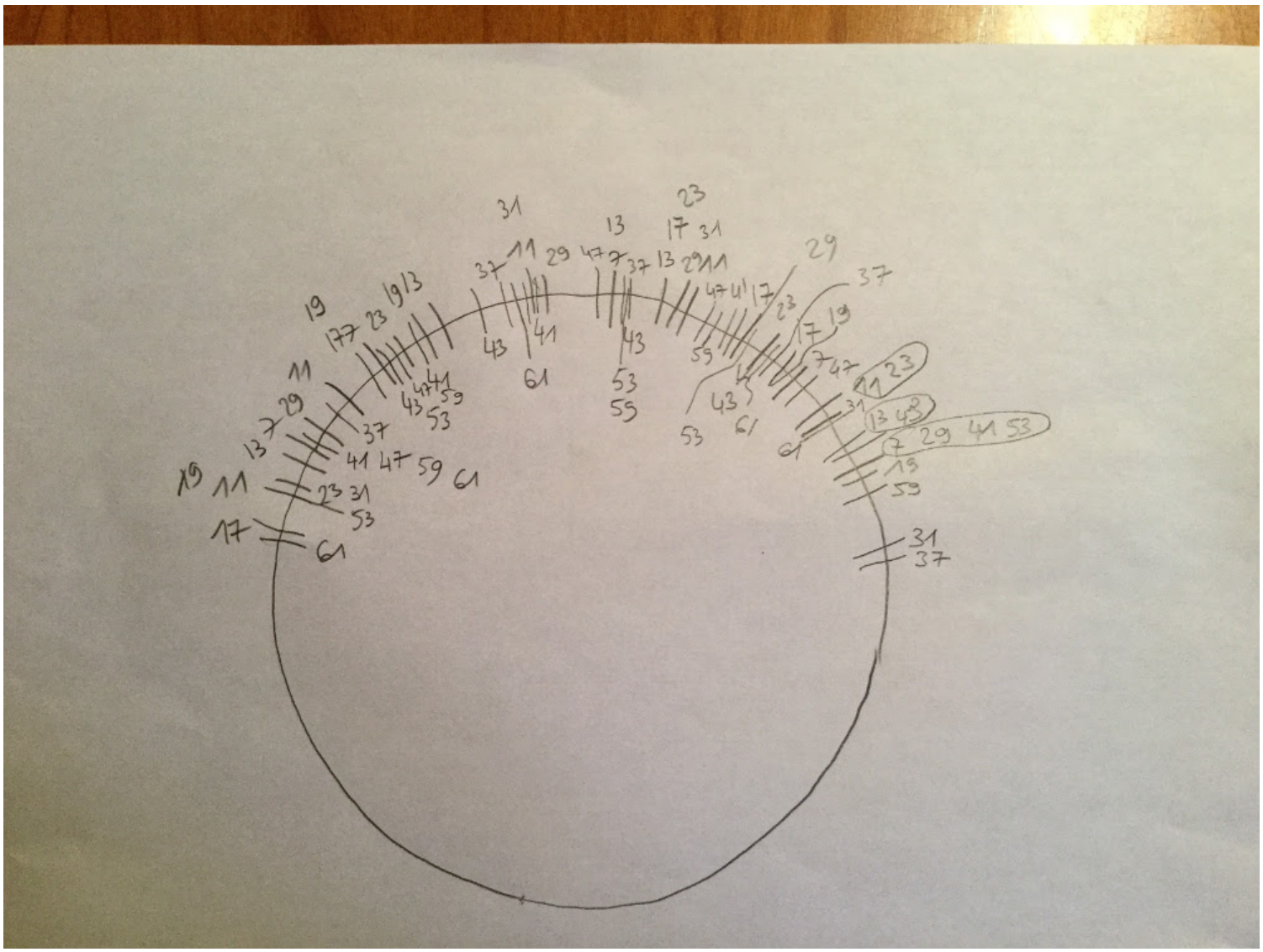
$$= \sum_{k \geqslant 2, l=1}^{l=\left\lfloor \frac{1}{k}\ \frac{ln\ x}{ln\ 2} \right\rfloor} \frac{\mu(k)}{kl} F\left(x^{\frac{1}{kl}}\right)$$

(en échangeant k et l) $$F(x) = \sum_{l \geqslant 2, k=1}^{k=\left\lfloor \frac{1}{l}\ \frac{ln\ x}{ln\ 2} \right\rfloor} \frac{\mu(l)}{kl} F\left(x^{\frac{1}{kl}}\right)$$

On voit que la différence entre les deux fonctions se situe au niveau du dernier terme de la somme qui est $k = \left\lfloor \frac{ln\ x}{ln\ 2} \right\rfloor$ pour le calcul de $f(x)$ et $\lfloor \frac{1}{l}\ \frac{ln\ x}{ln\ 2} \rfloor$ pour le calcul de $F(x)$.

$$n \ \ premier$$
$$\Longleftrightarrow$$
$$\sum_{i=2}^{n-3} \left(\left\lfloor \frac{n}{i} \right\rfloor - 1 \right) = \#\left\{ xy \ \ tels \ \ que \ \ (xy < n) \ \wedge \ (2 \leqslant x \leqslant n-2) \ \wedge \ (2 \leqslant y \leqslant n-2) \right\}$$


Évariste Galois et la ...
www.dailymotion.com/video/xovjfs_evariste-galois-et-la-theorie-de-l-ambiguite_tech
dailymotion
Vidéo, chaîne...
Racines de l'équation auxiliaire
9 5 8 12
41 17 13 2 16 20 44
49 33 36 52
37 21 24 40
57 53 45 29 25 28 32 48 56 60
4
59 55 47 31 27 26 30 46 54 58
39 23 22 38
51 35 34 50
43 19 15 1 14 18 42
11 7 6 10
1:02:19 / 1:21:06
HD
Évariste Galois et la théorie de l'ambiguïté
J'aime
Reposter
par IHES Institut des Hautes Études Scientifiques
Suivre 118
9 028 vues
Partager 71
Tweeter



Pile la moitié *(Denise Vella-Chemla, 17.10.2017)*

On rappelle la section 96 des Recherches arithmétiques de Gauss :

> *96. Le nombre premier p étant pris pour module, la moitié des nombres $1, 2, 3 \ldots p-1$, sera composée de résidus quadratiques, et l'autre moitié de non-résidus, c'est-à-dire qu'il y aura $\frac{1}{2}(p-1)$ résidus et autant de non-résidus.*
>
> *On prouve facilement que tous les carrés $1, 4, 9 \ldots \left(\frac{p-1}{2}\right)^2$ sont incongrus ; car si l'on pouvait avoir $r^2 \equiv r'^2 \pmod{p}$ et que les nombres r et r' fussent inégaux et $< \frac{p-1}{2}$, soit $r > r'$, on aurait $(r-r')(r+r')$, divisible par p ; mais chaque facteur étant $< p$, la proposition ne peut subsister. Il y a donc $\frac{p-1}{2}$ résidus quadratiques entre les nombres $1, 2, 3 \ldots p-1$; il ne peut y en avoir davantage, car en y joignant 0, le nombre en devient $\frac{1}{2}(p+1)$, limite qu'il ne peut pas dépasser. Donc les autres nombres seront non-résidus, et il y en aura $\frac{p-1}{2}$.*
>
> *Comme 0 est toujours résidu, nous l'excluons.*

Les nombres premiers p sont *les seuls* nombres à partager exactement l'ensemble des nombres compris entre 1 et $p-1$ en deux ensembles de même cardinal : l'ensemble des résidus quadratiques et l'ensemble des non-résidus quadratiques.

On illustre ci-dessous ce partage équitable des $p-1$ premiers entiers strictement positifs entre les résidus quadratiques et les non-résidus quadratiques modulo 17 (de la forme $4k+1$) et modulo 19 (de la forme $4k+3$). Les résidus quadratiques sont colorés en bleu. On a noté les valeurs des carrés pour rappel en bas, en deça du trait séparateur. L'usage de la couleur permet aussi de mettre en évidence, pour p premier, une relation entre le caractère de résiduosité quadratique d'un nombre x et celui de son complémentaire à p (ou $p - x = -x = (-1) \times x$).

Résidus quadratiques pour $p = 17$

16	15	14	13	12	11	10	9
1	2	3	4	5	6	7	8
1	4	9	16	8	2	15	13

Résidus quadratiques pour $p = 19$

18	17	16	15	14	13	12	11	10
1	2	3	4	5	6	7	8	9
1	4	9	16	6	17	11	7	5

On voit que pour p premier de la forme $4k+1$, x et $p-x$, dans la même colonne, sont soit tous deux résidus quadratiques, soit tous deux non-résidus quadratiques (cela est dû aux faits que $p - x = -x$ et que $p - 1 = -1$ est résidu quadratique).

Tandis que pour p de la forme $4k+3$, x est résidu quadratique équivaut à $p-x$ n'est pas résidu quadratique et inversement ($p - 1 = -1$ est alors non-résidu quadratique).

Ces équivalences ne sont pas vérifiées pour les nombres composés.

Pour le module 15, on a le petit tableau de Gauss des résidus quadratiques suivant :

14	13	12	11	10	9	8
1	2	3	4	5	6	7
1	4	9	1	10	6	4

Tout résidu quadratique r de tout nombre premier p vérifie la congruence :

$$r^{\frac{p-1}{2}} \equiv +1 \ (mod\ p)$$

tandis que tout non-résidu quadratique n de tout nombre premier p vérifie la congruence :

$$n^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$$

On vérifie ces congruences en calculant les valeurs des puissances $8^{èmes}$ des nombres modulo 17 ($8 = \frac{17-1}{2}$) et $9^{èmes}$ des nombres modulo 19 ($9 = \frac{18-1}{2}$) :

puissance	*valeur*	*classe* (*mod* 17)	*puissance*	*valeur*	*classe* (*mod* 19)
1^8	1	$+1$	1^9	1	$+1$
2^8	256	$+1$	2^9	512	-1
3^8	6 561	-1	3^9	19 683	-1
4^8	65 536	$+1$	4^9	262 144	$+1$
5^8	390 625	-1	5^9	1 953 125	$+1$
6^8	1 679 616	-1	6^9	10 077 696	$+1$
7^8	5 764 801	-1	7^9	40 353 607	$+1$
8^8	16 777 216	$+1$	8^9	134 217 728	-1
9^8	43 046 721	$+1$	9^9	387 420 480	$+1$
10^8	100 000 000	-1	10^9	1 000 000 000	-1
11^8	214 358 881	-1	11^9	2 357 947 691	$+1$
12^8	429 981 696	-1	12^9	5 159 780 352	-1
13^8	815 730 721	$+1$	13^9	10 604 499 373	-1
14^8	1 475 789 056	-1	14^9	20 661 046 784	-1
15^8	2 562 890 625	$+1$	15^9	38 443 359 375	-1
16^8	4 294 967 296	$+1$	16^9	68 719 476 736	$+1$
			17^9	118 587 876 497	$+1$
			18^9	198 359 290 368	-1

En annexe sont fournies les tables des résidus des puissances des nombres modulo 17 et 19.

Etudions maintenant les puissances successives modulaires de nombres (dont la racine carrée de la $(p-1)^{ème}$ puissance ou $\frac{1}{2}(p-1)^{ème}$ puissance). On peut voir la suite des puissances successives d'un résidu quadratique comme une suite (une chaîne orientée) $\mathcal{C}$ de $\frac{p-1}{2}$ nombres. Par l'opération d'inversion ($f : x \mapsto \frac{1}{x}$), on obtient une chaîne de nombres $\mathcal{C}'$ orientée dans l'ordre inverse de l'ordre des nombres dans $\mathcal{C}$.

Ci-dessous, les chaînes des 2^x et 9^x, tous résidus quadratiques modulo 17, en sens inverse l'une de l'autre, dont les nombres sont inverses 2 à 2 les uns des autres (par colonne).

x	1	2	3	4	5	6	7	8
2^x	2	$\to 4$	$\to 8$	$\to 16$	$\to 15$	$\to 13$	$\to 9$	$\to 1$
9^x	9	$\to 13$	$\to 15$	$\to 16$	$\to 8$	$\to 4$	$\to 2$	$\to 1$

Toute puissance d'un résidu quadratique est un résidu quadratique. Dans chaque colonne, les nombres sont inverses l'un de l'autre, par exemple, 15 et 8 sont inverses ($15 = \frac{1}{8}$) puisque $15 \times 8 = 120 \equiv 1 \ (mod\ 17)$ (*rappel: car* $119 = 7 \times 17$). De même, $2 = \frac{1}{9}$, $4 = \frac{1}{13}$,...

Voyons maintenant les chaînes des 3^x et 6^x, tous les deux non-résidus quadratiques modulo 17, les nombres des deux chaînes sont inverses 2 à 2 les uns des autres (par colonne), de même que dans le tableau précédent. On a indiqué les résidus par un R et les non-résidus par un N entre parenthèses.

x	1	2	3	4	5	6	7	8
3^x	3 (N)	$\to 9$ (R)	$\to 10$ (N)	$\to 13$ (R)	$\to 5$ (N)	$\to 15$ (R)	$\to 11$ (N)	$\to 16$ (R) ($\equiv -1$)
6^x	6 (N)	$\to 2$ (R)	$\to 12$ (N)	$\to 4$ (R)	$\to 7$ (N)	$\to 8$ (R)	$\to 14$ (N)	$\to 16$ (R) ($\equiv -1$)

Toute puissance paire d'un non-résidu quadratique est un résidu quadratique alors que toute puissance impaire d'un non-résidu quadratique est un résidu quadratique (selon l'adage "moins par moins donne plus"). On peut regarder les deux chaînes de nombres ci-dessus comme "faisant la navette" entre l'ensemble des résidus quadratiques et l'ensemble des non-résidus quadratiques. L'ensemble des résidus quadratiques forme un groupe pour la multiplication (on n'en sort pas en multipliant deux éléments) alors que l'ensemble des non-résidus quadratiques n'est pas un groupe puisque le résultat de la multiplication de deux non-résidus quadratiques est un résidu quadratique.

Voici les chaînes pour le module 19, on les a fait démarrer à 4 et 5 pour les résidus et à 2 et 10 pour les non-résidus :

x	1	2	3	4	5	6	7	8	9
4^x	4	$\to 16$	$\to 7$	$\to 9$	$\to 17$	$\to 11$	$\to 6$	$\to 5$	$\to 1$
5^x	5	$\to 6$	$\to 11$	$\to 17$	$\to 9$	$\to 7$	$\to 16$	$\to 4$	$\to 1$

x	1	2	3	4	5	6	7	8	9
2^x	2 (N)	$\to 4$ (R)	$\to 8$ (N)	$\to 16$ (R)	$\to 13$ (N)	$\to 7$ (R)	$\to 14$ (N)	$\to 9$ (R)	$\to 18$ (N) $(\equiv -1)$
10^x	10 (N)	$\to 5$ (R)	$\to 12$ (N)	$\to 6$ (R)	$\to 3$ (N)	$\to 11$ (R)	$\to 15$ (N)	$\to 17$ (R)	$\to 18$ (N) $(\equiv -1)$

Seuls les nombres premiers ont pour propriété de partager l'ensemble des résidus quadratiques exactement en 2. Du fait de redondances intervenant dans les factorisations ($4 \times 6 = 3 \times 8$ par exemple), les nombres composés ont moins de résidus quadratiques que de non-résidus quadratiques.

En s'aidant du tableau des résidus des puissances modulaires pour le module $x = 15$ fourni en annexe, on constate qu'aucune puissance $\frac{1}{2}(x-1)^{ème}$ n'est égale à 1, seule la puissance $\frac{1}{2}(x-1)^{ème}$ de $x - 1 = 14$ est égal à $-1 = 14$ et seules les puissances $(x-1)^{èmes}$ des nombres 4, 11 et 14 sont égales à 1 alors qu'on a vu que 4 est résidu quadratique de 15 quand 11 et 14 ne le sont pas. Pour les nombres composés, on ne peut établir de caractéristique générale, comme on a pu le faire pour les nombres premiers.

Résumons ce qui a été présenté.

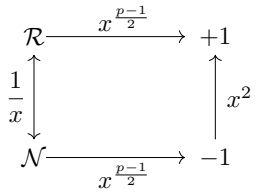
Pour p premier, si on note $\mathcal{R} = \{x / x^{\frac{p-1}{2}} \equiv +1 \ (mod\ p)\}$ et $\mathcal{N} = \{x / x^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)\}$, on a les chaînes d'élévations successives au carré suivantes, dans le groupe des résidus quadratiques :

$$f \quad : \underset{R}{x_1} \mapsto \underset{R}{x_2} \mapsto \underset{R}{x_3} \ldots \mapsto \mathbf{1} = \underset{R}{x_1}^{\frac{p-1}{2}}$$

et alternativement de l'ensemble des non-résidus quadratiques vers l'ensemble des résidus quadratiques :

$$g \quad : \underset{N}{y_1} \mapsto \underset{R}{y_2} \mapsto \underset{N}{y_3} \mapsto \underset{R}{y_4} \ldots \mapsto \mathbf{-1} = \underset{N}{y_1}^{\frac{p-1}{2}}$$

Un schéma résume la constitution des chaînes.



Lorsqu'on développe la fonction zêta de Riemann, on obtient :

$$\zeta(a+ib) = 1 + \left(\frac{1}{2}\right)^a e^{-ib\ ln\ 2} + \left(\frac{1}{3}\right)^a e^{-ib\ ln\ 3} + \left(\frac{1}{4}\right)^a e^{-ib\ ln\ 4} + \ldots$$

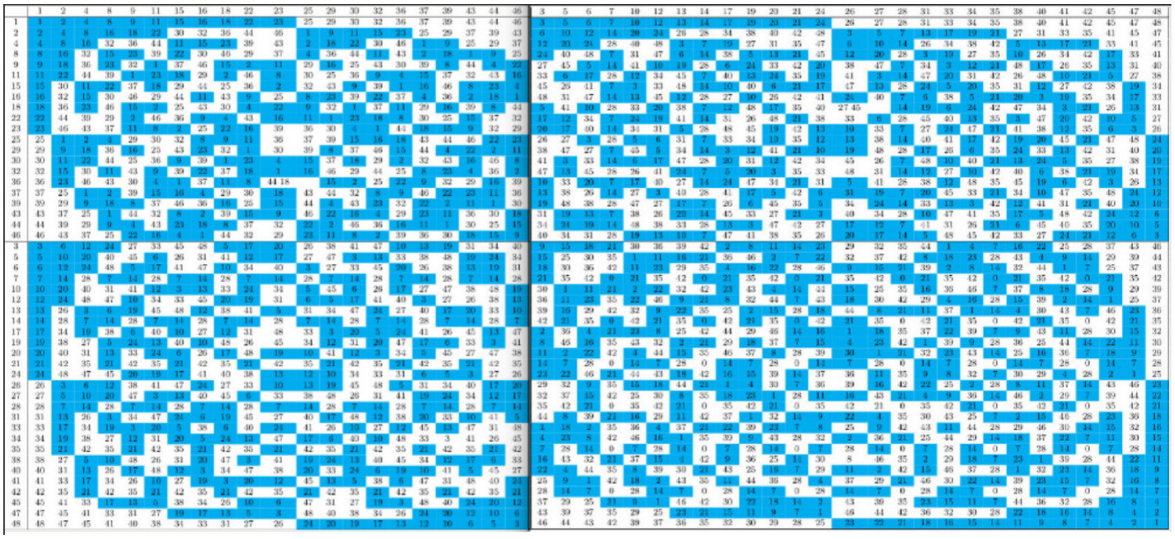
Quand $a = \frac{1}{2}$, pour les points du plan complexe situés sur la droite critique (points de partie réelle égale à $\frac{1}{2}$), les fractions devant chaque exponentielle sont les inverses des racines carrés des nombres entiers successifs : $\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{3}}, \frac{1}{\sqrt{4}}, \ldots$.

Un nombre premier (appelons le p) symétrise l'espace constitué de l'ensemble des nombres en établissant des relations particulières et systématiques entre un nombre x et son complémentaire à p $(p-x)$. On avait déjà présenté cette symétrie que l'on voit aisément dans les tables de multiplication suivantes, la première étant la table du nombre premier 23 et la seconde étant celle du nombre composé 49.

La table de multiplication de 23 qui présente symétrise les résidus qudratiques et les non-résidus quadratiques :

	1	2	3	4	6	8	9	12	13	16	18	5	7	10	11	14	15	17	19	20	21	22
1	1	2	3	4	6	8	9	12	13	16	18	5	7	10	11	14	15	17	19	20	21	22
2	2	4	6	8	12	16	18	1	3	9	13	10	14	20	22	5	7	11	15	17	19	21
3	3	6	9	12	18	1	4	13	16	2	8	15	21	7	10	19	22	5	11	14	17	20
4	4	8	12	16	1	9	13	2	6	18	3	20	5	17	21	10	14	22	7	11	15	19
6	6	12	18	1	13	2	8	3	9	4	16	7	19	14	20	15	21	10	22	5	11	17
8	8	16	1	9	2	18	3	4	12	13	6	17	10	11	19	20	5	21	14	22	7	15
9	9	18	4	13	8	3	12	16	2	6	1	22	17	21	7	11	20	15	10	19	5	14
12	12	1	13	2	3	4	16	6	18	8	9	14	15	5	17	7	19	20	21	10	22	11
13	13	3	16	6	9	12	2	18	8	1	4	19	22	15	5	21	11	14	17	7	20	10
16	16	9	2	18	4	13	6	8	1	3	12	11	20	22	15	17	10	19	5	21	14	7
18	18	13	8	3	16	6	1	9	4	12	2	21	11	19	14	22	17	7	20	15	10	5
5	5	10	15	20	7	17	22	14	19	11	21	2	12	4	9	1	6	16	3	8	13	18
7	7	14	21	5	19	10	17	15	22	20	11	12	3	1	8	6	13	4	18	2	9	16
10	10	20	7	17	14	11	21	5	15	22	19	4	1	8	18	2	12	9	6	16	3	13
11	11	22	10	21	20	19	7	17	5	15	14	9	8	18	6	16	4	3	2	13	1	12
14	14	5	19	10	15	20	11	7	21	17	22	1	6	2	16	12	3	8	13	4	18	9
15	15	7	22	14	21	5	20	19	11	10	17	6	13	12	4	3	18	2	9	1	16	8
17	17	11	5	22	10	21	15	20	14	19	7	16	4	9	3	8	2	13	1	18	12	6
19	19	15	11	7	22	14	10	21	17	5	20	3	18	6	2	13	9	1	16	12	8	4
20	20	17	14	11	5	22	19	10	7	21	15	8	2	16	13	4	1	18	12	9	6	3
21	21	19	17	15	11	7	5	22	20	14	10	13	9	3	1	18	16	12	8	6	4	2
22	22	21	20	19	17	15	14	11	10	7	5	18	16	13	12	9	8	6	4	3	2	1

La table de multiplication de 49 qui ne symétrise pas les résidus qudratiques et les non-résidus quadratiques



De manière anecdotique, les éléments caractéristiques qui ont été identifiés permettraient de représenter un nombre premier p par $1+log_2\left(\frac{p-1}{2}\right)$ booléens, correspondant aux caractères de résiduosité quadratique des nombres de 1 à $\frac{p-1}{2}$ que l'on fait précéder d'un booléen qui exprime que le nombre p est de la forme $4k+1$ ou $4k+3$ (on code -1 par 0).

La loi de réciprocité quadratique facilite le calcul des relations qui lie deux nombres $((x\ R\ y)\ ou\ (x\ N\ y)$ d'une part et $((y\ R\ x)\ ou\ (y\ N\ x))$ d'autre part) : on a une relation symétrique $(x\ R\ y)\ et\ (y\ R\ x)$ dès que l'un des 2 nombres est de la forme $4k+1$, on a une relation anti-symétrique

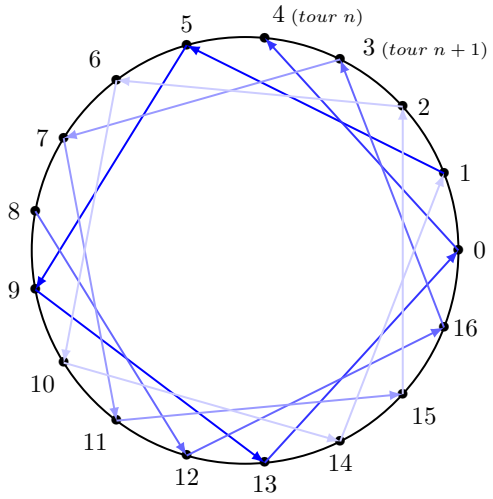
$$((x\ R\ y)\ et\ (y\ N\ x))\ ou\ exclusif\ ((xNy)\ et\ (y\ N\ x))$$

si les deux sont de la forme $4k+3$.

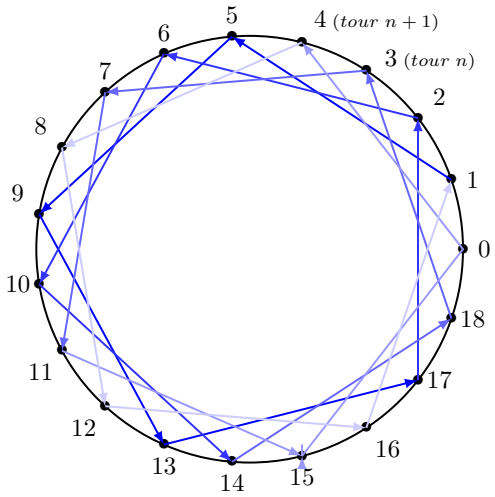
La notion d'orientation de chaînes de nombres fait toucher du doigt cette grande complexité de la loi de réciprocité quadratique : si l'on place les classes de restes sur un cercle et qu'on relie entre eux des

nombres espacés de 4, on voit que d'un tour à l'autre, les restes augmentent pour le module 17 de la forme $4k+1$ tandis qu'ils diminuent pour le module 19 de la forme $4k+3(=4k-1)$ (on indique cela en notant symboliquement les indices de deux tours successifs n et $n+1$ pour les restes 3 et 4 (pris au hasard) sur chaque cercle, en dégradant davantage le bleu à chaque tour - on voit que le dégradé décroît dans le sens anti-horaire pour le module 17 et dans le sens horaire pour 19, et en orientant les liens (correspondant à l'opération +4) par des flèches).

Cycle des restes des $4k+1$ *ou des* $4k+3$ *successifs modulo* $p=17$



Cycle des restes des $4k+1$ *ou des* $4k+3$ *successifs modulo* $p=19$



Rappelons d'une autre manière ce qui a été vu (et qui est connu depuis Gauss) : un nombre p est premier s'il partage l'ensemble des nombres de 1 à $p-1$ en deux ensembles que l'on peut mettre en bijection car ils sont de même cardinal. Ces deux ensembles sont l'ensemble des résidus quadratiques de p et l'ensemble des non-résidus quadratiques de p. Il y a exactement $\frac{p-1}{2}$ résidus et le même nombre de non-résidus lorsque p est premier.

Les résidus sont les $\frac{p-1}{2}$ solutions (notées par la variable x) de l'équation :

$$x^{\frac{p-1}{2}} - py - 1 = 0$$

avec x entier compris au sens large entre 1 et $p-1$, et y entier positif.

Les non-résidus sont les $\frac{p-1}{2}$ solutions de l'équation :

$$x^{\frac{p-1}{2}} - py + 1 = 0$$

dans les mêmes conditions.

On peut imaginer l'espace des nombres comme un polyèdre composé de multiples petites faces triangulaires, chacune autour d'un nombre et une petite boule à deux hémisphères, l'un noir (pour 1), l'autre blanc (pour -1), sur lesquels une fonction envoie les faces. Les faces correspondant aux nombres résidus quadratiques ont pour image 1, i.e. "s'envoient" sur l'hémisphère noir, tandis que celles qui correspondent aux non-résidus quadratiques s'envoient sur l'hémisphère blanc.

Prenons un exemple : les résidus quadratiques de 11 sont les entiers x compris entre 1 et 10 tels qu'il existe un y entier positif avec $x^5 - 11y - 1 = 0$. On a

$$\begin{aligned}
1^5 - 11 \times 0 - 1 &= 0 \\
3^5 - 11 \times 22 - 1 &= 0 \\
4^5 - 11 \times 93 - 1 &= 0 \\
5^5 - 11 \times 284 - 1 &= 0 \\
9^5 - 11 \times 5368 - 1 &= 0
\end{aligned}$$

donc 1, 3, 4, 5 et 9 sont résidus quadratiques de 11.

Les non-résidus quadratiques de 11 sont les entiers x compris entre 1 et 10 tels qu'il existe un y entier positif avec $\mathrm{x}^5 - 11y + 1 = 0$.

On a

$$\begin{aligned}
2^5 - 11 \times 3 + 1 &= 0 \\
6^5 - 11 \times 707 + 1 &= 0 \\
7^5 - 11 \times 1528 + 1 &= 0 \\
8^5 - 11 \times 2979 + 1 &= 0 \\
10^5 - 11 \times 9091 + 1 &= 0
\end{aligned}$$

donc 2, 6, 7, 8 et 10 sont non-résidus quadratiques de 11.

Aux nombres premiers de la forme $4k + 1$ (milieu pair, symétrie exacte des couleurs) correspondent des variétés de degré de plus en plus grand mais pair tandis qu'aux nombres premiers de la forme $4k + 3$ (milieu impair, nombres en bijection de couleurs inverse l'une de l'autre) correspondent des variétés de degré de plus en plus grand mais impair.

Sur les variétés correspondant aux nombres composés, il n'y a pas de symétrie ou anti-symétrie systématique entre les images par la fonction $x^{\frac{p-1}{2}}$ (qui vaut 1 ou -1) des points entiers résidu quadratique et non-résidu quadratique qui sont en bijection.

Annexe : Tables des résidus modulaires des puissances des nombres modulo 17, 19 et 15

mod 17	1	2	3	4	5	6	7	8
2	2	4	8	16	15	13	9	1
3	3	9	10	13	5	15	11	16
4	4	16	13	1	4	16	13	1
5	5	8	6	13	14	2	10	16
6	6	2	12	4	7	8	14	16
7	7	15	3	4	11	9	12	16
8	8	13	2	16	9	4	15	1
9	9	13	15	16	8	4	2	1
10	10	15	14	4	6	9	5	16
11	11	2	5	4	10	8	3	16
12	12	8	11	13	3	2	7	16
13	13	16	4	1	13	16	4	1
14	14	9	7	13	12	15	6	16
15	15	4	9	16	2	13	8	1
16	16	1	16	1	16	1	16	1

mod 19	1	2	3	4	5	6	7	8	9
2	2	4	8	16	13	7	14	9	18
3	3	9	8	5	15	7	2	6	18
4	4	16	7	9	17	11	6	5	1
5	5	6	11	17	9	7	16	4	1
6	6	17	7	4	5	11	9	16	1
7	7	11	1	7	11	1	7	11	1
8	8	7	18	11	12	1	8	7	18
9	9	5	7	6	16	11	4	17	1
10	10	5	12	6	3	11	15	17	18
11	11	7	1	11	7	1	11	7	1
12	12	11	18	7	8	1	12	11	18
13	13	17	12	4	14	11	10	16	18
14	14	6	8	17	10	7	3	4	18
15	15	16	12	9	2	11	13	5	18
16	16	9	11	5	4	7	17	6	1
17	17	4	11	16	6	7	5	9	1
18	18	1	18	1	18	1	18	1	18

mod 15	1	2	3	4	5	6	7
2	2	4	8	1	2	4	8
3	3	9	12	6	3	9	12
4	4	1	4	1	4	1	4
5	5	10	5	10	5	10	5
6	6	6	6	6	6	6	6
7	7	4	13	1	7	4	13
8	8	4	2	1	8	4	2
9	9	6	9	6	9	6	9
10	10	10	10	10	10	10	10
11	11	1	11	1	11	1	11
12	12	9	3	6	12	9	3
13	13	4	7	1	13	4	7
14	14	1	14	1	14	1	14

Espace (Denise Vella-Chemla, 19.10.2017)
On constate par programme que, si on note $\mathcal{P}$ l'ensemble des nombres premiers et $\pi(N)$ l'ensemble des nombres premiers inférieurs à N :

$$\sum_{p\in\mathcal{P},\ p\leqslant N} e^{\frac{2i\pi}{p}} \simeq \pi(N) + i\ ln(N)$$

On obtient par ce calcul une valeur de 78492 pour la partie réelle du membre gauche de l'égalité quand le nombre de nombres premiers inférieurs à 10^6 (le membre droit de l'égalité) est égal à 78498 (l'erreur est de $\frac{6}{10^6} = 0,000006$). Que la partie réelle du complexe obtenu vaille $\pi(N)$ est normal : les dénominateurs croissant, l'angle du complexe $e^{\frac{2i\pi}{p}}$ est de plus en plus minuscule et l'extrémité de l'angle sur le cercle unité se rapproche de plus en plus de 1. On aimerait comprendre pourquoi la partie imaginaire est égale au logarithme népérien.
On définit l'espace des matrices infinies diagonales de la forme :

$$\begin{pmatrix} exp(\frac{\mathbf{x1}.2i\pi}{2}) & 0 & 0 & 0 & \dots \\ 0 & exp(\frac{\mathbf{x2}.2i\pi}{3}) & 0 & 0 & \dots \\ 0 & 0 & exp(\frac{\mathbf{x3}.2i\pi}{5}) & 0 & \dots \\ 0 & 0 & 0 & exp(\frac{\mathbf{x4}.2i\pi}{7}) & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

A un nombre entier n quelconque est associée la matrice

$$\begin{pmatrix} exp(\frac{\mathbf{k1}.2i\pi}{2}) & 0 & 0 & 0 & \dots \\ 0 & exp(\frac{\mathbf{k2}.2i\pi}{3}) & 0 & 0 & \dots \\ 0 & 0 & exp(\frac{\mathbf{k3}.2i\pi}{5}) & 0 & \dots \\ 0 & 0 & 0 & exp(\frac{\mathbf{k4}.2i\pi}{7}) & \dots \\ \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

avec $n \equiv k_p$ dans le corps $\mathbb{Z}/p\mathbb{Z}$.
Par exemple, on associe à 11 (de restes (1,2,1,4,0,...) modulo (2,3,5,7,11,...)) la matrice :

$$\begin{pmatrix} exp(\frac{\mathbf{1}.2i\pi}{2}) & 0 & 0 & 0 & 0 & \dots \\ 0 & exp(\frac{\mathbf{2}.2i\pi}{3}) & 0 & 0 & 0 & \dots \\ 0 & 0 & exp(\frac{\mathbf{1}.2i\pi}{5}) & 0 & 0 & \dots \\ 0 & 0 & 0 & exp(\frac{\mathbf{4}.2i\pi}{7}) & 0 & \dots \\ 0 & 0 & 0 & 0 & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

Les nombres premiers n'ont qu'un seul 1 sur leur diagonale.

L'opérateur $Succ(n)$ de l'arithmétique de Peano (l'addition de 1 à n) correspond à la multiplication dans l'espace des matrices de la matrice associé à n par la matrice (que l'on appelle $PlusUn$) dont tous les k_i valent 1.

$$PlusUn = \begin{pmatrix} exp(\frac{2i\pi}{2}) & 0 & 0 & 0 & 0 & \dots \\ 0 & exp(\frac{2i\pi}{3}) & 0 & 0 & 0 & \dots \\ 0 & 0 & exp(\frac{2i\pi}{5}) & 0 & 0 & \dots \\ 0 & 0 & 0 & exp(\frac{2i\pi}{7}) & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

On calcule par programme les traces successives des portions finies hautes-gauches de la matrice carrée $PlusUn$; ce sont les sommes partielles successives des éléments diagonaux de $PlusUn$.
Pour les nombres premiers jusqu'à 97, cette somme est égale à $19.8703 + 6.46254i$.
Pour les nombres premiers inférieurs à 10^7, elle vaut $664577 + 8.73825i$.
A cause du Théorème des nombres premiers d'Hadamard et La Vallée-Poussin, on remplace chaque p dans les $e^{\frac{2i\pi}{p}}$ par $\frac{p}{ln\, p}$, on obtient $\sum_{p\in\mathcal{P},\, p\leqslant N} e^{\frac{2i\pi\ ln\ p}{p}}$ soit $\sum_{p\in\mathcal{P},\, p\leqslant N} \left(\left(e^{ln\ p}\right)^{\frac{2i\pi}{n}}\right)$ soit $\sum_{p\in\mathcal{P},\, p\leqslant N} n^{\frac{2i\pi}{n}} = \sum_{p\in\mathcal{P},\, p\leqslant N} \sqrt[n]{n^{2i\pi}}$. On vérifie par programme qu'on obtient sensiblement les mêmes valeurs que grâce à la formule précédente, avec le petit escalier de 1 en 1 à chaque nombre premier.
Pour le montrer, on reproduit simplement ici les lignes du début et les lignes de la fin de l'exécution du programme, jusqu'à 10^6, qui montre le logarithme en partie imaginaire.

$2 \to (-1, 1.22465e-16)$
$3 \to (-1.5, 0.866025)$
$5 \to (-1.19098, 1.81708)$
$7 \to (-0.567493, 2.59891)$
$11 \to (0.27376, 3.13955)$
$13 \to (1.15922, 3.60428)$
$17 \to (2.09169, 3.96552)$
$19 \to (3.03751, 4.29022)$
$23 \to (4.00042, 4.56002)$
$29 \to (4.97704, 4.77499)$
$31 \to (5.95657, 4.97628)$
$37 \to (6.94219, 5.14529)$
$41 \to (7.93047, 5.29793)$
$43 \to (8.91981, 5.44354)$
$47 \to (9.91089, 5.57682)$
$53 \to (10.9039, 5.6951)$
$59 \to (11.8982, 5.80139)$
$61 \to (12.8929, 5.90421)$
$67 \to (13.8885, 5.99785)$
$71 \to (14.8846, 6.08623)$
$73 \to (15.8809, 6.1722)$
$79 \to (16.8777, 6.25165)$
$83 \to (17.8749, 6.32728)$
$89 \to (18.8724, 6.39781)$
$97 \to (19.8703, 6.46254)$
$101 \to (20.8683, 6.52471)$
$103 \to (21.8665, 6.58568)$
. . . . . .

$$
\begin{aligned}
99563 &\rightarrow (78465.8, 13.2761)\\
999599 &\rightarrow (78466.8, 13.2761)\\
999611 &\rightarrow (78467.8, 13.2762)\\
999613 &\rightarrow (78468.8, 13.2762)\\
999623 &\rightarrow (78469.8, 13.2762)\\
999631 &\rightarrow (78470.8, 13.2762)\\
999653 &\rightarrow (78471.8, 13.2762)\\
999667 &\rightarrow (78472.8, 13.2762)\\
999671 &\rightarrow (78473.8, 13.2762)\\
999683 &\rightarrow (78474.8, 13.2762)\\
999721 &\rightarrow (78475.8, 13.2762)\\
999727 &\rightarrow (78476.8, 13.2762)\\
999749 &\rightarrow (78477.8, 13.2762)\\
999763 &\rightarrow (78478.8, 13.2762)\\
999769 &\rightarrow (78479.8, 13.2762)\\
999773 &\rightarrow (78480.8, 13.2762)\\
999809 &\rightarrow (78481.8, 13.2762)\\
999853 &\rightarrow (78482.8, 13.2762)\\
999863 &\rightarrow (78483.8, 13.2763)\\
999883 &\rightarrow (78484.8, 13.2763)\\
999907 &\rightarrow (78485.8, 13.2763)\\
999917 &\rightarrow (78486.8, 13.2763)\\
999931 &\rightarrow (78487.8, 13.2763)\\
999953 &\rightarrow (78488.8, 13.2763)\\
999959 &\rightarrow (78489.8, 13.2763)\\
999961 &\rightarrow (78490.8, 13.2763)\\
999979 &\rightarrow (78491.8, 13.2763)\\
999983 &\rightarrow (78492.8, 13.2763)
\end{aligned}
$$

Un internaute[1] du forum les-mathematiques.net m'a indiqué que la somme d'exponentielles $\sum_{p\in\mathcal{P},\ p\leqslant N} e^{\frac{2i\pi}{p}}$ avait pour partie imaginaire un nombre approximativement égal à $2\pi\ cos(1)ln(ln(N))$, on peut le vérifier par programme.

[1] bisam

Matrices pour la somme des diviseurs d'Euler, version simplifiée (Denise Vella-Chemla, 27.10.2017)

On souhaite "voir la primalité" en effectuant un calcul matriciel.

Appelons $M = (m_{ij})$ la matrice infinie d'entiers définie par $M_{ij} = j$ si $j \mid i$ et $M_{ij} = 0$ sinon.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & \dots \\ 1 & 2 & \boxed{3} & 0 & 0 & 6 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & \dots \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Appelons N une matrice infinie dont tous les éléments sont nuls sauf ceux de la première ligne qui valent tous 1.

$$N = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Appelons P une matrice colonne contenant les entiers successifs à partir de 1.

$$P = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ \vdots \end{pmatrix}$$

Alors $M^2N - P$ est une matrice colonne de nombres B_i telle que $B_i = 1$ si et seulement si i est premier et qui est strictement supérieur à 1 sinon (sauf $B_1 = 0$).
En effet, élever M au carré permet d'obtenir en première colonne le cumul (la somme) des diviseurs de

chaque entier.

$$M^2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & \dots \\ 1 & 2 & 3 & 0 & 0 & 6 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & \dots \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & \dots \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 5 & 0 & 0 & 0 & \dots \\ 1 & 2 & 3 & 0 & 0 & 6 & 0 & 0 & \dots \\ 1 & 0 & 0 & 0 & 0 & 0 & 7 & 0 & \dots \\ 1 & 2 & 0 & 4 & 0 & 0 & 0 & 8 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 3 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 4 & 0 & 9 & 0 & 0 & 0 & 0 & 0 & \dots \\ 7 & 12 & 0 & 16 & 0 & 0 & 0 & 0 & \dots \\ 6 & 0 & 0 & 0 & 25 & 0 & 0 & 0 & \dots \\ 12 & 16 & 27 & 0 & 0 & 36 & 0 & 0 & \dots \\ 8 & 0 & 0 & 0 & 0 & 0 & 49 & 0 & \dots \\ 15 & 28 & 0 & 48 & 0 & 0 & 0 & 64 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

Un nombre p étant premier si sa somme des diviseurs vaut $p+1$, la soustraction de la colonne d'entiers sucessifs de la première colonne de M^2, qui contient pour chaque entier la somme de ses diviseurs, permet d'obtenir 1 comme image des nombres premiers et d'eux seulement (un nombre composé (sauf 1) a une somme de diviseurs strictement supérieure à son successeur au sens de Peano).

$$M^2N - P = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 3 & 4 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 4 & 0 & 9 & 0 & 0 & 0 & 0 & 0 & \dots \\ 7 & 12 & 0 & 16 & 0 & 0 & 0 & 0 & \dots \\ 6 & 0 & 0 & 0 & 25 & 0 & 0 & 0 & \dots \\ 12 & 16 & 27 & 0 & 0 & 36 & 0 & 0 & \dots \\ 8 & 0 & 0 & 0 & 0 & 0 & 49 & 0 & \dots \\ 15 & 28 & 0 & 48 & 0 & 0 & 0 & 64 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} - \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ \vdots \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 4 \\ 7 \\ 6 \\ 12 \\ 8 \\ 15 \\ \vdots \end{pmatrix} - \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ \vdots \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 3 \\ 1 \\ 6 \\ 1 \\ 7 \\ \vdots \end{pmatrix}$$

Bibliographie

[1] L. Euler, *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs*, Bibliothèque impartiale 3, 1751, S. 10-31. In : Opera omnia (1) 2, Leipzig, Berlin 1915, S. 241-253 (E 175).

Spirale et ζ (suite) (Denise Vella-Chemla, 28.10.2017)

On étudie une spirale du plan cartésien dont les coordonnées des sommets sont définis par la suite :

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n \\ y_n \end{pmatrix} + \lambda_n \begin{pmatrix} cos\ \theta_n & -sin\ \theta_n \\ sin\ \theta_n & cos\ \theta_n \end{pmatrix} \begin{pmatrix} x_n - x_{n-1} \\ y_n - y_{n-1} \end{pmatrix}$$

$$= \begin{pmatrix} x_n + \lambda_n cos\ \theta_n x_n - \lambda_n cos\ \theta_n x_{n-1} - \lambda_n sin\ \theta_n y_n + \lambda_n sin\ \theta_n y_{n-1} \\ y_n + \lambda_n sin\ \theta_n x_n - \lambda_n sin\ \theta_n x_{n-1} + \lambda_n cos\ \theta_n y_n - \lambda_n cos\ \theta_n y_{n-1} \end{pmatrix}$$

On peut aussi écrire la suite des coordonnées en utilisant des vecteurs de $\mathbb{R}^4$ et une matrice 4×4 pour la transformation.

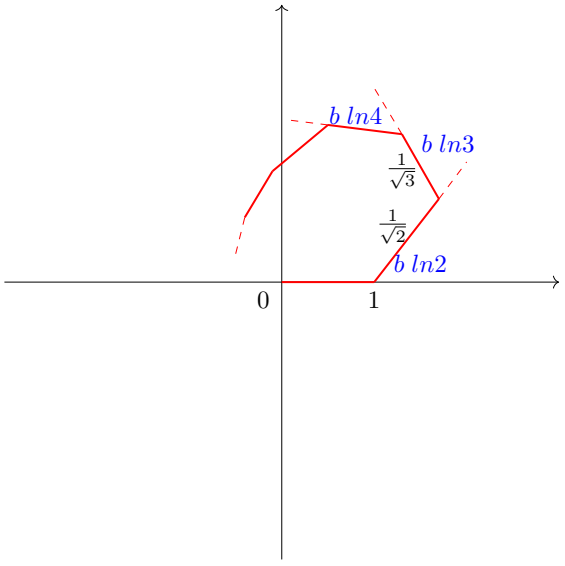
$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \\ x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 1 + \lambda_n cos\ \theta_n & -\lambda_n sin\ \theta_n & -\lambda_n cos\ \theta_n & \lambda_n sin\ \theta_n \\ \lambda_n sin\ \theta_n & 1 + \lambda_n cos\ \theta_n & -\lambda_n sin\ \theta_n & -\lambda_n cos\ \theta_n \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \\ x_{n-1} \\ y_{n-1} \end{pmatrix}$$

Les angles de rotation $\theta, \theta', \theta''$ qui séparent deux côtés successifs de la spirale sont tous différents : quand on écrit littéralement la somme $\zeta(s)$ avec $s = a + ib$, on obtient

$$1 + \left(\frac{1}{2}\right)^a e^{-ib\ ln\ 2} + \left(\frac{1}{3}\right)^a e^{-ib\ ln\ 3} + \left(\frac{1}{4}\right)^a e^{-ib\ ln\ 4} + \ldots$$

Les deux premiers points de la spirale sont $z = 0$ et $z = 1$.

Dans le cas où $a = \frac{1}{2}$, les côtés successifs de la spirale brisée ont pour longueur $\frac{1}{\sqrt{2}}$, $\frac{1}{\sqrt{3}}$, $\frac{1}{\sqrt{4}}$, ... (sur le dessin ci-dessous, on a bêtement mis les angles dans le sens anti-horaire, ça correspond à des $+ib\ldots$ comme puissances des e dans la formule ci-dessus plutôt que des $-ib$, c'est sans importance car l'axe des abcissses est axe de symétrie de ζ). Les λ_n (coefficients réducteurs pour passer de la longueur d'un côté à la longueur du côté suivant de la spirale) sont de la forme $\frac{\sqrt{n}}{\sqrt{n+1}}$.



Au départ, on était plutôt parti sur une décomposition en trois opérations successives, une translation, une homothétie puis une rotation codées par les matrices de transformation ci-dessous.

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 2 & 0 \\ 0 & -1 & 0 & 2 \end{pmatrix} \begin{pmatrix} x \\ y_n \\ x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_{n+1} \\ y_{n+1} \\ 2x_{n+1} - x_n \\ 2y_{n+1} - y_n \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ (1-\lambda_n) & 0 & \lambda_n & 0 \\ 0 & (1-\lambda_n) & 0 & \lambda_n \end{pmatrix} \begin{pmatrix} x \\ y_n \\ x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n \\ y_n \\ x_n + \lambda_n x_{n+1} - \lambda_n x_n \\ y_n + \lambda_n y_{n+1} - \lambda_n y_n \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\theta & -\sin\theta \\ 0 & 0 & \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y_n \\ x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} x_n \\ y_n \\ \cos\theta\, x_{n+1} - \sin\theta\, y_{n+1} \\ \sin\theta\, x_{n+1} + \cos\theta\, y_{n+1} \end{pmatrix}$$

Refaire ses gammes (Denise Vella-Chemla, 7.6.2017)

On va étudier les fréquences des notes de la gamme, suite au visionnage de la petite video Science étonnante #41 intitulée *Les mathématiques de la musique* qui se trouve ici https://www.youtube.com/watch?v=cTYvCpLRwao.

David Louapre explique dans cette video pourquoi il y a 12 notes dans la gamme chromatique et pourquoi certaines notes s'accordent bien (les écouter jouées ensemble est agréable à l'oreille).

On retiendra en résumant que la raison essentielle à cela est que $2^{19} = 524288 \simeq 3^{12} = 531441$ et qu'il s'agit d'écarter les notes entre elles en "mettant en face" 12 facteurs 2 ou 4 et 12 facteurs 3, ce qu'on fait en utilisant pour passer d'une note à la suivante immédiate les fractions rationnelles $\left\{\frac{3}{2}, \frac{3}{4}, \frac{3}{4}, \frac{3}{2}, \frac{3}{4}, \frac{3}{2}, \frac{3}{4}, \frac{3}{4}, \frac{3}{2}, \frac{3}{4}, \frac{3}{4}, \frac{3}{2}\right\}$ en partant initialement d'une note *La*.

L'ensemble des dénominateurs comprend 19 facteurs 2, et l'ensemble des numérateurs comprend 12 facteurs 3 et les fractions rationnelles $\frac{3}{2}$ sont équitablement réparties au sein de l'ensemble des fractions $\frac{3}{4}$ plus nombreuses.

Le tableau ci-dessous est celui fourni dans la video : on passe d'une note (de sa fréquence) à celle de la note à sa droite en "passant à la quinte", en multipliant la fréquence par $\frac{3}{2}$ ou par $\frac{3}{4}$ (on a mis le multiplicateur qui permet de passer des nombres d'une colonne à ceux de la suivante en bas de cette colonne) ; on passe d'une note à celle au-dessous dans la même colonne en "passant à l'octave" (en multipliant la fréquence par 2).

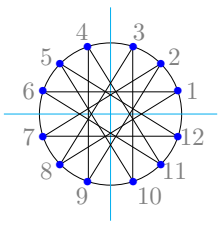
La	*Mi*	*Si*	*Fa#*	*Do#*	*Sol#*	*Ré#*	*La#*	*Fa*	*Do*	*Sol*	*Ré*	~~*La*~~
55	83	62	46	70	52	78	59	44	66	50	37	~~56~~
110	165	124	93	139	104	157	117	88	132	99	74	~~112~~
220	330	248	186	278	209	313	235	176	264	198	149	~~223~~
440	660	495	371	557	418	626	470	352	529	396	297	~~446~~
880	1320	990	743	1114	835	1253	940	705	1057	793	595	~~892~~
1760	2640	1980	1485	2228	1671	2506	1879	1410	2114	1586	1189	~~1784~~
3520	5280	3960	2970	4455	3341	5012	3759	2819	4229	3172	2379	~~3568~~
$\times\frac{3}{2}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{2}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{2}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{2}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{4}\nearrow$	$\times\frac{3}{2}\nearrow$	
8	3	10	5	12	7	2	9	4	11	6	1	

Permutons maintenant les colonnes de ce tableau de façon à remettre les notes dans l'ordre habituel d'une gamme ascendante. On passe cette fois-ci de chaque fréquence à la suivante selon l'ordre habituel de lecture (de gauche à droite et de haut en bas) en multipliant cette fréquence par $\sqrt[12]{2} \simeq 1.059463\ldots$.

1	2	3	4	5	6	7	8	9	10	11	12	
Ré	*Ré#*	*Mi*	*Fa*	*Fa#*	*Sol*	*Sol#*	*La*	*La#*	*Si*	*Do*	*Do#*	
74	78	83	88	93	99	104	110	117	124	132	139	+4→+7
149	157	165	176	186	198	209	220	235	248	264	278	+8→+14
297	313	330	352	371	396	418	440	470	495	529	557	+16→+28
595	626	660	705	743	793	835	880	940	990	1057	1114	+31→+57
1189	1253	1320	1410	1485	1586	1671	1760	1879	1980	2114	2228	+64→+114
2379	2506	2640	2819	2970	3172	3341	3520	3759	3960	4229	4455	+127→+226
4758	5012	5280	5638	5940	6344	6682	7040	7518	7920	8458	8910	+254→+452

On peut calculer approximativement par ligne les additions à effectuer pour passer d'une note à la suivante. On les a notées en fin de lignes en gris, de la plus petite somme à effectuer à la plus grande.

On peut enfin en ayant numéroté les colonnes de 1 à 12, noter ces nombres sur un cercle pour bien montrer la cyclicité et relier les notes successives par "passage à la quinte" (on a reporté ces nombres dans la dernière ligne du premier tableau également). Du fait de la cyclicité, ce dessin possède de multiples symétries.



Ce qu'il semble intéressant de faire, c'est de prolonger notre tableau de fréquences vers le domaine de l'inaudible, en réappliquant vers le haut du tableau les divisions par 2 des nombres des colonnes : moyennant le passage du discret au continu, on a un rapprochement des valeurs qu'il faut garder à l'esprit, en se rappelant cependant que toutes les fréquences fournies dans les 2 tableaux sont des valeurs entières arrondies les plus proches de réels.

Ré	*Ré#*	*Mi*	*Fa*	*Fa#*	*Sol*	*Sol#*	*La*	*La#*	*Si*	*Do*	*Do#*
1	1	1	1	1	2	2	2	2	2	2	2
2	2	3	3	3	3	3	3	4	4	4	4
5	5	5	6	6	6	7	7	7	8	8	9
9	10	10	11	12	12	13	14	15	16	17	18
19	20	21	22	23	25	26	28	29	31	33	35
37	39	42	44	47	50	52	55	59	62	66	70
74	78	83	88	93	99	104	110	117	124	132	139

On pourrait de la même manière fabriquer une gamme à 3 notes : on utilise le fait que $2^7 = 128 \simeq 5^3 = 125$. On doit mettre 7 facteurs 2 en face de 3 facteurs 5. On utilise les 3 fractions rationnelles $\left\{\frac{5}{4}, \frac{5}{8}, \frac{5}{4}\right\}$.

Admettons qu'on parte du nombre 500. Multiplié par $\frac{5}{4}$, on obtient 625, qu'on multiplie par $\frac{5}{8}$ pour obtenir 391, qu'on multiplie quant à lui par $\frac{5}{4}$ pour obtenir 489. On est quasiment revenu au chiffre initial 500.

On remet les nombres dans l'ordre $391 \to 489 \to 500 \to 625$. On doit passer de l'un à l'autre par multiplication par $\sqrt[3]{2} \simeq 1.025992\ldots$ (la suite obtenue est $391, 493, 621$. Il manque un nombre de la séquence, le 500 qui a disparu...?).

On a également $7^5 \simeq 2^{14} \simeq 11^4$ et $13^4 \simeq 2^{15}$ mais les écarts sont de plus en plus grands : $2^{14} = 16384$, $7^5 = 16807$, $11^4 = 14641$ d'une part, et $2^{15} = 32768$ et $13^4 = 28561$ d'autre part, "presque" égaux.

$\sqrt[4]{2} \simeq 1.18921\ldots$
$\sqrt[14]{11} \simeq 1.18682\ldots$
$\sqrt[15]{13} \simeq 1.18649\ldots$

$\sqrt[5]{2} \simeq 1.1487\ldots$
$\sqrt[14]{7} \simeq 1.14912\ldots$

Ci-dessous, un programme pour convertir les fréquences des notes de la gamme en fixant l'origine 0 pour la plus petite fréquence (32.7) trouvée dans un tableau sur la toile (cf. code) en nombres espacés de 1. Pour convertir une fréquence, on soustrait ln(32.7) à son logarithme népérien, on divise par ln(2) et on multiplie par 12.

```
\end{document}
#include <iostream>
#include <stdio.h>
#include <cmath>
#include <math.h>
#include <string>

float convertis(float x, float y) {
  float calcul ;

  calcul = (12*(log(y)-log(x)))/log(2) ;
  return calcul ;
}

int main (int argc, char* argv[]) {
  float freq[13][10] ;
  float freq2[13][10] ;
  float freq3[13][10] ;
  std::string trad[13] ;
  int i, j ;
  float rac12emede2=1.059463 ;
  float prems, convprems, calcul ;

  freq[1][0] = 32.7 ; // do
  freq[2][0] = 34.7 ; // do dièse
  freq[3][0] = 36.7 ; // ré
  freq[4][0] = 38.9 ; // ré dièse
  freq[5][0] = 41.2 ; // mi
  freq[6][0] = 43.7 ; // fa
  freq[7][0] = 46.3 ; // fa dièse
  freq[8][0] = 49.0 ; // sol
  freq[9][0] = 51.9; // sol dièse
  freq[10][0] = 55.0; // la
  freq[11][0] = 58.3 ; // la dièse
  freq[12][0] = 61.7 ; // si

  freq[1][1] = 65.4 ; // do
  freq[2][1] = 69.3 ; // do dièse
  freq[3][1] = 73.4 ; // ré
  freq[4][1] = 77.8 ; // ré dièse
  freq[5][1] = 82.4 ; // mi
  freq[6][1] = 87.3 ; // fa
  freq[7][1] = 92.5 ; // fa dièse
  freq[8][1] = 98.0 ; // sol
  freq[9][1] = 103.8 ; // sol dièse
  freq[10][1] = 110.0 ; // la
  freq[11][1] = 116.5 ; // la dièse
  freq[12][1] = 123.5 ; // si

  freq[1][2] = 130.8 ; // do
  freq[2][2] = 138.6 ; // do dièse
  freq[3][2] = 146.8 ; // ré
  freq[4][2] = 155.6 ; // ré dièse
  freq[5][2] = 164.8 ; // mi
  freq[6][2] = 174.6 ; // fa
  freq[7][2] = 185.0 ; // fa dièse
  freq[8][2] = 196.0 ; // sol
  freq[9][2] = 207.7 ; // sol dièse
  freq[10][2] = 220.0 ; // la
  freq[11][2] = 233.1 ; // la dièse
  freq[12][2] = 246.9 ; // si
```

```
freq[1][3] = 261.6 ; // do
freq[2][3] = 277.2 ; // do dièse
freq[3][3] = 293.7 ; // ré
freq[4][3] = 311.1 ; // ré dièse
freq[5][3] = 329.6 ; // mi
freq[6][3] = 349.2 ; // fa
freq[7][3] = 370.0 ; // fa dièse
freq[8][3] = 392.0 ; // sol
freq[9][3] = 415.3 ; // sol dièse
freq[10][3] = 440.0 ; // la
freq[11][3] = 466.2 ; // la dièse
freq[12][3] = 493.9 ; // si

freq[1][4] = 523.3 ; // do
freq[2][4] = 554.4 ; // do dièse
freq[3][4] = 587.3 ; // ré
freq[4][4] = 622.3 ; // ré dièse
freq[5][4] = 659.3 ; // mi
freq[6][4] = 698.5 ; // fa
freq[7][4] = 740.0 ; // fa dièse
freq[8][4] = 784.0 ; // sol
freq[9][4] = 830.6 ; // sol dièse
freq[10][4] = 880.0 ; // la
freq[11][4] = 932.3 ; // la dièse
freq[12][4] = 987.8 ; // si

freq[1][5] = 1046.5 ; // do
freq[2][5] = 1108.7 ; // do dièse
freq[3][5] = 1174.7 ; // ré
freq[4][5] = 1244.5 ; // ré dièse
freq[5][5] = 1318.5 ; // mi
freq[6][5] = 1396.9 ; // fa
freq[7][5] = 1480.0 ; // fa dièse
freq[8][5] = 1568.0 ; // sol
freq[9][5] = 1661.2 ; // sol dièse
freq[10][5] = 1760.0 ; // la
freq[11][5] = 1864.7 ; // la dièse
freq[12][5] = 1975.5 ; // si

freq[1][6] = 2093.0 ; // do
freq[2][6] = 2217.5 ; // do dièse
freq[3][6] = 2349.3 ; // ré
freq[4][6] = 2489.0 ; // ré dièse
freq[5][6] = 2637.0 ; // mi
freq[6][6] = 2793.8 ; // fa
freq[7][6] = 2960.0 ; // fa dièse
freq[8][6] = 3136.0 ; // sol
freq[9][6] = 3322.4 ; // sol dièse
freq[10][6] = 3520.0 ; // la
freq[11][6] = 3729.3 ; // la dièse
freq[12][6] = 3951.1 ; // si

freq[1][7] = 4186.0 ; // do
freq[2][7] = 4434.9 ; // do dièse
freq[3][7] = 4698.6 ; // ré
freq[4][7] = 4978.0 ; // ré dièse
freq[5][7] = 5274.0 ; // mi
freq[6][7] = 5587.7 ; // fa
freq[7][7] = 5919.9 ; // fa dièse
freq[8][7] = 6271.9 ; // sol
freq[9][7] = 6644.9 ; // sol dièse
freq[10][7] = 7040.0 ; // la
freq[11][7] = 7458.6 ; // la dièse
freq[12][7] = 7902.1 ; // si
```

```
freq[1][8] = 8372.0 ; // do
freq[2][8] = 8869.8 ; // do dièse
freq[3][8] = 9397.3 ; // ré
freq[4][8] = 9956.1 ; // ré dièse
freq[5][8] = 10548.1 ; // mi
freq[6][8] = 11175.3 ; // fa
freq[7][8] = 11839.8 ; // fa dièse
freq[8][8] = 12543.9 ; // sol
freq[9][8] = 13289.8 ; // sol dièse
freq[10][8] = 14080.0 ; // la
freq[11][8] = 14917.2 ; // la dièse
freq[12][8] = 15804.3 ; // si


trad[1] = "do " ;
trad[2] = "do# " ;
trad[3] = "re " ;
trad[4] = "re# " ;
trad[5] = "mi " ;
trad[6] = "fa " ;
trad[7] = "sol " ;
trad[8] = "sol#" ;
trad[9] = "la " ;
trad[10] = "la# " ;
trad[11] = "si " ;
trad[12] = "do " ;

std::cout << "     " ;
for (i = 1 ; i <= 12 ; ++i)
  std::cout << trad[i] << "   " ;
std::cout << "\n" ;

for (j = 0 ; j <= 8 ; ++j)
  {
    for (i = 1 ; i <= 12 ; ++i)
      printf("%10.3f", freq[i][j]) ;
    std::cout << "\n" ;
  }
std::cout << "\n" ;
prems = 32.7 ;
convprems = 0.0 ;
for (j = 0 ; j <= 8 ; ++j)
  {
    for (i = 1 ; i <= 12 ; ++i)
      {
        freq2[i][j] = prems ;
        printf("%10.3f", freq2[i][j]) ;
        prems = prems * rac12emede2 ;
        //convprems = convprems+0.5 ;
        freq3[i][j] = convprems ;
        convprems = convprems+1.0 ;
      }
    std::cout << "\n" ;
  }
std::cout << "\n" ;
//for (j = 0 ; j <= 8 ; ++j)
// {
//   for (i = 1 ; i <= 12 ; ++i)
//    printf("%10.3f", freq3[i][j]) ;
//   std::cout << "\n" ;
// }
```

```
  calcul = (12*(log(1479.826)-log(32.7)))/log(2) ;
  std::cout << calcul << "\n" ;

  for (j = 0 ; j <= 8 ; ++j)
    {
      for (i = 1 ; i <= 12 ; ++i)
        {
          calcul = convertis(32.7, freq2[i][j]) ;
          printf("%9.3f",calcul) ;
        }
      std::cout << "\n" ;
    }
}
```

Résultat de l'exécution

```
      do       do#      re       re#      mi       fa       fa#       sol      sol#     la       la#
         si
   32.700   34.700   36.700   38.900   41.200   43.700   46.300   49.000   51.900   55.000   58.300
       61.700
   65.400   69.300   73.400   77.800   82.400   87.300   92.500   98.000  103.800  110.000  116.500
      123.500
  130.800  138.600  146.800  155.600  164.800  174.600  185.000  196.000  207.700  220.000  233.100
      246.900
  261.600  277.200  293.700  311.100  329.600  349.200  370.000  392.000  415.300  440.000  466.200
      493.900
  523.300  554.400  587.300  622.300  659.300  698.500  740.000  784.000  830.600  880.000  932.300
      987.800
 1046.500 1108.700 1174.700 1244.500 1318.500 1396.900 1480.000 1568.000 1661.200 1760.000 1864.700
     1975.500
 2093.000 2217.500 2349.300 2489.000 2637.000 2793.800 2960.000 3136.000 3322.400 3520.000 3729.300
     3951.100
 4186.000 4434.900 4698.600 4978.000 5274.000 5587.700 5919.900 6271.900 6644.900 7040.000 7458.600
     7902.100
 8372.000 8869.800 9397.300 9956.100 10548.100 11175.300 11839.800 12543.900 13289.800 14080.000
     14917.200 15804.300

   32.700   34.644   36.705   38.887   41.199   43.649   46.245   48.995   51.908   54.995   58.265
       61.729
   65.400   69.289   73.409   77.774   82.399   87.298   92.489   97.989  103.816  109.989  116.529
      123.459
  130.800  138.578  146.818  155.548  164.797  174.597  184.979  195.978  207.632  219.978  233.059
      246.917
  261.599  277.155  293.635  311.096  329.594  349.193  369.957  391.956  415.263  439.956  466.117
      493.833
  523.198  554.309  587.270  622.191  659.188  698.386  739.914  783.911  830.525  879.911  932.233
      987.666
 1046.396 1108.617 1174.539 1244.381 1318.375 1396.770 1479.826 1567.821 1661.049 1759.820 1864.464
     1975.331
 2092.790 2217.233 2349.077 2488.760 2636.749 2793.538 2959.651 3135.640 3322.095 3519.637 3728.925
     3950.658
 4185.576 4434.463 4698.150 4977.516 5273.494 5587.072 5919.296 6271.276 6644.185 7039.269 7457.845
     7901.311
 8371.146 8868.920 9396.293 9955.025 10546.981 11174.137 11838.585 12542.543 13288.360 14078.526
     14915.678 15802.609

 65.9999
```

```
  0.000   1.000   2.000   3.000   4.000   5.000   6.000   7.000   8.000   9.000  10.000  11.000
 12.000  13.000  14.000  15.000  16.000  17.000  18.000  19.000  20.000  21.000  22.000  23.000
 24.000  25.000  26.000  27.000  28.000  29.000  30.000  31.000  32.000  33.000  34.000  35.000
 36.000  37.000  38.000  39.000  40.000  41.000  42.000  43.000  44.000  45.000  46.000  47.000
 48.000  49.000  50.000  51.000  52.000  53.000  54.000  55.000  56.000  57.000  58.000  59.000
 60.000  61.000  62.000  63.000  64.000  65.000  66.000  67.000  68.000  69.000  70.000  71.000
 72.000  73.000  74.000  75.000  76.000  77.000  78.000  79.000  80.000  81.000  82.000  83.000
 84.000  85.000  86.000  87.000  88.000  89.000  90.000  91.000  92.000  93.000  94.000  95.000
 96.000  97.000  98.000  99.000 100.000 101.000 102.000 103.000 104.000 105.000 106.000 107.000
```

On a ainsi trouvé une fonction qui, grosso-modo, convertit les notes de la gamme tempérée en la suite des entiers (c'est la fonction $f(y) = 12 \times (ln(y) - ln(32.7))/ln(2)$ qui est codée par la fonction $convertis(x, y)$ dans le programme ci-dessus).

On découvre, et c'est surprenant, qu'en calculant les rapports des carrés des parties imaginaires des premiers zéros de ζ, on aboutit aussi à une séquence d'entiers qui ressemble à la suite des entiers successifs, du moins au tout début.

```
zeros[1] = 14.1347
zeros[2]^2/zeros[1]^2 -> 2.21195
zeros[3]^2/zeros[1]^2 -> 3.131
zeros[4]^2/zeros[1]^2 -> 4.63322
zeros[5]^2/zeros[1]^2 -> 5.42928
zeros[6]^2/zeros[1]^2 -> 7.07101
zeros[7]^2/zeros[1]^2 -> 8.38049
zeros[8]^2/zeros[1]^2 -> 9.39602
zeros[9]^2/zeros[1]^2 -> 11.5346
zeros[10]^2/zeros[1]^2 -> 12.4002
zeros[11]^2/zeros[1]^2 -> 14.044
zeros[12]^2/zeros[1]^2 -> 15.9476
zeros[13]^2/zeros[1]^2 -> 17.6288
zeros[14]^2/zeros[1]^2 -> 18.5219
zeros[15]^2/zeros[1]^2 -> 21.2205
zeros[16]^2/zeros[1]^2 -> 22.5221
zeros[17]^2/zeros[1]^2 -> 24.2089
zeros[18]^2/zeros[1]^2 -> 25.9956
zeros[19]^2/zeros[1]^2 -> 28.6861
zeros[20]^2/zeros[1]^2 -> 29.7878
zeros[21]^2/zeros[1]^2 -> 31.5051
zeros[22]^2/zeros[1]^2 -> 34.4067
zeros[23]^2/zeros[1]^2 -> 35.9382
zeros[24]^2/zeros[1]^2 -> 38.256
zeros[25]^2/zeros[1]^2 -> 39.4767
zeros[26]^2/zeros[1]^2 -> 39.4767
```

Nombre de solutions de l'équation $xy = -1$ dans les corps premiers (Denise Vella-Chemla, 31.10.2017)

On réalise par programme que dans un corps premier $\mathbb{Z}/p\mathbb{Z}$, le nombre de couples (x, y) solutions de l'équation $xy = -1\ (mod\ p)$ avec x différent de y est égal à $\frac{p-1}{2}$ si p est de la forme $4k+3$ et à $\frac{p-3}{2}$ si p est de la forme $4k+1$; dans ce second cas, deux nombres sont racines de -1.

Donnons deux exemples :

- pour $p = 13$ de la forme $4k+1$, les couples dont le produit est égal à -1 sont les couples

  $$(1, 12), (2, 6), (3, 4), (7, 11), (9, 10)$$

  et les racines carrées de -1 sont 5 et 8.

  Il y a bien 5 couples de nombres différents avec $5 = \frac{13-3}{2}$;

- pour $p = 19$ de la forme $4k+3$, les couples dont le produit est égal à -1 sont les couples

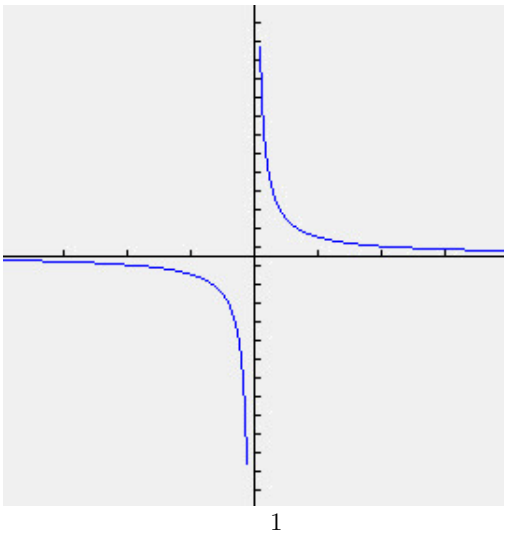
  $$(1, 18), (2, 9), (3, 6), (4, 14), (5, 15), (7, 8), (10, 17), (11, 12), (13, 16).$$

  Il y a bien 9 couples de nombres différents avec $9 = \frac{19-1}{2}$.

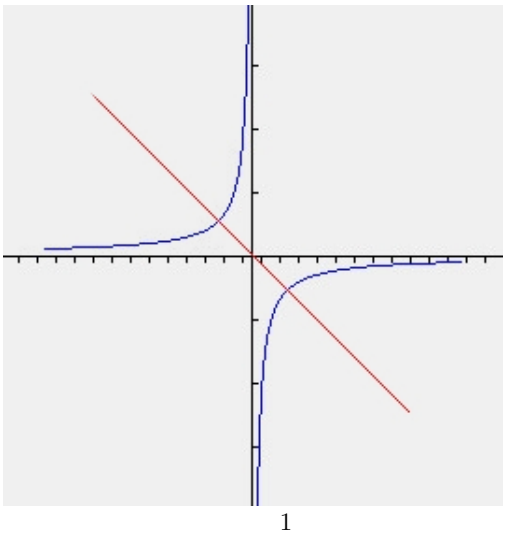
Il est plus simple pour les premiers de la forme $p = 4k+1$ de compter les couples (x, x) avec les autres et de voir les $4k+3$ comme des $4k-1$, cela permet d'unifier les deux cas de la façon suivante : pour les nombres premiers et eux seulement de la forme $4k+1$, il y a $2k+1$ couples (x, y) solutions à l'équation $xy = -1$ tandis que pour les nombres premiers de la forme $4k-1$, il y a $2k-1$ couples (x, y) solutions à cette équation.

(On a bien pour $13 = 4 \times 3 + 1$ un nombre de 7 couples avec $7 = 2 \times 3 + 1$ et pour $19 = 4 \times 5 - 1$ un nombre de 9 couples avec $9 = 2 \times 5 - 1$).

L'équation $xy = -1$, dans le plan cartésien habituel, est l'équation d'une hyperbole toute semblable à l'hyperbole $y = \frac{1}{x}$, cette dernière se trouvant être l'inverse du logarithme. Elle est simplement dans les deuxième et quatrième quadrants du plan cartésien (alors que la courbe de l'inverse du logarithme est dans les premier et troisième quadrants). On peut l'obtenir à partir de l'hyperbole inverse du logarithme par une symétrie verticale, ou bien par une symétrie horizontale, ou bien par une rotation d'un quart ou de trois quarts de tours. Ces deux courbes ont toutes deux deux axes de symétrie et elles sont invariantes par une rotation d'un demi-tour.



$y = \frac{1}{x}$



$y = -\frac{1}{x}$

Causer ou ne pas causer (Denise Vella-Chemla, 5.11.2017)

Du fait de recherches récentes sur les nombres de résidus quadratiques ou de racines de -1, on voudrait fournir ici un tableau qui présente certains éléments qui amènent à rappeler des caractérisations des nombres premiers et de certaines de leurs puissances.

La colonne B contient un $+$ si n est de la forme $4k+1$ et un $-$ si n est de la forme $4k-1$. La colonne $2k \pm 1$ contient $2k+1$ si n est de la forme $4k+1$ et $2k-1$ si n est de la forme $4k-1$. La colonne $nbRQ$ contient le nombre de résidus quadratiques de n, marqué d'une étoile lorsqu'il est pair, et la colonne $Nb\sqrt{-1}$ contient le nombre de racines de -1 lorsqu'il n'est pas nul. La colonne P contient une croix si n est premier.

n	B	$2k \pm 1$	$NbRQ$	$Nb\sqrt{-1}$	P	n	B	$2k \pm 1$	$NbRQ$	$Nb\sqrt{-1}$	P	n	B	$2k \pm 1$	$NbRQ$	$Nb\sqrt{-1}$	P
1	+	1	0 ⋆			34			17	2		67	−	33	33		×
2			1	1	×	35	−	17	11			68			17		
3	−	1	1		×	36			7			69	+	35	23		
4			1			37	+	19	18 ⋆	2	×	70			23		
5	+	3	2 ⋆	2	×	38			19			71	−	35	35		×
6			3			39	−	19	13			72			11		
7	−	3	3		×	40			8 ⋆			73	+	37	36 ⋆	2	×
8			2 ⋆			41	+	21	20 ⋆	2	×	74			37	2	
9	+	5	3			42			15			75	−	37	21		
10			5	2		43	−	21	21		×	76			19		
11	−	5	5		×	44			11			77	+	39	23		
12			3			45	+	23	11			78			27		
13	+	7	6 ⋆	2	×	46			23			79	−	39	39		×
14			7			47	−	23	23		×	80			11		
15	−	7	5			48			7			81	+	41	30 ⋆		
16			3			49	+	25	21			82			41	2	
17	+	9	8 ⋆	2	×	50			21	2		83	−	41	41		×
18			7			51	−	25	17			84			15		
19	−	9	9		×	52			13			85	+	43	26 ⋆	4	
20			5			53	+	27	26 ⋆	2	×	86			43		
21	+	11	7			54			21			87	−	43	29		
22			11			55	−	27	17			88			17		
23	−	11	11		×	56			11			89	+	45	44 ⋆	2	×
24			5			57	+	29	19			90			23		
25	+	13	10 ⋆	2		58			29	2		91	−	45	27		
26			13			59	−	29	29		×	92			23		
27	−	13	10 ⋆			60			11	2		93	+	47	31		
28			7			61	+	31	30 ⋆	2	×	94			47		
29	+	15	14 ⋆	2	×	62			31			95	−	47	29		
30			11			63	−	31	15			96			13		
31	−	15	15		×	64			11			97	+	49	48 ⋆	2	×
32			6 ⋆			65	+	33	20 ⋆	4		98			43		
33	+	17	11			66			23			99	−	49	23		
												100			21		

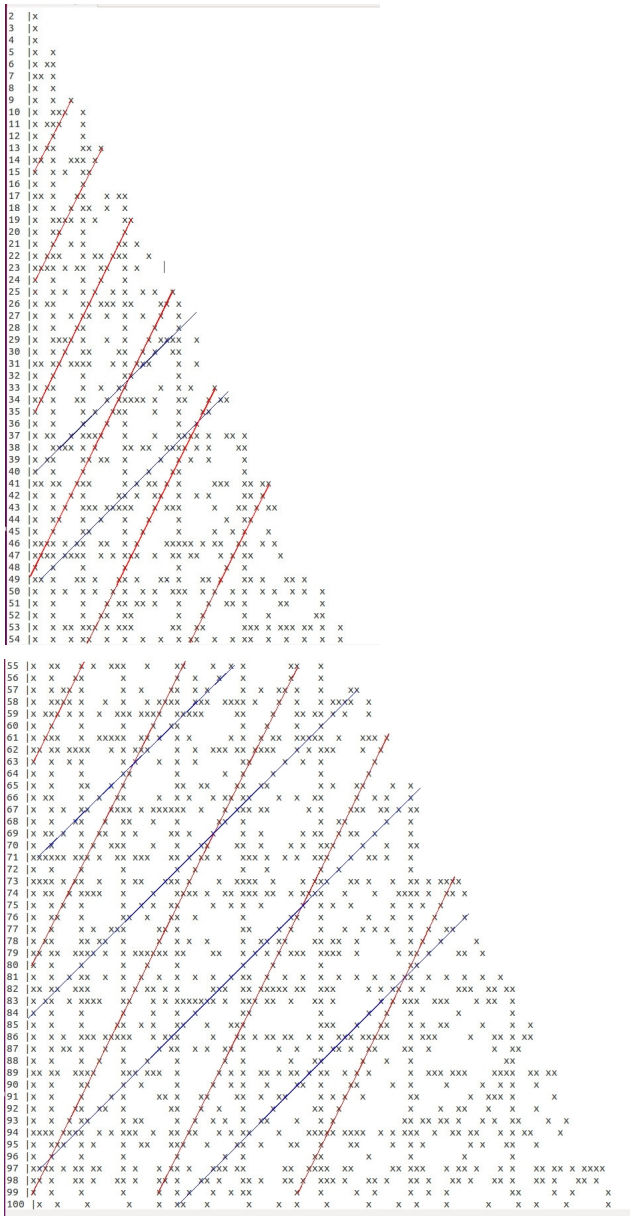
Les nombres premiers de la forme $4k+1$ sont caractérisés par un nombre de résidus quadratiques pair et le fait d'avoir exactement deux racines de -1. On peut obtenir une autre caractérisation en remplaçant la parité du nombre de résidus quadratiques par la parité de $(n-1)/2$.

Mais les puissances des nombres premiers $4k+1$ vérifient eux-aussi ces contraintes : on teste par programme jusqu'à 10^5 et c'est sympathique de retrouver les puissances de nombres premiers suivantes indirectement : $9409 = 97^2, 7921 = 89^2, 5329 = 73^2, 4913 = 17^3, 3721 = 61^2, 3125 = 5^5, 2809 = 53^2, 2197 = 13^3, 1681 = 41^2, 1369 = 37^2, 841 = 29^2, 625 = 5^4, 289 = 17^2, 169 = 13^2, 125 = 5^3$ et $25 = 5^2$).

Les nombres premiers de la forme $4k-1$ sont caractérisés par le fait que leur nombre de résidus quadratiques est égal à $2k-1$.

Suites de relations "est résidu quadratique de" en miroir (Denise Vella-Chemla, 31.10.2017)

Les deux graphiques ci-dessous rappellent le contenu de la table de l'annexe des Recherches arithmétiques de Gauss[1] et fournissent pour un nombre ses résidus quadratiques (compter une croix par colonne, la première correspondant à 1).



Le trait rouge qui démarre à la croix $(48, 1)$ correspond aux équation de la forme $7^2 - a - b = 0$ avec $a + b = 49$. On a de la même manière un trait rouge qui débute à chaque croix $(x^2 - 1, 1)$. Si on note[2] R la relation *"est un résidu quadratique de"*, les traits rouges correspondent à l'équivalence $b\ R\ a \iff (b + i)\ R\ (a - i)$.

Les traits bleus identiquement correspondent au fait qu'un certain nombre d'équations quadratiques sont simultanément vérifiées (il s'agit, comme pour ce que nous avons proposé au sujet de la conjecture de Goldbach, de lier entre elles deux assertions logiques, l'une correspondant au fait qu'une équation soit ou non vérifiée par les coordonnées d'un point, et l'autre correspondant au fait qu'*une autre équation* soit ou non vérifiée par *un autre point*. Prenons par exemple la ligne reliant les points $(71, 2)$, $(70, 4)$, $(69, 6)$, $(68, 8), \ldots$, ces points représentent les équations $12^2 - 71 \times 2 - 2 = 0, 12^2 - 70 \times 2 - 4 = 0, 12^2 - 69 \times 2 - 6 = 0, 12^2 - 68 \times 2 - 8 = 0, \ldots$. On a fixé dans l'équation $x^2 - zy - t = 0$ les valeurs de x et y à 12 et 2 et z et t sont les coordonnées de points alignés. On remarque que ces droites passent par des points dont les ordonnées sont toutes impaires $1, 3, 5, \ldots$ ou toutes paires $2, 4, 6$ suivant que le carré est impair ou pair.

[1] Table II, n°99, p.499 de l'édition Jacques Gabay.

[2] comme Gauss.

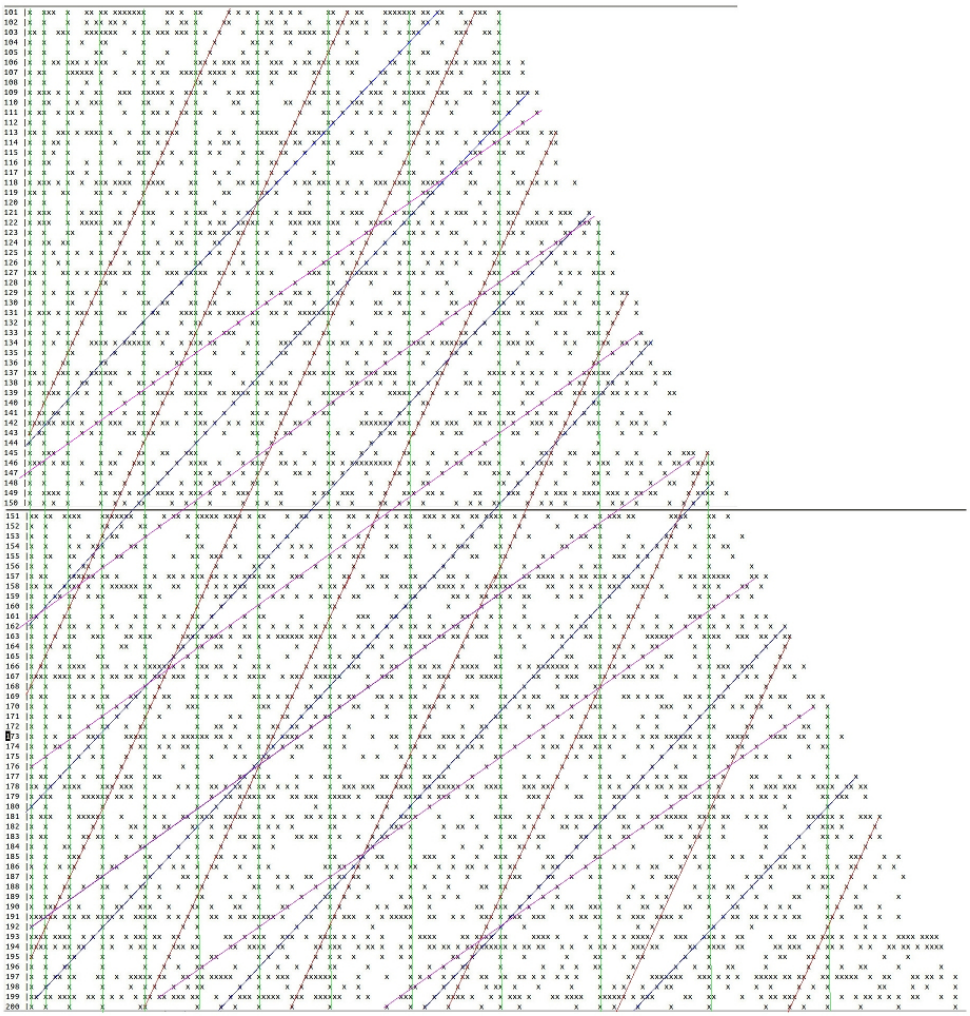
Il faut insister sur le fait que chaque croix représente une assertion logique contenant deux quantificateurs existentiels. Par exemple, les 3 points $(71,2),(70,4)$ et $(69,6)$ représentent les 3 assertions logiques :

- $\exists x_1, 1 \leqslant x_1 < 71, \exists y_1, 1 \leqslant y_1 < 71$, tels que $x_1^2 - 71y_1 - 2 = 0$ (que l'on peut écrire $x_1^2 \equiv 2\ (mod\ 71)$) ;
- $\exists x_2, 1 \leqslant x_2 < 70, \exists y_2, 1 \leqslant y_2 < 70$, tels que $x_2^2 - 70y_2 - 4 = 0$ (que l'on peut écrire $x_2^2 \equiv 4\ (mod\ 70)$) ;
- $\exists x_3, 1 \leqslant x_3 < 69, \exists y_3, 1 \leqslant y_3 < 69$, tels que $x_3^2 - 69y_3 - 6 = 0$ (que l'on peut écrire $x_3^3 \equiv 6\ (mod\ 69)$) ;

Ces trois assertions sont simultanément vérifiées par $x_1 = x_2 = x_3 = 12$ et $y_1 = y_2 = y_3 = 2$.

Le nombre de résidus quadratiques d'un nombre premier p est égal à $\dfrac{p-1}{2}$, c'est un fait démontré par Gauss. On peut relier les résultats présentés ici à ce fait en distinguant les deux sortes de nombres premiers :

- pour un nombre premier p de la forme $4k-1$, il y a autant de couples (x,y) de produit $xy \equiv -1\ (mod\ p)$ que de résidus quadratiques de p (i.e. $2k-1 = \dfrac{p-1}{2}$) ; chacun des couples en question contient un résidu quadratique et un non-résidu quadratique
- pour un nombre premier p de la forme $4k+1$, si on note r le nombre de résidus quadratiques de p (égal à $\dfrac{p-1}{2}$), alors il y a $r+1$ couples (x,y) de produit $xy \equiv -1\ (mod\ p)$ (i.e. $\dfrac{p+1}{2}$) : deux résidus quadratiques sont systématiquement de carré congru à $-1\ (mod\ p)$ tandis que les autres couples de produit -1 font intervenir deux résidus quadratiques chacun.



En fixant 2 variables sur 4 dans les équations de la forme $x^2 - yz - t = 0$, on explique les droites de pente 1, 2 ou 3 qui apparaissent sur la table de résiduosité quadratique de Gauss pour les modules compris entre 100

et 200. On pourrait, de la même manière qu'on cherche des droites, chercher des points à coordonnées entières appartenant à certains cercles : ce qui importe, ce sont les liens que les points établissent entre 4 variables, pour ce qui concerne la résiduosité quadratique.

On voit clairement par les concentrations horizontales de points, le fait que les nombres premiers maximisent le nombre de résidus quadratiques (un nombre premier p a $\frac{p-1}{2}$ résidus quadratiques).

Rappels sur le nombre de racines de -1 dans les corps premiers (Denise Vella-Chemla, 4.11.2017)

On rappelle que :

- si p est de la forme $4k+1$, deux nombres et deux seulement ont pour carré -1 dans $\mathbb{Z}/p\mathbb{Z}$; ces nombres ont pour somme p et pour produit 1 ;
- il y a exactement $2k-1$ (respectivement $2k+1$) couples (x,y) tels que $xy \equiv -1\ (mod\ p)$.

Pour n composé, soit on trouve 0 ou 4 racines de -1 et non 2, soit on trouve, comme pour les nombres premiers, deux telles racines (par exemple, pour les carrés de nombres premiers de la forme $4k+1$) mais alors, le nombre de couples (x,y) tels que $xy \equiv -1\ (mod\ p)$ n'est pas égal à $2k-1$ si n est de la forme $4k-1$ ou n'est pas égal à $2k+1$ si n est de la forme $4k+1$.

Fournissons quelques valeurs pour fixer les idées :

- dans $\mathbb{Z}/5\mathbb{Z}$, 2 et 3 ont pour carré -1 ;
- dans $\mathbb{Z}/13\mathbb{Z}$, 5 et 8 ont pour carré -1 ;
- dans $\mathbb{Z}/17\mathbb{Z}$, 4 et 13 ont pour carré -1 ;
- dans $\mathbb{Z}/29\mathbb{Z}$, 12 et 17 ont pour carré -1 ;
- dans $\mathbb{Z}/37\mathbb{Z}$, 6 et 31 ont pour carré -1 ;
- dans $\mathbb{Z}/41\mathbb{Z}$, 9 et 32 ont pour carré -1 ;
- dans $\mathbb{Z}/53\mathbb{Z}$, 23 et 30 ont pour carré -1 ;
- dans $\mathbb{Z}/61\mathbb{Z}$, 11 et 50 ont pour carré -1 ;
- dans $\mathbb{Z}/73\mathbb{Z}$, 27 et 46 ont pour carré -1 ;
- dans $\mathbb{Z}/89\mathbb{Z}$, 34 et 55 ont pour carré -1 ;
- dans $\mathbb{Z}/97\mathbb{Z}$, 75 et 22 ont pour carré -1.

Dans $\mathbb{Z}/n\mathbb{Z}$ lorsque $n = 9, 21, 33, 45, 49, 57, 69, 77, 81, 93$, il n'y a pas de racine de -1.

Dans $\mathbb{Z}/n\mathbb{Z}$ lorsque $n = 65$ ou $n = 85$, il y a 4 racines de -1 (deux à deux de somme n et de produit 1), qui sont les nombres 8 et 57 ou bien 18 et 47 si $p = 65$ ou qui sont 13 et 72 ou bien 38 et 47 si $p = 85$.

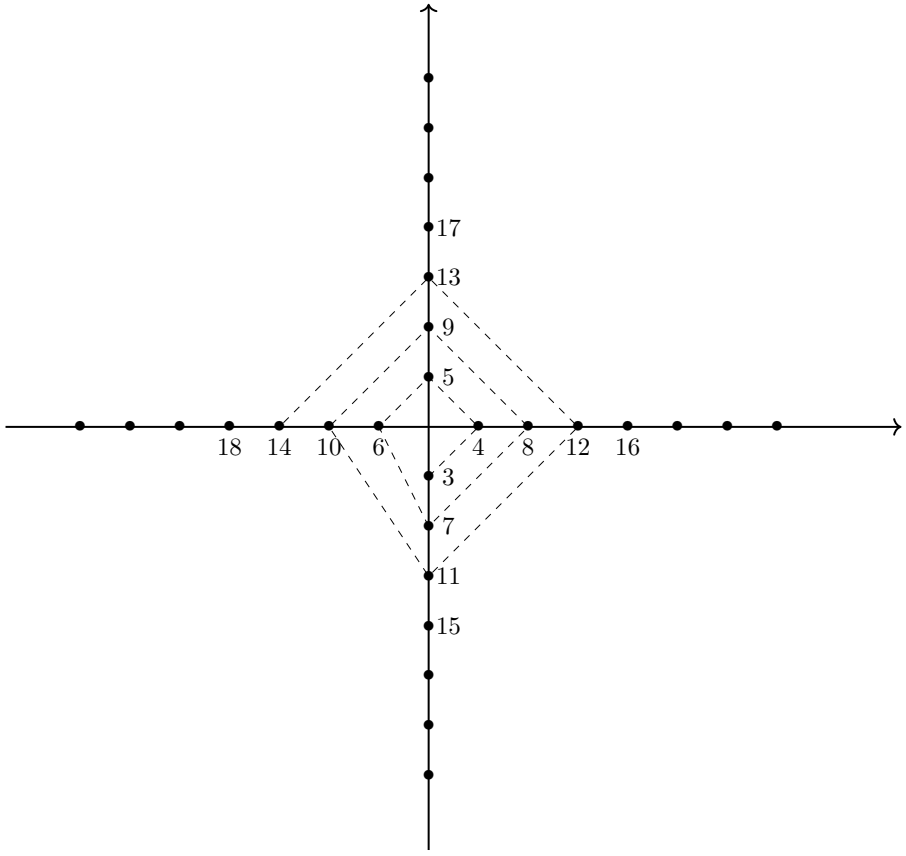
Pour 25 $(= 4 \times 6 + 1)$, carré d'un nombre premier de la forme $4k+1$, il y a, comme pour les nombres premiers de la forme $4k+1$, 2 racines carrées de -1 (7 et 18) mais ce qui exclut la primalité alors, c'est le nombre de couples (x,y) dont le produit est égal à -1 qui s'élève à 10, différent de 13 $(= 2 \times 6 + 1)$.

Pour les carrés de nombres premiers de la forme $4k+3$ (49, 121, 361), il n'y a pas de racine de -1.

Dans une note toute récente, on avait proposé un positionnement des nombres par des points du plan complexe qui les faisaient "faire la navette" entre les deux demi-axes positifs des coordonnées. On omettait les points associés aux nombres pairs parce qu'on ne voyait pas trop où les placer.

Essayons de proposer une nouvelle représentation graphique, qui pourrait peut-être être utile pour étudier la primalité.

On se place dans le plan complexe. On positionne les nombres sur une spirale selon le graphique suivant :



La transformation des coordonnées qui permet de passer d'un point de la spirale au suivant est la transformation qui permet d'obtenir la chaîne de points ci-dessous :

$$\begin{pmatrix}0\\-i\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\i\end{pmatrix}\begin{pmatrix}-1\\0\end{pmatrix}\begin{pmatrix}0\\-2i\end{pmatrix}\begin{pmatrix}2\\0\end{pmatrix}\begin{pmatrix}0\\2i\end{pmatrix}\begin{pmatrix}-2\\0\end{pmatrix}\cdots$$

Cette transformation a pour opérateur :

$$\begin{pmatrix}x\\y\end{pmatrix} \mapsto \begin{pmatrix}0 & i\\ i & 0\end{pmatrix}\begin{pmatrix}x\\y\end{pmatrix} = \begin{pmatrix}iy\\ix\end{pmatrix}$$

faux : cela ne fait pas augmenter le rayon.

On doit pour représenter les points de la spirale utiliser un complexe en première coordonnée (qui vaut k, $-k$, ki ou $-ki$ selon le graphique ci-dessus, i.e. $k = \left\lfloor \frac{n+1}{4} \right\rfloor$) et 3 booléens en $2^{ème}$, $3^{ème}$ et $4^{ème}$ coordonnées. Les booléens servent à se promener sur un carré de sommets $(1,1),(0,1),(0,0),(1,0)$ qui sont des points tels qu'effectuer un $\wedge$ logique entre leurs coordonnées permet d'obtenir un 1 une fois sur 4 (on voit dans la chaîne de bipoints fournie un peu plus haut qu'il fallait augmenter la valeur de la coordonnée non nulle tous les 4 points et que l'opérateur proposé n'effectuait pas cette augmentation périodique). La transformation corrigée devient :

$$\begin{pmatrix}x\\y\\z\\t\end{pmatrix} \mapsto \begin{pmatrix}ix+yz\\1-z\\y\\yz\end{pmatrix}$$

x est un $\pm k$ ou un $\pm ki$, y et z sont les booléens et yz calcule leur $\wedge$ logique)

Il faudrait maintenant essayer de démontrer les éléments rappelés en se basant sur cette représentation.

```
import mpmath
import math
from mpmath import *
from math import *

print(21.0220396387**2/14.1347251417**2)
print(25.0108575801**2/14.1347251417**2)
print(30.4248761258**2/14.1347251417**2)
print(32.9350615877**2/14.1347251417**2)
print(37.5861781588**2/14.1347251417**2)
print(40.9187190121**2/14.1347251417**2)
print(43.3270732809**2/14.1347251417**2)
print(48.0051508811**2/14.1347251417**2)
print(49.773832477**2/14.1347251417**2)
print(52.970321477**2/14.1347251417**2)
print(56.446247697**2/14.1347251417**2)
print(59.34704400**2/14.1347251417**2)
print(60.831778524**2/14.1347251417**2)
print(65.112544048**2/14.1347251417**2)
print(67.079810529**2/14.1347251417**2)
print(69.546401711**2/14.1347251417**2)
print(72.067157674**2/14.1347251417**2)
print(75.704690699**2/14.1347251417**2)
print(77.144840068**2/14.1347251417**2)
print(79.337375020**2/14.1347251417**2)
print(82.910380854**2/14.1347251417**2)
print(84.735492980**2/14.1347251417**2)
print(87.425274613**2/14.1347251417**2)
print(88.809111207**2/14.1347251417**2)
print(92.491899270**2/14.1347251417**2)
print("toto")
print(li(3)-li(15))
print(li(5)-li(15))
print(li(7)-li(15))
print(li(11)-li(15))
print(li(13)-li(15))
print(li(17)-li(15))
print(li(19)-li(15))
print(li(23)-li(15))
print(li(29)-li(15))
print(li(31)-li(15))
print(li(37)-li(15))
print(li(41)-li(15))
print(li(43)-li(15))
print(li(47)-li(15))
print(li(53)-li(15))
print(li(59)-li(15))
print(li(61)-li(15))
print(li(67)-li(15))
print(li(71)-li(15))
print(li(73)-li(15))
print(li(79)-li(15))
print(li(83)-li(15))
print(li(89)-li(15))
print(li(97)-li(15))
print(li(101)-li(15))
print(li(103)-li(15))
```

2.21194826822
3.13099540926
4.63321978045
5.42927980569
7.07101242538
8.38048828211
9.39602084931
11.5345576097
12.4001639695
14.0439890371
15.9476031113
17.6288283367
18.5219322991
21.2204501761
22.5221018912
24.2088742179
25.9956123509
28.6860560915
29.7878412367
31.5051040871
34.4067050608
35.9381722046
38.2559749794
39.4766518753
42.8186193269
toto
-5.99123626410135
-4.52023654873589
-3.39777309277094
-1.56381564304733
-0.758276910580418
0.72163974124984
1.41380097411922
2.7287221955143
4.57232654615584
5.16040562551971
6.8628615885764
7.95489746960261
8.49001101225739
9.5409390120119
11.0750284297464
12.5658468948806
13.0543337907783
14.4972171516195
15.4419725186481
15.9096316748034
17.2951998578258
18.2054697187695
19.5525573315657
21.3177221037543
22.1882293218323
22.6206664418309

```
import mpmath
import math
from mpmath import *
from math import *

print(21.0220396387**2/14.1347251417**2)
print(25.0108575801**2/14.1347251417**2)
print(30.4248761258**2/14.1347251417**2)
print(32.9350615877**2/14.1347251417**2)
print(37.5861781588**2/14.1347251417**2)
print(40.9187190121**2/14.1347251417**2)
print(43.3270732809**2/14.1347251417**2)
print(48.0051508811**2/14.1347251417**2)
print(49.773832477**2/14.1347251417**2)
print(52.970321477**2/14.1347251417**2)
print(56.446247697**2/14.1347251417**2)
print(59.34704400**2/14.1347251417**2)
print(60.831778524**2/14.1347251417**2)
print(65.112544048**2/14.1347251417**2)
print(67.079810529**2/14.1347251417**2)
print(69.546401711**2/14.1347251417**2)
print(72.067157674**2/14.1347251417**2)
print(75.704690699**2/14.1347251417**2)
print(77.144840068**2/14.1347251417**2)
print(79.337375020**2/14.1347251417**2)
print(82.910380854**2/14.1347251417**2)
print(84.735492980**2/14.1347251417**2)
print(87.425274613**2/14.1347251417**2)
print(88.809111207**2/14.1347251417**2)
print(92.491899270**2/14.1347251417**2)
print("toto")
print(li(3)-li(15))
print(li(5)-li(15))
print(li(7)-li(15))
print(li(11)-li(15))
print(li(13)-li(15))
print(li(17)-li(15))
print(li(19)-li(15))
print(li(23)-li(15))
print(li(29)-li(15))
print(li(31)-li(15))
print(li(37)-li(15))
print(li(41)-li(15))
print(li(43)-li(15))
print(li(47)-li(15))
print(li(53)-li(15))
print(li(59)-li(15))
print(li(61)-li(15))
print(li(67)-li(15))
print(li(71)-li(15))
print(li(73)-li(15))
print(li(79)-li(15))
print(li(83)-li(15))
print(li(89)-li(15))
print(li(97)-li(15))
print(li(101)-li(15))
print(li(103)-li(15))
```

2.21194826822
3.13099540926
4.63321978045
5.42927980569
7.07101242538
8.38048828211
9.39602084931
11.5345576097
12.4001639695
14.0439890371
15.9476031113
17.6288283367
18.5219322991
21.2204501761
22.5221018912
24.2088742179
25.9956123509
28.6860560915
29.7878412367
31.5051040871
34.4067050608
35.9381722046
38.2559749794
39.4766518753
42.8186193269
toto
-5.99123626410135
-4.52023654873589
-3.39777309277094
-1.56381564304733
-0.758276910580418
0.72163974124984
1.41380097411922
2.7287221955143
4.57232654615584
5.16040562551971
6.8628615885764
7.95489746960261
8.49001101225739
9.5409390120119
11.0750284297464
12.5658468948806
13.0543337907783
14.4972171516195
15.4419725186481
15.9096316748034
17.2951998578258
18.2054697187695
19.5525573315657
21.3177221037543
22.1882293218323
22.6206664418309

```
#include <iostream>
#include <stdio.h>
#include <cmath>
#include <fstream>
#include <complex>
#define _USE_MATH_DEFINES

using namespace std ;
typedef complex<double> dcomp ;
const dcomp racmoinsun = sqrt(dcomp(-1.0));

int prime(int atester)
{
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve)
    {
    if ((k * k) > atester) return 1;
    else
      if ((atester % k) == 0) {
      return 0 ;
      }
      else k++;
    }
}

int main (int argc, char* argv[])
{
  double zeros[100005], z ;
  dcomp somme ;
  int i, j, k, n, touslesmille ;
  double stocke[1000], rescalcul ;
  bool trouve ;

  std::ifstream fic2("leszerospourj", std::ios::in) ;
  if (fic2)
    {
      while (not fic2.eof()) {
      {
        fic2 >> i >> z ;
        zeros[i] = z ; ;
        //std::cout << z << "\n" ;
      }
      }
      fic2.close();
    }
  else std::cerr << "Impossible d'ouvrir le fichier !" << std::endl ;

  touslesmille=1 ;
  for (i = 2 ; i <= 100000 ; ++i)
    {
      touslesmille=touslesmille+1;
      if (touslesmille <= 1000)
      std::cout << "zeros[" << i << "]^2/zeros[1]^2 -> " << (zeros[i]*zeros[i])/
(zeros[1]*zeros[1]) << "\n" ;
      else if ((touslesmille%1000) == 0)
      std::cout << "zeros[" << i << "]^2/zeros[1]^2 -> " << (zeros[i]*zeros[i])/
(zeros[1]*zeros[1]) << "\n" ;
```

```
    }
  std:cout << "\n\n" ;
}
```

```
zeros[2]^2/zeros[1]^2 -> 2.21195
zeros[3]^2/zeros[1]^2 -> 3.131
zeros[4]^2/zeros[1]^2 -> 4.63322
zeros[5]^2/zeros[1]^2 -> 5.42928
zeros[6]^2/zeros[1]^2 -> 7.07101
zeros[7]^2/zeros[1]^2 -> 8.38049
zeros[8]^2/zeros[1]^2 -> 9.39602
zeros[9]^2/zeros[1]^2 -> 11.5346
zeros[10]^2/zeros[1]^2 -> 12.4002
zeros[11]^2/zeros[1]^2 -> 14.044
zeros[12]^2/zeros[1]^2 -> 15.9476
zeros[13]^2/zeros[1]^2 -> 17.6288
zeros[14]^2/zeros[1]^2 -> 18.5219
zeros[15]^2/zeros[1]^2 -> 21.2205
zeros[16]^2/zeros[1]^2 -> 22.5221
zeros[17]^2/zeros[1]^2 -> 24.2089
zeros[18]^2/zeros[1]^2 -> 25.9956
zeros[19]^2/zeros[1]^2 -> 28.6861
zeros[20]^2/zeros[1]^2 -> 29.7878
zeros[21]^2/zeros[1]^2 -> 31.5051
zeros[22]^2/zeros[1]^2 -> 34.4067
zeros[23]^2/zeros[1]^2 -> 35.9382
zeros[24]^2/zeros[1]^2 -> 38.256
zeros[25]^2/zeros[1]^2 -> 39.4767
zeros[26]^2/zeros[1]^2 -> 42.8186
zeros[27]^2/zeros[1]^2 -> 44.8414
zeros[28]^2/zeros[1]^2 -> 46.0041
zeros[29]^2/zeros[1]^2 -> 48.8892
zeros[30]^2/zeros[1]^2 -> 51.3804
zeros[31]^2/zeros[1]^2 -> 53.8514
zeros[32]^2/zeros[1]^2 -> 55.6533
zeros[33]^2/zeros[1]^2 -> 57.4858
zeros[34]^2/zeros[1]^2 -> 61.7024
zeros[35]^2/zeros[1]^2 -> 62.6453
zeros[36]^2/zeros[1]^2 -> 65.4141
zeros[37]^2/zeros[1]^2 -> 67.614
zeros[38]^2/zeros[1]^2 -> 70.6303
zeros[39]^2/zeros[1]^2 -> 73.7308
zeros[40]^2/zeros[1]^2 -> 75.6589
zeros[41]^2/zeros[1]^2 -> 77.2798
zeros[42]^2/zeros[1]^2 -> 81.3878
zeros[43]^2/zeros[1]^2 -> 84.0413
zeros[44]^2/zeros[1]^2 -> 86.01
zeros[45]^2/zeros[1]^2 -> 89.2017
zeros[46]^2/zeros[1]^2 -> 90.8918
zeros[47]^2/zeros[1]^2 -> 95.4802
zeros[48]^2/zeros[1]^2 -> 97.7334
zeros[49]^2/zeros[1]^2 -> 99.6839
zeros[50]^2/zeros[1]^2 -> 102.512
zeros[51]^2/zeros[1]^2 -> 106.693
zeros[52]^2/zeros[1]^2 -> 108.781
zeros[53]^2/zeros[1]^2 -> 112.698
zeros[54]^2/zeros[1]^2 -> 114.012
zeros[55]^2/zeros[1]^2 -> 117.206
zeros[56]^2/zeros[1]^2 -> 121.984
zeros[57]^2/zeros[1]^2 -> 124.315
zeros[58]^2/zeros[1]^2 -> 126.299
zeros[59]^2/zeros[1]^2 -> 130.046
zeros[60]^2/zeros[1]^2 -> 133.034
zeros[61]^2/zeros[1]^2 -> 137.156
zeros[62]^2/zeros[1]^2 -> 139.9
zeros[63]^2/zeros[1]^2 -> 143.115
zeros[64]^2/zeros[1]^2 -> 144.502
zeros[65]^2/zeros[1]^2 -> 150.516
```

```
zeros[66]^2/zeros[1]^2 -> 152.855
zeros[67]^2/zeros[1]^2 -> 155.821
zeros[68]^2/zeros[1]^2 -> 159.259
zeros[69]^2/zeros[1]^2 -> 162.019
zeros[70]^2/zeros[1]^2 -> 166.171
zeros[71]^2/zeros[1]^2 -> 171.072
zeros[72]^2/zeros[1]^2 -> 172.415
zeros[73]^2/zeros[1]^2 -> 175.457
zeros[74]^2/zeros[1]^2 -> 179.581
zeros[75]^2/zeros[1]^2 -> 184.565
zeros[76]^2/zeros[1]^2 -> 186.594
zeros[77]^2/zeros[1]^2 -> 190.843
zeros[78]^2/zeros[1]^2 -> 194.005
zeros[79]^2/zeros[1]^2 -> 196.256
zeros[80]^2/zeros[1]^2 -> 202.75
zeros[81]^2/zeros[1]^2 -> 205.233
zeros[82]^2/zeros[1]^2 -> 208.686
zeros[83]^2/zeros[1]^2 -> 211.156
zeros[84]^2/zeros[1]^2 -> 216.352
zeros[85]^2/zeros[1]^2 -> 219.842
zeros[86]^2/zeros[1]^2 -> 224.3
zeros[87]^2/zeros[1]^2 -> 227.825
zeros[88]^2/zeros[1]^2 -> 230.394
zeros[89]^2/zeros[1]^2 -> 233.891
zeros[90]^2/zeros[1]^2 -> 240.205
zeros[91]^2/zeros[1]^2 -> 243.831
zeros[92]^2/zeros[1]^2 -> 245.415
zeros[93]^2/zeros[1]^2 -> 251.159
zeros[94]^2/zeros[1]^2 -> 253.353
zeros[95]^2/zeros[1]^2 -> 258.874
zeros[96]^2/zeros[1]^2 -> 263.254
zeros[97]^2/zeros[1]^2 -> 267.664
zeros[98]^2/zeros[1]^2 -> 269.373
zeros[99]^2/zeros[1]^2 -> 273.349
zeros[100]^2/zeros[1]^2 -> 280.012
zeros[101]^2/zeros[1]^2 -> 282.969
zeros[102]^2/zeros[1]^2 -> 287.235
zeros[103]^2/zeros[1]^2 -> 290.828
zeros[104]^2/zeros[1]^2 -> 295.125
zeros[105]^2/zeros[1]^2 -> 298.165
zeros[106]^2/zeros[1]^2 -> 305.704
zeros[107]^2/zeros[1]^2 -> 308.096
zeros[108]^2/zeros[1]^2 -> 311.762
zeros[109]^2/zeros[1]^2 -> 315.373
zeros[110]^2/zeros[1]^2 -> 320.558
zeros[111]^2/zeros[1]^2 -> 326.248
zeros[112]^2/zeros[1]^2 -> 329
zeros[113]^2/zeros[1]^2 -> 334.748
zeros[114]^2/zeros[1]^2 -> 338.028
zeros[115]^2/zeros[1]^2 -> 340.453
zeros[116]^2/zeros[1]^2 -> 347.72
zeros[117]^2/zeros[1]^2 -> 352.975
zeros[118]^2/zeros[1]^2 -> 355.79
zeros[119]^2/zeros[1]^2 -> 359.287
zeros[120]^2/zeros[1]^2 -> 364.802
zeros[121]^2/zeros[1]^2 -> 368.932
zeros[122]^2/zeros[1]^2 -> 374.293
zeros[123]^2/zeros[1]^2 -> 380.141
zeros[124]^2/zeros[1]^2 -> 382.529
zeros[125]^2/zeros[1]^2 -> 387.523
zeros[126]^2/zeros[1]^2 -> 390.254
zeros[127]^2/zeros[1]^2 -> 399.351
zeros[128]^2/zeros[1]^2 -> 401.464
zeros[129]^2/zeros[1]^2 -> 406.083
```

```
zeros[130]^2/zeros[1]^2 -> 411.322
zeros[131]^2/zeros[1]^2 -> 414.901
zeros[132]^2/zeros[1]^2 -> 419.722
zeros[133]^2/zeros[1]^2 -> 426.318
zeros[134]^2/zeros[1]^2 -> 431.335
zeros[135]^2/zeros[1]^2 -> 435.479
zeros[136]^2/zeros[1]^2 -> 437.276
zeros[137]^2/zeros[1]^2 -> 444.424
zeros[138]^2/zeros[1]^2 -> 449.993
zeros[139]^2/zeros[1]^2 -> 455.439
zeros[140]^2/zeros[1]^2 -> 458.607
zeros[141]^2/zeros[1]^2 -> 465.199
zeros[142]^2/zeros[1]^2 -> 467.841
zeros[143]^2/zeros[1]^2 -> 472.414
zeros[144]^2/zeros[1]^2 -> 481.344
zeros[145]^2/zeros[1]^2 -> 484.626
zeros[146]^2/zeros[1]^2 -> 488.568
zeros[147]^2/zeros[1]^2 -> 493.451
zeros[148]^2/zeros[1]^2 -> 498.146
zeros[149]^2/zeros[1]^2 -> 505.306
zeros[150]^2/zeros[1]^2 -> 508.87
zeros[151]^2/zeros[1]^2 -> 516.26
zeros[152]^2/zeros[1]^2 -> 519.43
zeros[153]^2/zeros[1]^2 -> 523.703
zeros[154]^2/zeros[1]^2 -> 528.233
zeros[155]^2/zeros[1]^2 -> 536.66
zeros[156]^2/zeros[1]^2 -> 541.882
zeros[157]^2/zeros[1]^2 -> 544.917
zeros[158]^2/zeros[1]^2 -> 549.953
zeros[159]^2/zeros[1]^2 -> 557.18
zeros[160]^2/zeros[1]^2 -> 559.072
zeros[161]^2/zeros[1]^2 -> 567.907
zeros[162]^2/zeros[1]^2 -> 572.97
zeros[163]^2/zeros[1]^2 -> 578.124
zeros[164]^2/zeros[1]^2 -> 582.159
zeros[165]^2/zeros[1]^2 -> 585.621
zeros[166]^2/zeros[1]^2 -> 594.581
zeros[167]^2/zeros[1]^2 -> 600.413
zeros[168]^2/zeros[1]^2 -> 603.624
zeros[169]^2/zeros[1]^2 -> 610.749
zeros[170]^2/zeros[1]^2 -> 614.574
zeros[171]^2/zeros[1]^2 -> 619.742
zeros[172]^2/zeros[1]^2 -> 625.427
zeros[173]^2/zeros[1]^2 -> 634.407
zeros[174]^2/zeros[1]^2 -> 638.454
zeros[175]^2/zeros[1]^2 -> 641.323
zeros[176]^2/zeros[1]^2 -> 647.757
zeros[177]^2/zeros[1]^2 -> 653.335
zeros[178]^2/zeros[1]^2 -> 660.741
zeros[179]^2/zeros[1]^2 -> 665.859
zeros[180]^2/zeros[1]^2 -> 671.262
zeros[181]^2/zeros[1]^2 -> 677.807
zeros[182]^2/zeros[1]^2 -> 681.402
zeros[183]^2/zeros[1]^2 -> 685.407
zeros[184]^2/zeros[1]^2 -> 696.606
zeros[185]^2/zeros[1]^2 -> 699.608
zeros[186]^2/zeros[1]^2 -> 706.966
zeros[187]^2/zeros[1]^2 -> 708.842
zeros[188]^2/zeros[1]^2 -> 716.823
zeros[189]^2/zeros[1]^2 -> 722.274
zeros[190]^2/zeros[1]^2 -> 728.415
zeros[191]^2/zeros[1]^2 -> 735.916
zeros[192]^2/zeros[1]^2 -> 741.733
zeros[193]^2/zeros[1]^2 -> 745.226
```

```
zeros[194]^2/zeros[1]^2 -> 750.494
zeros[195]^2/zeros[1]^2 -> 756.799
zeros[196]^2/zeros[1]^2 -> 766.993
zeros[197]^2/zeros[1]^2 -> 770.088
zeros[198]^2/zeros[1]^2 -> 774.739
zeros[199]^2/zeros[1]^2 -> 783.25
zeros[200]^2/zeros[1]^2 -> 786.417
zeros[201]^2/zeros[1]^2 -> 792.527
zeros[202]^2/zeros[1]^2 -> 800.779
zeros[203]^2/zeros[1]^2 -> 808.221
zeros[204]^2/zeros[1]^2 -> 812.34
zeros[205]^2/zeros[1]^2 -> 817.892
zeros[206]^2/zeros[1]^2 -> 821.53
zeros[207]^2/zeros[1]^2 -> 831.484
zeros[208]^2/zeros[1]^2 -> 837.066
zeros[209]^2/zeros[1]^2 -> 843.492
zeros[210]^2/zeros[1]^2 -> 849.496
zeros[211]^2/zeros[1]^2 -> 854.826
zeros[212]^2/zeros[1]^2 -> 862.106
zeros[213]^2/zeros[1]^2 -> 863.92
zeros[214]^2/zeros[1]^2 -> 876.159
zeros[215]^2/zeros[1]^2 -> 882.342
zeros[216]^2/zeros[1]^2 -> 885.634
zeros[217]^2/zeros[1]^2 -> 891.678
zeros[218]^2/zeros[1]^2 -> 898.62
zeros[219]^2/zeros[1]^2 -> 904.37
zeros[220]^2/zeros[1]^2 -> 913.494
zeros[221]^2/zeros[1]^2 -> 917.429
zeros[222]^2/zeros[1]^2 -> 926.885
zeros[223]^2/zeros[1]^2 -> 931.08
zeros[224]^2/zeros[1]^2 -> 934.698
zeros[225]^2/zeros[1]^2 -> 942.287
zeros[226]^2/zeros[1]^2 -> 952.18
zeros[227]^2/zeros[1]^2 -> 958.393
zeros[228]^2/zeros[1]^2 -> 962.954
zeros[229]^2/zeros[1]^2 -> 968.656
zeros[230]^2/zeros[1]^2 -> 976.443
zeros[231]^2/zeros[1]^2 -> 981.851
zeros[232]^2/zeros[1]^2 -> 988.134
zeros[233]^2/zeros[1]^2 -> 999.469
zeros[234]^2/zeros[1]^2 -> 1002.07
zeros[235]^2/zeros[1]^2 -> 1009.73
zeros[236]^2/zeros[1]^2 -> 1014.13
zeros[237]^2/zeros[1]^2 -> 1019.89
zeros[238]^2/zeros[1]^2 -> 1031.6
zeros[239]^2/zeros[1]^2 -> 1036.1
zeros[240]^2/zeros[1]^2 -> 1042.27
zeros[241]^2/zeros[1]^2 -> 1049.48
zeros[242]^2/zeros[1]^2 -> 1056.87
zeros[243]^2/zeros[1]^2 -> 1059.51
zeros[244]^2/zeros[1]^2 -> 1068.64
zeros[245]^2/zeros[1]^2 -> 1077.88
zeros[246]^2/zeros[1]^2 -> 1085.39
zeros[247]^2/zeros[1]^2 -> 1089.58
zeros[248]^2/zeros[1]^2 -> 1093.64
zeros[249]^2/zeros[1]^2 -> 1103.48
zeros[250]^2/zeros[1]^2 -> 1109.3
zeros[251]^2/zeros[1]^2 -> 1118.87
zeros[252]^2/zeros[1]^2 -> 1123.78
zeros[253]^2/zeros[1]^2 -> 1132.16
zeros[254]^2/zeros[1]^2 -> 1137.74
zeros[255]^2/zeros[1]^2 -> 1143.98
zeros[256]^2/zeros[1]^2 -> 1148.13
zeros[257]^2/zeros[1]^2 -> 1162.02
```

```
zeros[258]^2/zeros[1]^2 -> 1166.87
zeros[259]^2/zeros[1]^2 -> 1171.79
zeros[260]^2/zeros[1]^2 -> 1179.98
zeros[261]^2/zeros[1]^2 -> 1184.79
zeros[262]^2/zeros[1]^2 -> 1193.83
zeros[263]^2/zeros[1]^2 -> 1200.1
zeros[264]^2/zeros[1]^2 -> 1208.63
zeros[265]^2/zeros[1]^2 -> 1218.07
zeros[266]^2/zeros[1]^2 -> 1221.25
zeros[267]^2/zeros[1]^2 -> 1228.19
zeros[268]^2/zeros[1]^2 -> 1233.5
zeros[269]^2/zeros[1]^2 -> 1244.22
zeros[270]^2/zeros[1]^2 -> 1252.86
zeros[271]^2/zeros[1]^2 -> 1259.35
zeros[272]^2/zeros[1]^2 -> 1262.73
zeros[273]^2/zeros[1]^2 -> 1273.93
zeros[274]^2/zeros[1]^2 -> 1278.56
zeros[275]^2/zeros[1]^2 -> 1283.87
zeros[276]^2/zeros[1]^2 -> 1295.75
zeros[277]^2/zeros[1]^2 -> 1303.21
zeros[278]^2/zeros[1]^2 -> 1309.85
zeros[279]^2/zeros[1]^2 -> 1315.29
zeros[280]^2/zeros[1]^2 -> 1320.66
zeros[281]^2/zeros[1]^2 -> 1329.76
zeros[282]^2/zeros[1]^2 -> 1340.9
zeros[283]^2/zeros[1]^2 -> 1344.24
zeros[284]^2/zeros[1]^2 -> 1353.97
zeros[285]^2/zeros[1]^2 -> 1361.37
zeros[286]^2/zeros[1]^2 -> 1366.24
zeros[287]^2/zeros[1]^2 -> 1374.11
zeros[288]^2/zeros[1]^2 -> 1379.98
zeros[289]^2/zeros[1]^2 -> 1394.87
zeros[290]^2/zeros[1]^2 -> 1397.53
zeros[291]^2/zeros[1]^2 -> 1404.95
zeros[292]^2/zeros[1]^2 -> 1410.58
zeros[293]^2/zeros[1]^2 -> 1420.27
zeros[294]^2/zeros[1]^2 -> 1426.1
zeros[295]^2/zeros[1]^2 -> 1436.19
zeros[296]^2/zeros[1]^2 -> 1443.73
zeros[297]^2/zeros[1]^2 -> 1451.05
zeros[298]^2/zeros[1]^2 -> 1460.68
zeros[299]^2/zeros[1]^2 -> 1462.94
zeros[300]^2/zeros[1]^2 -> 1469.53
zeros[301]^2/zeros[1]^2 -> 1483
zeros[302]^2/zeros[1]^2 -> 1490.16
zeros[303]^2/zeros[1]^2 -> 1497.67
zeros[304]^2/zeros[1]^2 -> 1502.72
zeros[305]^2/zeros[1]^2 -> 1511.32
zeros[306]^2/zeros[1]^2 -> 1519.43
zeros[307]^2/zeros[1]^2 -> 1525.39
zeros[308]^2/zeros[1]^2 -> 1534.89
zeros[309]^2/zeros[1]^2 -> 1546.14
zeros[310]^2/zeros[1]^2 -> 1552.31
zeros[311]^2/zeros[1]^2 -> 1556.02
zeros[312]^2/zeros[1]^2 -> 1565.81
zeros[313]^2/zeros[1]^2 -> 1570.99
zeros[314]^2/zeros[1]^2 -> 1584.02
zeros[315]^2/zeros[1]^2 -> 1593.06
zeros[316]^2/zeros[1]^2 -> 1595.01
zeros[317]^2/zeros[1]^2 -> 1607.42
zeros[318]^2/zeros[1]^2 -> 1613.29
zeros[319]^2/zeros[1]^2 -> 1620.07
zeros[320]^2/zeros[1]^2 -> 1626.5
zeros[321]^2/zeros[1]^2 -> 1640.04
```

```
zeros[322]^2/zeros[1]^2 -> 1646.89
zeros[323]^2/zeros[1]^2 -> 1655.4
zeros[324]^2/zeros[1]^2 -> 1659.51
zeros[325]^2/zeros[1]^2 -> 1666.62
zeros[326]^2/zeros[1]^2 -> 1678.54
zeros[327]^2/zeros[1]^2 -> 1684.56
zeros[328]^2/zeros[1]^2 -> 1695.09
zeros[329]^2/zeros[1]^2 -> 1702.61
zeros[330]^2/zeros[1]^2 -> 1710.35
zeros[331]^2/zeros[1]^2 -> 1718.69
zeros[332]^2/zeros[1]^2 -> 1723.14
zeros[333]^2/zeros[1]^2 -> 1731.36
zeros[334]^2/zeros[1]^2 -> 1746.23
zeros[335]^2/zeros[1]^2 -> 1752.53
zeros[336]^2/zeros[1]^2 -> 1757.55
zeros[337]^2/zeros[1]^2 -> 1765.88
zeros[338]^2/zeros[1]^2 -> 1776.32
zeros[339]^2/zeros[1]^2 -> 1780.11
zeros[340]^2/zeros[1]^2 -> 1792.85
zeros[341]^2/zeros[1]^2 -> 1799.16
zeros[342]^2/zeros[1]^2 -> 1811.52
zeros[343]^2/zeros[1]^2 -> 1817.41
zeros[344]^2/zeros[1]^2 -> 1823.73
zeros[345]^2/zeros[1]^2 -> 1829.72
zeros[346]^2/zeros[1]^2 -> 1840.43
zeros[347]^2/zeros[1]^2 -> 1852.77
zeros[348]^2/zeros[1]^2 -> 1858.73
zeros[349]^2/zeros[1]^2 -> 1867.58
zeros[350]^2/zeros[1]^2 -> 1873.3
zeros[351]^2/zeros[1]^2 -> 1884.5
zeros[352]^2/zeros[1]^2 -> 1890.93
zeros[353]^2/zeros[1]^2 -> 1896.43
zeros[354]^2/zeros[1]^2 -> 1912.32
zeros[355]^2/zeros[1]^2 -> 1918.96
zeros[356]^2/zeros[1]^2 -> 1925.71
zeros[357]^2/zeros[1]^2 -> 1934.64
zeros[358]^2/zeros[1]^2 -> 1938.78
zeros[359]^2/zeros[1]^2 -> 1950.61
zeros[360]^2/zeros[1]^2 -> 1961.56
zeros[361]^2/zeros[1]^2 -> 1969.39
zeros[362]^2/zeros[1]^2 -> 1976.04
zeros[363]^2/zeros[1]^2 -> 1989.57
zeros[364]^2/zeros[1]^2 -> 1991.67
zeros[365]^2/zeros[1]^2 -> 2000.64
zeros[366]^2/zeros[1]^2 -> 2009.01
zeros[367]^2/zeros[1]^2 -> 2021.57
zeros[368]^2/zeros[1]^2 -> 2033.51
zeros[369]^2/zeros[1]^2 -> 2036.88
zeros[370]^2/zeros[1]^2 -> 2043.29
zeros[371]^2/zeros[1]^2 -> 2054.6
zeros[372]^2/zeros[1]^2 -> 2062.63
zeros[373]^2/zeros[1]^2 -> 2071.21
zeros[374]^2/zeros[1]^2 -> 2082.25
zeros[375]^2/zeros[1]^2 -> 2091.02
zeros[376]^2/zeros[1]^2 -> 2100.18
zeros[377]^2/zeros[1]^2 -> 2106.83
zeros[378]^2/zeros[1]^2 -> 2116
zeros[379]^2/zeros[1]^2 -> 2119.07
zeros[380]^2/zeros[1]^2 -> 2138.53
zeros[381]^2/zeros[1]^2 -> 2142.8
zeros[382]^2/zeros[1]^2 -> 2152.03
zeros[383]^2/zeros[1]^2 -> 2160.27
zeros[384]^2/zeros[1]^2 -> 2168.25
zeros[385]^2/zeros[1]^2 -> 2178.06
```

```
zeros[386]^2/zeros[1]^2 -> 2185.02
zeros[387]^2/zeros[1]^2 -> 2195.48
zeros[388]^2/zeros[1]^2 -> 2208.42
zeros[389]^2/zeros[1]^2 -> 2215.73
zeros[390]^2/zeros[1]^2 -> 2223.54
zeros[391]^2/zeros[1]^2 -> 2227.77
zeros[392]^2/zeros[1]^2 -> 2239.99
zeros[393]^2/zeros[1]^2 -> 2249.02
zeros[394]^2/zeros[1]^2 -> 2263.37
zeros[395]^2/zeros[1]^2 -> 2267.31
zeros[396]^2/zeros[1]^2 -> 2276.16
zeros[397]^2/zeros[1]^2 -> 2288.22
zeros[398]^2/zeros[1]^2 -> 2295.61
zeros[399]^2/zeros[1]^2 -> 2299.48
zeros[400]^2/zeros[1]^2 -> 2312.67
zeros[401]^2/zeros[1]^2 -> 2327.34
zeros[402]^2/zeros[1]^2 -> 2332.18
zeros[403]^2/zeros[1]^2 -> 2341.83
zeros[404]^2/zeros[1]^2 -> 2348.4
zeros[405]^2/zeros[1]^2 -> 2356.57
zeros[406]^2/zeros[1]^2 -> 2368.94
zeros[407]^2/zeros[1]^2 -> 2378.64
zeros[408]^2/zeros[1]^2 -> 2386.28
zeros[409]^2/zeros[1]^2 -> 2399.96
zeros[410]^2/zeros[1]^2 -> 2404.99
zeros[411]^2/zeros[1]^2 -> 2414.42
zeros[412]^2/zeros[1]^2 -> 2422.71
zeros[413]^2/zeros[1]^2 -> 2428.98
zeros[414]^2/zeros[1]^2 -> 2446.49
zeros[415]^2/zeros[1]^2 -> 2454.65
zeros[416]^2/zeros[1]^2 -> 2461.7
zeros[417]^2/zeros[1]^2 -> 2468.2
zeros[418]^2/zeros[1]^2 -> 2480.92
zeros[419]^2/zeros[1]^2 -> 2488.62
zeros[420]^2/zeros[1]^2 -> 2496.1
zeros[421]^2/zeros[1]^2 -> 2510.86
zeros[422]^2/zeros[1]^2 -> 2517.67
zeros[423]^2/zeros[1]^2 -> 2531.18
zeros[424]^2/zeros[1]^2 -> 2536.67
zeros[425]^2/zeros[1]^2 -> 2542.72
zeros[426]^2/zeros[1]^2 -> 2552.25
zeros[427]^2/zeros[1]^2 -> 2566.77
zeros[428]^2/zeros[1]^2 -> 2576.61
zeros[429]^2/zeros[1]^2 -> 2585.67
zeros[430]^2/zeros[1]^2 -> 2592.54
zeros[431]^2/zeros[1]^2 -> 2604.47
zeros[432]^2/zeros[1]^2 -> 2611.16
zeros[433]^2/zeros[1]^2 -> 2622.51
zeros[434]^2/zeros[1]^2 -> 2627.71
zeros[435]^2/zeros[1]^2 -> 2645.83
zeros[436]^2/zeros[1]^2 -> 2655.66
zeros[437]^2/zeros[1]^2 -> 2658.23
zeros[438]^2/zeros[1]^2 -> 2670.34
zeros[439]^2/zeros[1]^2 -> 2677.66
zeros[440]^2/zeros[1]^2 -> 2687.93
zeros[441]^2/zeros[1]^2 -> 2702.41
zeros[442]^2/zeros[1]^2 -> 2709.59
zeros[443]^2/zeros[1]^2 -> 2719.08
zeros[444]^2/zeros[1]^2 -> 2730.37
zeros[445]^2/zeros[1]^2 -> 2740.2
zeros[446]^2/zeros[1]^2 -> 2745.12
zeros[447]^2/zeros[1]^2 -> 2753.91
zeros[448]^2/zeros[1]^2 -> 2769.8
zeros[449]^2/zeros[1]^2 -> 2780.61
```

```
zeros[450]^2/zeros[1]^2 -> 2789.23
zeros[451]^2/zeros[1]^2 -> 2798.02
zeros[452]^2/zeros[1]^2 -> 2802.27
zeros[453]^2/zeros[1]^2 -> 2820.38
zeros[454]^2/zeros[1]^2 -> 2822.71
zeros[455]^2/zeros[1]^2 -> 2837.17
zeros[456]^2/zeros[1]^2 -> 2848
zeros[457]^2/zeros[1]^2 -> 2859.46
zeros[458]^2/zeros[1]^2 -> 2866.49
zeros[459]^2/zeros[1]^2 -> 2876.61
zeros[460]^2/zeros[1]^2 -> 2882.67
zeros[461]^2/zeros[1]^2 -> 2893.18
zeros[462]^2/zeros[1]^2 -> 2911.61
zeros[463]^2/zeros[1]^2 -> 2918.43
zeros[464]^2/zeros[1]^2 -> 2923.89
zeros[465]^2/zeros[1]^2 -> 2937.53
zeros[466]^2/zeros[1]^2 -> 2946.21
zeros[467]^2/zeros[1]^2 -> 2954.38
zeros[468]^2/zeros[1]^2 -> 2965.25
zeros[469]^2/zeros[1]^2 -> 2975.87
zeros[470]^2/zeros[1]^2 -> 2990.48
zeros[471]^2/zeros[1]^2 -> 2999.43
zeros[472]^2/zeros[1]^2 -> 3006.65
zeros[473]^2/zeros[1]^2 -> 3014.04
zeros[474]^2/zeros[1]^2 -> 3024.14
zeros[475]^2/zeros[1]^2 -> 3038.61
zeros[476]^2/zeros[1]^2 -> 3047.92
zeros[477]^2/zeros[1]^2 -> 3061.9
zeros[478]^2/zeros[1]^2 -> 3065.51
zeros[479]^2/zeros[1]^2 -> 3078.77
zeros[480]^2/zeros[1]^2 -> 3090.17
zeros[481]^2/zeros[1]^2 -> 3095.85
zeros[482]^2/zeros[1]^2 -> 3103.78
zeros[483]^2/zeros[1]^2 -> 3124.24
zeros[484]^2/zeros[1]^2 -> 3130.35
zeros[485]^2/zeros[1]^2 -> 3143
zeros[486]^2/zeros[1]^2 -> 3146.66
zeros[487]^2/zeros[1]^2 -> 3159.33
zeros[488]^2/zeros[1]^2 -> 3168.27
zeros[489]^2/zeros[1]^2 -> 3181.48
zeros[490]^2/zeros[1]^2 -> 3193.01
zeros[491]^2/zeros[1]^2 -> 3200.59
zeros[492]^2/zeros[1]^2 -> 3216.22
zeros[493]^2/zeros[1]^2 -> 3223.75
zeros[494]^2/zeros[1]^2 -> 3229.38
zeros[495]^2/zeros[1]^2 -> 3241.61
zeros[496]^2/zeros[1]^2 -> 3250.47
zeros[497]^2/zeros[1]^2 -> 3268.97
zeros[498]^2/zeros[1]^2 -> 3277.44
zeros[499]^2/zeros[1]^2 -> 3284.6
zeros[500]^2/zeros[1]^2 -> 3293.55
zeros[501]^2/zeros[1]^2 -> 3306.45
zeros[502]^2/zeros[1]^2 -> 3316.83
zeros[503]^2/zeros[1]^2 -> 3323.55
zeros[504]^2/zeros[1]^2 -> 3338.72
zeros[505]^2/zeros[1]^2 -> 3352.25
zeros[506]^2/zeros[1]^2 -> 3359
zeros[507]^2/zeros[1]^2 -> 3371.45
zeros[508]^2/zeros[1]^2 -> 3379.61
zeros[509]^2/zeros[1]^2 -> 3383.59
zeros[510]^2/zeros[1]^2 -> 3402.78
zeros[511]^2/zeros[1]^2 -> 3415.28
zeros[512]^2/zeros[1]^2 -> 3422.45
zeros[513]^2/zeros[1]^2 -> 3434.34
```

```
zeros[514]^2/zeros[1]^2 -> 3443.44
zeros[515]^2/zeros[1]^2 -> 3455.56
zeros[516]^2/zeros[1]^2 -> 3463.08
zeros[517]^2/zeros[1]^2 -> 3473.11
zeros[518]^2/zeros[1]^2 -> 3486.87
zeros[519]^2/zeros[1]^2 -> 3503.95
zeros[520]^2/zeros[1]^2 -> 3509.43
zeros[521]^2/zeros[1]^2 -> 3516.99
zeros[522]^2/zeros[1]^2 -> 3527.21
zeros[523]^2/zeros[1]^2 -> 3540.42
zeros[524]^2/zeros[1]^2 -> 3548.89
zeros[525]^2/zeros[1]^2 -> 3566.82
zeros[526]^2/zeros[1]^2 -> 3572.23
zeros[527]^2/zeros[1]^2 -> 3583.98
zeros[528]^2/zeros[1]^2 -> 3599.05
zeros[529]^2/zeros[1]^2 -> 3603.45
zeros[530]^2/zeros[1]^2 -> 3615.12
zeros[531]^2/zeros[1]^2 -> 3621.78
zeros[532]^2/zeros[1]^2 -> 3643.25
zeros[533]^2/zeros[1]^2 -> 3651.22
zeros[534]^2/zeros[1]^2 -> 3661.41
zeros[535]^2/zeros[1]^2 -> 3671.67
zeros[536]^2/zeros[1]^2 -> 3678.76
zeros[537]^2/zeros[1]^2 -> 3692.45
zeros[538]^2/zeros[1]^2 -> 3705.41
zeros[539]^2/zeros[1]^2 -> 3711.97
zeros[540]^2/zeros[1]^2 -> 3729.39
zeros[541]^2/zeros[1]^2 -> 3739.34
zeros[542]^2/zeros[1]^2 -> 3750.2
zeros[543]^2/zeros[1]^2 -> 3757.39
zeros[544]^2/zeros[1]^2 -> 3768.41
zeros[545]^2/zeros[1]^2 -> 3776.9
zeros[546]^2/zeros[1]^2 -> 3795.85
zeros[547]^2/zeros[1]^2 -> 3807.56
zeros[548]^2/zeros[1]^2 -> 3815.51
zeros[549]^2/zeros[1]^2 -> 3822.58
zeros[550]^2/zeros[1]^2 -> 3840.78
zeros[551]^2/zeros[1]^2 -> 3846.17
zeros[552]^2/zeros[1]^2 -> 3855.43
zeros[553]^2/zeros[1]^2 -> 3870.61
zeros[554]^2/zeros[1]^2 -> 3883.42
zeros[555]^2/zeros[1]^2 -> 3897.11
zeros[556]^2/zeros[1]^2 -> 3906.34
zeros[557]^2/zeros[1]^2 -> 3913.14
zeros[558]^2/zeros[1]^2 -> 3922.65
zeros[559]^2/zeros[1]^2 -> 3936.66
zeros[560]^2/zeros[1]^2 -> 3951.08
zeros[561]^2/zeros[1]^2 -> 3962.3
zeros[562]^2/zeros[1]^2 -> 3971.9
zeros[563]^2/zeros[1]^2 -> 3985.94
zeros[564]^2/zeros[1]^2 -> 3992.49
zeros[565]^2/zeros[1]^2 -> 4008.31
zeros[566]^2/zeros[1]^2 -> 4012.89
zeros[567]^2/zeros[1]^2 -> 4023.96
zeros[568]^2/zeros[1]^2 -> 4047.24
zeros[569]^2/zeros[1]^2 -> 4052.98
zeros[570]^2/zeros[1]^2 -> 4061.91
zeros[571]^2/zeros[1]^2 -> 4074.48
zeros[572]^2/zeros[1]^2 -> 4082.22
zeros[573]^2/zeros[1]^2 -> 4096.73
zeros[574]^2/zeros[1]^2 -> 4106.94
zeros[575]^2/zeros[1]^2 -> 4123.52
zeros[576]^2/zeros[1]^2 -> 4129.68
zeros[577]^2/zeros[1]^2 -> 4146.54
```

```
zeros[578]^2/zeros[1]^2 -> 4156.1
zeros[579]^2/zeros[1]^2 -> 4166.1
zeros[580]^2/zeros[1]^2 -> 4170.61
zeros[581]^2/zeros[1]^2 -> 4188.04
zeros[582]^2/zeros[1]^2 -> 4202.94
zeros[583]^2/zeros[1]^2 -> 4216.43
zeros[584]^2/zeros[1]^2 -> 4225.73
zeros[585]^2/zeros[1]^2 -> 4231.36
zeros[586]^2/zeros[1]^2 -> 4247.1
zeros[587]^2/zeros[1]^2 -> 4259.5
zeros[588]^2/zeros[1]^2 -> 4266.75
zeros[589]^2/zeros[1]^2 -> 4280.51
zeros[590]^2/zeros[1]^2 -> 4296.99
zeros[591]^2/zeros[1]^2 -> 4309.05
zeros[592]^2/zeros[1]^2 -> 4316.6
zeros[593]^2/zeros[1]^2 -> 4327.86
zeros[594]^2/zeros[1]^2 -> 4338.44
zeros[595]^2/zeros[1]^2 -> 4346.3
zeros[596]^2/zeros[1]^2 -> 4369.96
zeros[597]^2/zeros[1]^2 -> 4375.67
zeros[598]^2/zeros[1]^2 -> 4387.22
zeros[599]^2/zeros[1]^2 -> 4399.45
zeros[600]^2/zeros[1]^2 -> 4413.46
zeros[601]^2/zeros[1]^2 -> 4419.44
zeros[602]^2/zeros[1]^2 -> 4433.53
zeros[603]^2/zeros[1]^2 -> 4441.97
zeros[604]^2/zeros[1]^2 -> 4462.13
zeros[605]^2/zeros[1]^2 -> 4472.96
zeros[606]^2/zeros[1]^2 -> 4486.53
zeros[607]^2/zeros[1]^2 -> 4489.5
zeros[608]^2/zeros[1]^2 -> 4501.52
zeros[609]^2/zeros[1]^2 -> 4518.67
zeros[610]^2/zeros[1]^2 -> 4527.06
zeros[611]^2/zeros[1]^2 -> 4543.21
zeros[612]^2/zeros[1]^2 -> 4556.59
zeros[613]^2/zeros[1]^2 -> 4563.28
zeros[614]^2/zeros[1]^2 -> 4580.94
zeros[615]^2/zeros[1]^2 -> 4588.94
zeros[616]^2/zeros[1]^2 -> 4597.61
zeros[617]^2/zeros[1]^2 -> 4607.64
zeros[618]^2/zeros[1]^2 -> 4628.89
zeros[619]^2/zeros[1]^2 -> 4643.46
zeros[620]^2/zeros[1]^2 -> 4647.18
zeros[621]^2/zeros[1]^2 -> 4661.55
zeros[622]^2/zeros[1]^2 -> 4671.74
zeros[623]^2/zeros[1]^2 -> 4683.94
zeros[624]^2/zeros[1]^2 -> 4696.2
zeros[625]^2/zeros[1]^2 -> 4710.65
zeros[626]^2/zeros[1]^2 -> 4719.84
zeros[627]^2/zeros[1]^2 -> 4740.42
zeros[628]^2/zeros[1]^2 -> 4747.12
zeros[629]^2/zeros[1]^2 -> 4755.91
zeros[630]^2/zeros[1]^2 -> 4769.62
zeros[631]^2/zeros[1]^2 -> 4776.84
zeros[632]^2/zeros[1]^2 -> 4794.94
zeros[633]^2/zeros[1]^2 -> 4812.71
zeros[634]^2/zeros[1]^2 -> 4819.69
zeros[635]^2/zeros[1]^2 -> 4830.58
zeros[636]^2/zeros[1]^2 -> 4842.17
zeros[637]^2/zeros[1]^2 -> 4858.06
zeros[638]^2/zeros[1]^2 -> 4867.37
zeros[639]^2/zeros[1]^2 -> 4873.54
zeros[640]^2/zeros[1]^2 -> 4895.66
zeros[641]^2/zeros[1]^2 -> 4907.86
```

```
zeros[642]^2/zeros[1]^2 -> 4919.27
zeros[643]^2/zeros[1]^2 -> 4932.72
zeros[644]^2/zeros[1]^2 -> 4937.55
zeros[645]^2/zeros[1]^2 -> 4949.39
zeros[646]^2/zeros[1]^2 -> 4967.33
zeros[647]^2/zeros[1]^2 -> 4980.37
zeros[648]^2/zeros[1]^2 -> 4993.51
zeros[649]^2/zeros[1]^2 -> 5003.16
zeros[650]^2/zeros[1]^2 -> 5018.76
zeros[651]^2/zeros[1]^2 -> 5029.34
zeros[652]^2/zeros[1]^2 -> 5038.01
zeros[653]^2/zeros[1]^2 -> 5052.15
zeros[654]^2/zeros[1]^2 -> 5060.89
zeros[655]^2/zeros[1]^2 -> 5085.72
zeros[656]^2/zeros[1]^2 -> 5093.68
zeros[657]^2/zeros[1]^2 -> 5103.89
zeros[658]^2/zeros[1]^2 -> 5111.61
zeros[659]^2/zeros[1]^2 -> 5130.25
zeros[660]^2/zeros[1]^2 -> 5136.82
zeros[661]^2/zeros[1]^2 -> 5153.37
zeros[662]^2/zeros[1]^2 -> 5167.31
zeros[663]^2/zeros[1]^2 -> 5179.58
zeros[664]^2/zeros[1]^2 -> 5193.23
zeros[665]^2/zeros[1]^2 -> 5206.56
zeros[666]^2/zeros[1]^2 -> 5216.83
zeros[667]^2/zeros[1]^2 -> 5223.24
zeros[668]^2/zeros[1]^2 -> 5236.96
zeros[669]^2/zeros[1]^2 -> 5261.36
zeros[670]^2/zeros[1]^2 -> 5265.9
zeros[671]^2/zeros[1]^2 -> 5283.99
zeros[672]^2/zeros[1]^2 -> 5290.79
zeros[673]^2/zeros[1]^2 -> 5302.1
zeros[674]^2/zeros[1]^2 -> 5319.32
zeros[675]^2/zeros[1]^2 -> 5328.98
zeros[676]^2/zeros[1]^2 -> 5339.11
zeros[677]^2/zeros[1]^2 -> 5357.73
zeros[678]^2/zeros[1]^2 -> 5374.14
zeros[679]^2/zeros[1]^2 -> 5382.74
zeros[680]^2/zeros[1]^2 -> 5393.78
zeros[681]^2/zeros[1]^2 -> 5404.07
zeros[682]^2/zeros[1]^2 -> 5416.42
zeros[683]^2/zeros[1]^2 -> 5430.57
zeros[684]^2/zeros[1]^2 -> 5451.47
zeros[685]^2/zeros[1]^2 -> 5460.78
zeros[686]^2/zeros[1]^2 -> 5466.97
zeros[687]^2/zeros[1]^2 -> 5487.74
zeros[688]^2/zeros[1]^2 -> 5497.14
zeros[689]^2/zeros[1]^2 -> 5507.29
zeros[690]^2/zeros[1]^2 -> 5518.24
zeros[691]^2/zeros[1]^2 -> 5534.87
zeros[692]^2/zeros[1]^2 -> 5552.45
zeros[693]^2/zeros[1]^2 -> 5568.65
zeros[694]^2/zeros[1]^2 -> 5570.98
zeros[695]^2/zeros[1]^2 -> 5588.81
zeros[696]^2/zeros[1]^2 -> 5593.16
zeros[697]^2/zeros[1]^2 -> 5614.7
zeros[698]^2/zeros[1]^2 -> 5625.37
zeros[699]^2/zeros[1]^2 -> 5639.83
zeros[700]^2/zeros[1]^2 -> 5654.87
zeros[701]^2/zeros[1]^2 -> 5667.18
zeros[702]^2/zeros[1]^2 -> 5678.37
zeros[703]^2/zeros[1]^2 -> 5692.68
zeros[704]^2/zeros[1]^2 -> 5702.89
zeros[705]^2/zeros[1]^2 -> 5708.99
```

```
zeros[706]^2/zeros[1]^2 -> 5736.24
zeros[707]^2/zeros[1]^2 -> 5747.85
zeros[708]^2/zeros[1]^2 -> 5757.79
zeros[709]^2/zeros[1]^2 -> 5768.81
zeros[710]^2/zeros[1]^2 -> 5781.47
zeros[711]^2/zeros[1]^2 -> 5797.82
zeros[712]^2/zeros[1]^2 -> 5804.91
zeros[713]^2/zeros[1]^2 -> 5823.5
zeros[714]^2/zeros[1]^2 -> 5836.06
zeros[715]^2/zeros[1]^2 -> 5850.78
zeros[716]^2/zeros[1]^2 -> 5870.08
zeros[717]^2/zeros[1]^2 -> 5873.8
zeros[718]^2/zeros[1]^2 -> 5883.43
zeros[719]^2/zeros[1]^2 -> 5899.34
zeros[720]^2/zeros[1]^2 -> 5913.08
zeros[721]^2/zeros[1]^2 -> 5933.16
zeros[722]^2/zeros[1]^2 -> 5944.5
zeros[723]^2/zeros[1]^2 -> 5956.15
zeros[724]^2/zeros[1]^2 -> 5965.61
zeros[725]^2/zeros[1]^2 -> 5984.33
zeros[726]^2/zeros[1]^2 -> 5993.57
zeros[727]^2/zeros[1]^2 -> 6006.16
zeros[728]^2/zeros[1]^2 -> 6016.79
zeros[729]^2/zeros[1]^2 -> 6043.59
zeros[730]^2/zeros[1]^2 -> 6049.31
zeros[731]^2/zeros[1]^2 -> 6062.67
zeros[732]^2/zeros[1]^2 -> 6076.61
zeros[733]^2/zeros[1]^2 -> 6084.48
zeros[734]^2/zeros[1]^2 -> 6097.51
zeros[735]^2/zeros[1]^2 -> 6118.36
zeros[736]^2/zeros[1]^2 -> 6131.17
zeros[737]^2/zeros[1]^2 -> 6142.26
zeros[738]^2/zeros[1]^2 -> 6157.62
zeros[739]^2/zeros[1]^2 -> 6171.9
zeros[740]^2/zeros[1]^2 -> 6183.01
zeros[741]^2/zeros[1]^2 -> 6194.03
zeros[742]^2/zeros[1]^2 -> 6204.77
zeros[743]^2/zeros[1]^2 -> 6223.37
zeros[744]^2/zeros[1]^2 -> 6242.61
zeros[745]^2/zeros[1]^2 -> 6255.79
zeros[746]^2/zeros[1]^2 -> 6263.83
zeros[747]^2/zeros[1]^2 -> 6272.67
zeros[748]^2/zeros[1]^2 -> 6291.54
zeros[749]^2/zeros[1]^2 -> 6306.17
zeros[750]^2/zeros[1]^2 -> 6313.4
zeros[751]^2/zeros[1]^2 -> 6338.31
zeros[752]^2/zeros[1]^2 -> 6343.36
zeros[753]^2/zeros[1]^2 -> 6364.73
zeros[754]^2/zeros[1]^2 -> 6373.45
zeros[755]^2/zeros[1]^2 -> 6388.13
zeros[756]^2/zeros[1]^2 -> 6395.63
zeros[757]^2/zeros[1]^2 -> 6408.12
zeros[758]^2/zeros[1]^2 -> 6433.22
zeros[759]^2/zeros[1]^2 -> 6446.58
zeros[760]^2/zeros[1]^2 -> 6454.27
zeros[761]^2/zeros[1]^2 -> 6469.82
zeros[762]^2/zeros[1]^2 -> 6483.74
zeros[763]^2/zeros[1]^2 -> 6493.32
zeros[764]^2/zeros[1]^2 -> 6513.06
zeros[765]^2/zeros[1]^2 -> 6519.21
zeros[766]^2/zeros[1]^2 -> 6537.48
zeros[767]^2/zeros[1]^2 -> 6559.51
zeros[768]^2/zeros[1]^2 -> 6567.56
zeros[769]^2/zeros[1]^2 -> 6580.09
```

```
zeros[770]^2/zeros[1]^2 -> 6590.71
zeros[771]^2/zeros[1]^2 -> 6603.5
zeros[772]^2/zeros[1]^2 -> 6619.24
zeros[773]^2/zeros[1]^2 -> 6637.44
zeros[774]^2/zeros[1]^2 -> 6653.36
zeros[775]^2/zeros[1]^2 -> 6664.3
zeros[776]^2/zeros[1]^2 -> 6673.62
zeros[777]^2/zeros[1]^2 -> 6695.88
zeros[778]^2/zeros[1]^2 -> 6705.27
zeros[779]^2/zeros[1]^2 -> 6711.87
zeros[780]^2/zeros[1]^2 -> 6729.03
zeros[781]^2/zeros[1]^2 -> 6751.28
zeros[782]^2/zeros[1]^2 -> 6763.97
zeros[783]^2/zeros[1]^2 -> 6778.1
zeros[784]^2/zeros[1]^2 -> 6790.18
zeros[785]^2/zeros[1]^2 -> 6796.41
zeros[786]^2/zeros[1]^2 -> 6815.93
zeros[787]^2/zeros[1]^2 -> 6829.28
zeros[788]^2/zeros[1]^2 -> 6848.15
zeros[789]^2/zeros[1]^2 -> 6857.11
zeros[790]^2/zeros[1]^2 -> 6876.54
zeros[791]^2/zeros[1]^2 -> 6890.45
zeros[792]^2/zeros[1]^2 -> 6901.34
zeros[793]^2/zeros[1]^2 -> 6912.9
zeros[794]^2/zeros[1]^2 -> 6929.58
zeros[795]^2/zeros[1]^2 -> 6935.16
zeros[796]^2/zeros[1]^2 -> 6965.77
zeros[797]^2/zeros[1]^2 -> 6977.02
zeros[798]^2/zeros[1]^2 -> 6984.28
zeros[799]^2/zeros[1]^2 -> 6999.84
zeros[800]^2/zeros[1]^2 -> 7013.23
zeros[801]^2/zeros[1]^2 -> 7030.34
zeros[802]^2/zeros[1]^2 -> 7038.88
zeros[803]^2/zeros[1]^2 -> 7056.34
zeros[804]^2/zeros[1]^2 -> 7074.31
zeros[805]^2/zeros[1]^2 -> 7087.49
zeros[806]^2/zeros[1]^2 -> 7105.6
zeros[807]^2/zeros[1]^2 -> 7114.38
zeros[808]^2/zeros[1]^2 -> 7127.58
zeros[809]^2/zeros[1]^2 -> 7133.95
zeros[810]^2/zeros[1]^2 -> 7160
zeros[811]^2/zeros[1]^2 -> 7172.42
zeros[812]^2/zeros[1]^2 -> 7191.78
zeros[813]^2/zeros[1]^2 -> 7199.82
zeros[814]^2/zeros[1]^2 -> 7213.95
zeros[815]^2/zeros[1]^2 -> 7229.31
zeros[816]^2/zeros[1]^2 -> 7245.29
zeros[817]^2/zeros[1]^2 -> 7253.94
zeros[818]^2/zeros[1]^2 -> 7267.56
zeros[819]^2/zeros[1]^2 -> 7290.32
zeros[820]^2/zeros[1]^2 -> 7309.67
zeros[821]^2/zeros[1]^2 -> 7315.94
zeros[822]^2/zeros[1]^2 -> 7326.94
zeros[823]^2/zeros[1]^2 -> 7345.34
zeros[824]^2/zeros[1]^2 -> 7353.8
zeros[825]^2/zeros[1]^2 -> 7371.83
zeros[826]^2/zeros[1]^2 -> 7393.61
zeros[827]^2/zeros[1]^2 -> 7403.27
zeros[828]^2/zeros[1]^2 -> 7415.34
zeros[829]^2/zeros[1]^2 -> 7438.21
zeros[830]^2/zeros[1]^2 -> 7445.1
zeros[831]^2/zeros[1]^2 -> 7459.78
zeros[832]^2/zeros[1]^2 -> 7470.49
zeros[833]^2/zeros[1]^2 -> 7485.91
```

```
zeros[834]^2/zeros[1]^2 -> 7511.22
zeros[835]^2/zeros[1]^2 -> 7521.48
zeros[836]^2/zeros[1]^2 -> 7538.39
zeros[837]^2/zeros[1]^2 -> 7546.81
zeros[838]^2/zeros[1]^2 -> 7557.58
zeros[839]^2/zeros[1]^2 -> 7579.63
zeros[840]^2/zeros[1]^2 -> 7591.68
zeros[841]^2/zeros[1]^2 -> 7603.61
zeros[842]^2/zeros[1]^2 -> 7625.2
zeros[843]^2/zeros[1]^2 -> 7640.34
zeros[844]^2/zeros[1]^2 -> 7651.43
zeros[845]^2/zeros[1]^2 -> 7670.98
zeros[846]^2/zeros[1]^2 -> 7676.92
zeros[847]^2/zeros[1]^2 -> 7689.74
zeros[848]^2/zeros[1]^2 -> 7706.16
zeros[849]^2/zeros[1]^2 -> 7734.32
zeros[850]^2/zeros[1]^2 -> 7740.05
zeros[851]^2/zeros[1]^2 -> 7756.4
zeros[852]^2/zeros[1]^2 -> 7766.43
zeros[853]^2/zeros[1]^2 -> 7787.85
zeros[854]^2/zeros[1]^2 -> 7796.48
zeros[855]^2/zeros[1]^2 -> 7810.19
zeros[856]^2/zeros[1]^2 -> 7829.11
zeros[857]^2/zeros[1]^2 -> 7841.48
zeros[858]^2/zeros[1]^2 -> 7866.73
zeros[859]^2/zeros[1]^2 -> 7876.24
zeros[860]^2/zeros[1]^2 -> 7888.51
zeros[861]^2/zeros[1]^2 -> 7898.23
zeros[862]^2/zeros[1]^2 -> 7915.34
zeros[863]^2/zeros[1]^2 -> 7930.94
zeros[864]^2/zeros[1]^2 -> 7950.67
zeros[865]^2/zeros[1]^2 -> 7966.67
zeros[866]^2/zeros[1]^2 -> 7978.61
zeros[867]^2/zeros[1]^2 -> 7992.77
zeros[868]^2/zeros[1]^2 -> 8008.98
zeros[869]^2/zeros[1]^2 -> 8024.45
zeros[870]^2/zeros[1]^2 -> 8037.4
zeros[871]^2/zeros[1]^2 -> 8042.1
zeros[872]^2/zeros[1]^2 -> 8074.47
zeros[873]^2/zeros[1]^2 -> 8087.39
zeros[874]^2/zeros[1]^2 -> 8099.47
zeros[875]^2/zeros[1]^2 -> 8114.47
zeros[876]^2/zeros[1]^2 -> 8126.39
zeros[877]^2/zeros[1]^2 -> 8137.82
zeros[878]^2/zeros[1]^2 -> 8160.18
zeros[879]^2/zeros[1]^2 -> 8171.95
zeros[880]^2/zeros[1]^2 -> 8192.05
zeros[881]^2/zeros[1]^2 -> 8202.59
zeros[882]^2/zeros[1]^2 -> 8224.04
zeros[883]^2/zeros[1]^2 -> 8239.08
zeros[884]^2/zeros[1]^2 -> 8243.38
zeros[885]^2/zeros[1]^2 -> 8262.92
zeros[886]^2/zeros[1]^2 -> 8273.73
zeros[887]^2/zeros[1]^2 -> 8295.81
zeros[888]^2/zeros[1]^2 -> 8318.45
zeros[889]^2/zeros[1]^2 -> 8330.58
zeros[890]^2/zeros[1]^2 -> 8334.62
zeros[891]^2/zeros[1]^2 -> 8354.37
zeros[892]^2/zeros[1]^2 -> 8374.41
zeros[893]^2/zeros[1]^2 -> 8382.5
zeros[894]^2/zeros[1]^2 -> 8398.66
zeros[895]^2/zeros[1]^2 -> 8417.28
zeros[896]^2/zeros[1]^2 -> 8436.19
zeros[897]^2/zeros[1]^2 -> 8451.12
```

```
zeros[898]^2/zeros[1]^2 -> 8465.24
zeros[899]^2/zeros[1]^2 -> 8478.34
zeros[900]^2/zeros[1]^2 -> 8489.43
zeros[901]^2/zeros[1]^2 -> 8501.51
zeros[902]^2/zeros[1]^2 -> 8529.3
zeros[903]^2/zeros[1]^2 -> 8543.77
zeros[904]^2/zeros[1]^2 -> 8553.7
zeros[905]^2/zeros[1]^2 -> 8576.24
zeros[906]^2/zeros[1]^2 -> 8581.92
zeros[907]^2/zeros[1]^2 -> 8603.36
zeros[908]^2/zeros[1]^2 -> 8615.31
zeros[909]^2/zeros[1]^2 -> 8629.3
zeros[910]^2/zeros[1]^2 -> 8642.73
zeros[911]^2/zeros[1]^2 -> 8671.16
zeros[912]^2/zeros[1]^2 -> 8682.5
zeros[913]^2/zeros[1]^2 -> 8696.99
zeros[914]^2/zeros[1]^2 -> 8707.24
zeros[915]^2/zeros[1]^2 -> 8720.23
zeros[916]^2/zeros[1]^2 -> 8742.66
zeros[917]^2/zeros[1]^2 -> 8751
zeros[918]^2/zeros[1]^2 -> 8777.05
zeros[919]^2/zeros[1]^2 -> 8790.48
zeros[920]^2/zeros[1]^2 -> 8800.36
zeros[921]^2/zeros[1]^2 -> 8822.32
zeros[922]^2/zeros[1]^2 -> 8841.05
zeros[923]^2/zeros[1]^2 -> 8843.2
zeros[924]^2/zeros[1]^2 -> 8859.5
zeros[925]^2/zeros[1]^2 -> 8878.13
zeros[926]^2/zeros[1]^2 -> 8902.75
zeros[927]^2/zeros[1]^2 -> 8917.09
zeros[928]^2/zeros[1]^2 -> 8929.76
zeros[929]^2/zeros[1]^2 -> 8943.07
zeros[930]^2/zeros[1]^2 -> 8956.44
zeros[931]^2/zeros[1]^2 -> 8972.98
zeros[932]^2/zeros[1]^2 -> 8993.14
zeros[933]^2/zeros[1]^2 -> 9003.07
zeros[934]^2/zeros[1]^2 -> 9022.44
zeros[935]^2/zeros[1]^2 -> 9043.25
zeros[936]^2/zeros[1]^2 -> 9061.04
zeros[937]^2/zeros[1]^2 -> 9064.46
zeros[938]^2/zeros[1]^2 -> 9088.57
zeros[939]^2/zeros[1]^2 -> 9095.28
zeros[940]^2/zeros[1]^2 -> 9109.7
zeros[941]^2/zeros[1]^2 -> 9139.58
zeros[942]^2/zeros[1]^2 -> 9151.95
zeros[943]^2/zeros[1]^2 -> 9169.19
zeros[944]^2/zeros[1]^2 -> 9174.66
zeros[945]^2/zeros[1]^2 -> 9198.99
zeros[946]^2/zeros[1]^2 -> 9211.55
zeros[947]^2/zeros[1]^2 -> 9227.39
zeros[948]^2/zeros[1]^2 -> 9236.75
zeros[949]^2/zeros[1]^2 -> 9263.05
zeros[950]^2/zeros[1]^2 -> 9276.67
zeros[951]^2/zeros[1]^2 -> 9298.89
zeros[952]^2/zeros[1]^2 -> 9310.59
zeros[953]^2/zeros[1]^2 -> 9320.11
zeros[954]^2/zeros[1]^2 -> 9332.64
zeros[955]^2/zeros[1]^2 -> 9354.67
zeros[956]^2/zeros[1]^2 -> 9371.46
zeros[957]^2/zeros[1]^2 -> 9390.05
zeros[958]^2/zeros[1]^2 -> 9407.7
zeros[959]^2/zeros[1]^2 -> 9417.49
zeros[960]^2/zeros[1]^2 -> 9438.32
zeros[961]^2/zeros[1]^2 -> 9451.41
```

```
zeros[962]^2/zeros[1]^2 -> 9467.2
zeros[963]^2/zeros[1]^2 -> 9479.04
zeros[964]^2/zeros[1]^2 -> 9493.04
zeros[965]^2/zeros[1]^2 -> 9527.61
zeros[966]^2/zeros[1]^2 -> 9534.04
zeros[967]^2/zeros[1]^2 -> 9546.83
zeros[968]^2/zeros[1]^2 -> 9564.42
zeros[969]^2/zeros[1]^2 -> 9577.6
zeros[970]^2/zeros[1]^2 -> 9593.48
zeros[971]^2/zeros[1]^2 -> 9610.39
zeros[972]^2/zeros[1]^2 -> 9633.47
zeros[973]^2/zeros[1]^2 -> 9641.73
zeros[974]^2/zeros[1]^2 -> 9664.59
zeros[975]^2/zeros[1]^2 -> 9680.45
zeros[976]^2/zeros[1]^2 -> 9696.44
zeros[977]^2/zeros[1]^2 -> 9707.46
zeros[978]^2/zeros[1]^2 -> 9718.47
zeros[979]^2/zeros[1]^2 -> 9738.71
zeros[980]^2/zeros[1]^2 -> 9761.91
zeros[981]^2/zeros[1]^2 -> 9779.95
zeros[982]^2/zeros[1]^2 -> 9794
zeros[983]^2/zeros[1]^2 -> 9808.03
zeros[984]^2/zeros[1]^2 -> 9816.26
zeros[985]^2/zeros[1]^2 -> 9846.25
zeros[986]^2/zeros[1]^2 -> 9852
zeros[987]^2/zeros[1]^2 -> 9866.51
zeros[988]^2/zeros[1]^2 -> 9889.86
zeros[989]^2/zeros[1]^2 -> 9909.83
zeros[990]^2/zeros[1]^2 -> 9924.64
zeros[991]^2/zeros[1]^2 -> 9941.34
zeros[992]^2/zeros[1]^2 -> 9951.28
zeros[993]^2/zeros[1]^2 -> 9968.68
zeros[994]^2/zeros[1]^2 -> 9978.69
zeros[995]^2/zeros[1]^2 -> 10005.2
zeros[996]^2/zeros[1]^2 -> 10029.9
zeros[997]^2/zeros[1]^2 -> 10032.7
zeros[998]^2/zeros[1]^2 -> 10051.4
zeros[999]^2/zeros[1]^2 -> 10074.1
zeros[1000]^2/zeros[1]^2 -> 10084.4
zeros[2000]^2/zeros[1]^2 -> 31666.5
zeros[3000]^2/zeros[1]^2 -> 62487.5
zeros[4000]^2/zeros[1]^2 -> 101641
zeros[5000]^2/zeros[1]^2 -> 148552
zeros[6000]^2/zeros[1]^2 -> 202833
zeros[7000]^2/zeros[1]^2 -> 264160
zeros[8000]^2/zeros[1]^2 -> 332313
zeros[9000]^2/zeros[1]^2 -> 407086
zeros[10000]^2/zeros[1]^2 -> 488365
zeros[11000]^2/zeros[1]^2 -> 575866
zeros[12000]^2/zeros[1]^2 -> 669610
zeros[13000]^2/zeros[1]^2 -> 769331
zeros[14000]^2/zeros[1]^2 -> 875132
zeros[15000]^2/zeros[1]^2 -> 986706
zeros[16000]^2/zeros[1]^2 -> 1.10414e+06
zeros[17000]^2/zeros[1]^2 -> 1.22721e+06
zeros[18000]^2/zeros[1]^2 -> 1.35593e+06
zeros[19000]^2/zeros[1]^2 -> 1.49029e+06
zeros[20000]^2/zeros[1]^2 -> 1.63008e+06
zeros[21000]^2/zeros[1]^2 -> 1.77539e+06
zeros[22000]^2/zeros[1]^2 -> 1.92602e+06
zeros[23000]^2/zeros[1]^2 -> 2.08203e+06
zeros[24000]^2/zeros[1]^2 -> 2.2433e+06
zeros[25000]^2/zeros[1]^2 -> 2.40991e+06
zeros[26000]^2/zeros[1]^2 -> 2.58168e+06
```

```
zeros[27000]^2/zeros[1]^2 -> 2.75855e+06
zeros[28000]^2/zeros[1]^2 -> 2.94058e+06
zeros[29000]^2/zeros[1]^2 -> 3.12777e+06
zeros[30000]^2/zeros[1]^2 -> 3.32017e+06
zeros[31000]^2/zeros[1]^2 -> 3.51724e+06
zeros[32000]^2/zeros[1]^2 -> 3.71948e+06
zeros[33000]^2/zeros[1]^2 -> 3.92667e+06
zeros[34000]^2/zeros[1]^2 -> 4.13876e+06
zeros[35000]^2/zeros[1]^2 -> 4.35591e+06
zeros[36000]^2/zeros[1]^2 -> 4.57776e+06
zeros[37000]^2/zeros[1]^2 -> 4.80458e+06
zeros[38000]^2/zeros[1]^2 -> 5.03622e+06
zeros[39000]^2/zeros[1]^2 -> 5.27242e+06
zeros[40000]^2/zeros[1]^2 -> 5.51366e+06
zeros[41000]^2/zeros[1]^2 -> 5.75964e+06
zeros[42000]^2/zeros[1]^2 -> 6.01003e+06
zeros[43000]^2/zeros[1]^2 -> 6.26562e+06
zeros[44000]^2/zeros[1]^2 -> 6.5255e+06
zeros[45000]^2/zeros[1]^2 -> 6.79038e+06
zeros[46000]^2/zeros[1]^2 -> 7.0596e+06
zeros[47000]^2/zeros[1]^2 -> 7.33336e+06
zeros[48000]^2/zeros[1]^2 -> 7.61205e+06
zeros[49000]^2/zeros[1]^2 -> 7.89535e+06
zeros[50000]^2/zeros[1]^2 -> 8.18299e+06
zeros[51000]^2/zeros[1]^2 -> 8.47524e+06
zeros[52000]^2/zeros[1]^2 -> 8.77207e+06
zeros[53000]^2/zeros[1]^2 -> 9.07328e+06
zeros[54000]^2/zeros[1]^2 -> 9.3792e+06
zeros[55000]^2/zeros[1]^2 -> 9.68951e+06
zeros[56000]^2/zeros[1]^2 -> 1.00044e+07
zeros[57000]^2/zeros[1]^2 -> 1.03237e+07
zeros[58000]^2/zeros[1]^2 -> 1.06474e+07
zeros[59000]^2/zeros[1]^2 -> 1.09753e+07
zeros[60000]^2/zeros[1]^2 -> 1.13078e+07
zeros[61000]^2/zeros[1]^2 -> 1.16449e+07
zeros[62000]^2/zeros[1]^2 -> 1.19861e+07
zeros[63000]^2/zeros[1]^2 -> 1.23317e+07
zeros[64000]^2/zeros[1]^2 -> 1.2682e+07
zeros[65000]^2/zeros[1]^2 -> 1.30364e+07
zeros[66000]^2/zeros[1]^2 -> 1.33951e+07
zeros[67000]^2/zeros[1]^2 -> 1.37581e+07
zeros[68000]^2/zeros[1]^2 -> 1.41255e+07
zeros[69000]^2/zeros[1]^2 -> 1.44973e+07
zeros[70000]^2/zeros[1]^2 -> 1.48732e+07
zeros[71000]^2/zeros[1]^2 -> 1.52532e+07
zeros[72000]^2/zeros[1]^2 -> 1.56378e+07
zeros[73000]^2/zeros[1]^2 -> 1.60266e+07
zeros[74000]^2/zeros[1]^2 -> 1.64196e+07
zeros[75000]^2/zeros[1]^2 -> 1.68168e+07
zeros[76000]^2/zeros[1]^2 -> 1.72182e+07
zeros[77000]^2/zeros[1]^2 -> 1.76239e+07
zeros[78000]^2/zeros[1]^2 -> 1.80336e+07
zeros[79000]^2/zeros[1]^2 -> 1.84479e+07
zeros[80000]^2/zeros[1]^2 -> 1.88659e+07
zeros[81000]^2/zeros[1]^2 -> 1.92886e+07
zeros[82000]^2/zeros[1]^2 -> 1.97149e+07
zeros[83000]^2/zeros[1]^2 -> 2.01456e+07
zeros[84000]^2/zeros[1]^2 -> 2.05804e+07
zeros[85000]^2/zeros[1]^2 -> 2.10195e+07
zeros[86000]^2/zeros[1]^2 -> 2.14624e+07
zeros[87000]^2/zeros[1]^2 -> 2.19098e+07
zeros[88000]^2/zeros[1]^2 -> 2.23612e+07
zeros[89000]^2/zeros[1]^2 -> 2.28169e+07
zeros[90000]^2/zeros[1]^2 -> 2.32761e+07
```

```
zeros[91000]^2/zeros[1]^2 -> 2.37398e+07
zeros[92000]^2/zeros[1]^2 -> 2.42074e+07
zeros[93000]^2/zeros[1]^2 -> 2.46794e+07
zeros[94000]^2/zeros[1]^2 -> 2.51553e+07
zeros[95000]^2/zeros[1]^2 -> 2.56353e+07
zeros[96000]^2/zeros[1]^2 -> 2.61189e+07
zeros[97000]^2/zeros[1]^2 -> 2.66073e+07
zeros[98000]^2/zeros[1]^2 -> 2.70993e+07
zeros[99000]^2/zeros[1]^2 -> 2.7595e+07
zeros[100000]^2/zeros[1]^2 -> 2.80951e+07
```

Motifs rythmiques (Denise Vella-Chemla, 14/11/2017)

On cherche une caractérisation des nombres premiers par des motifs rythmiques, après avoir assisté, le 10 novembre 2017, à une conférence grand public d'Alain Connes à Gif-sur-Yvette, dans le cadre du programme de conférences UniverCité.

On dispose de la table de la relation *"est un résidu quadratique de"*, obtenue par programme, que Gauss "invente" dans les Recherches arithmétiques section 4 et dont il fournit un extrait (en annexe des Recherches). Dans l'extrait en question, seuls apparaissent, en tête des lignes et des colonnes, les nombres premiers. Notre programme fournit la relation t est un résidu quadratique de y pour t (entête de colonne) entier, compris entre 1 (première croix) et $y-1$, et y (entête de ligne), entier impair. t est un résidu quadratique de y signifie "il existe x compris entre 1 et $y-1$, il existe z compris entre 0 et $y-1$, tels que $x^2 - zy - t = 0$".

On voit clairement, et c'est un résultat connu de Gauss, qu'aux nombres premiers correspondent des lignes à forte densité de croix : en effet, les nombres premiers, qu'ils soient de la forme $4k+1$ ou $4k+3$, maximisent localement le nombre de résidus quadratiques puisque, pour eux, ce nombre est égal à $\frac{p-1}{2}$, alors qu'il est moindre pour les nombres composés.

De plus, les lignes, qu'on lit comme des mots booléens, des nombres premiers de la forme $4k+1$ sont des palindromes (elles se lisent identiquement de gauche à droite et de droite à gauche car x et $n-x$ sont soit tous deux résidus quadratiques soit tous deux non-résidus quadratiques).

Pour les nombres premiers de la forme $4k+3$, il y a une "anti-palindromie" des mots (x et $n-x$ sont l'un résidu quadratique et l'autre non-résidu quadratique).

On souhaiterait réduire la taille de l'information nécessitée pour caractériser les nombres premiers : au lieu de chercher les lignes "denses", on va chercher les lignes qui contiennent un motif de 5 croix successives.

On réalise avec grande surprise que cela suffit à caractériser presque tous les nombres premiers de 101 à 200, on n'en rate que 2 qui sont 149 et 193.

Ce qu'il est important d'avoir à l'esprit, c'est que le motif "5 croix consécutives" relie des équations qui semblent plutôt éloignées les unes des autres. Voyons un exemple pour illustrer cela : quand on voit 7 croix successives dans la ligne de 101, associées aux nombres 19, 20, 21, ... 25, les nombres en question

sont respectivement les carrés des nombres $25, 11, 18, 27, 15, 23$ et 5 (mod 101).

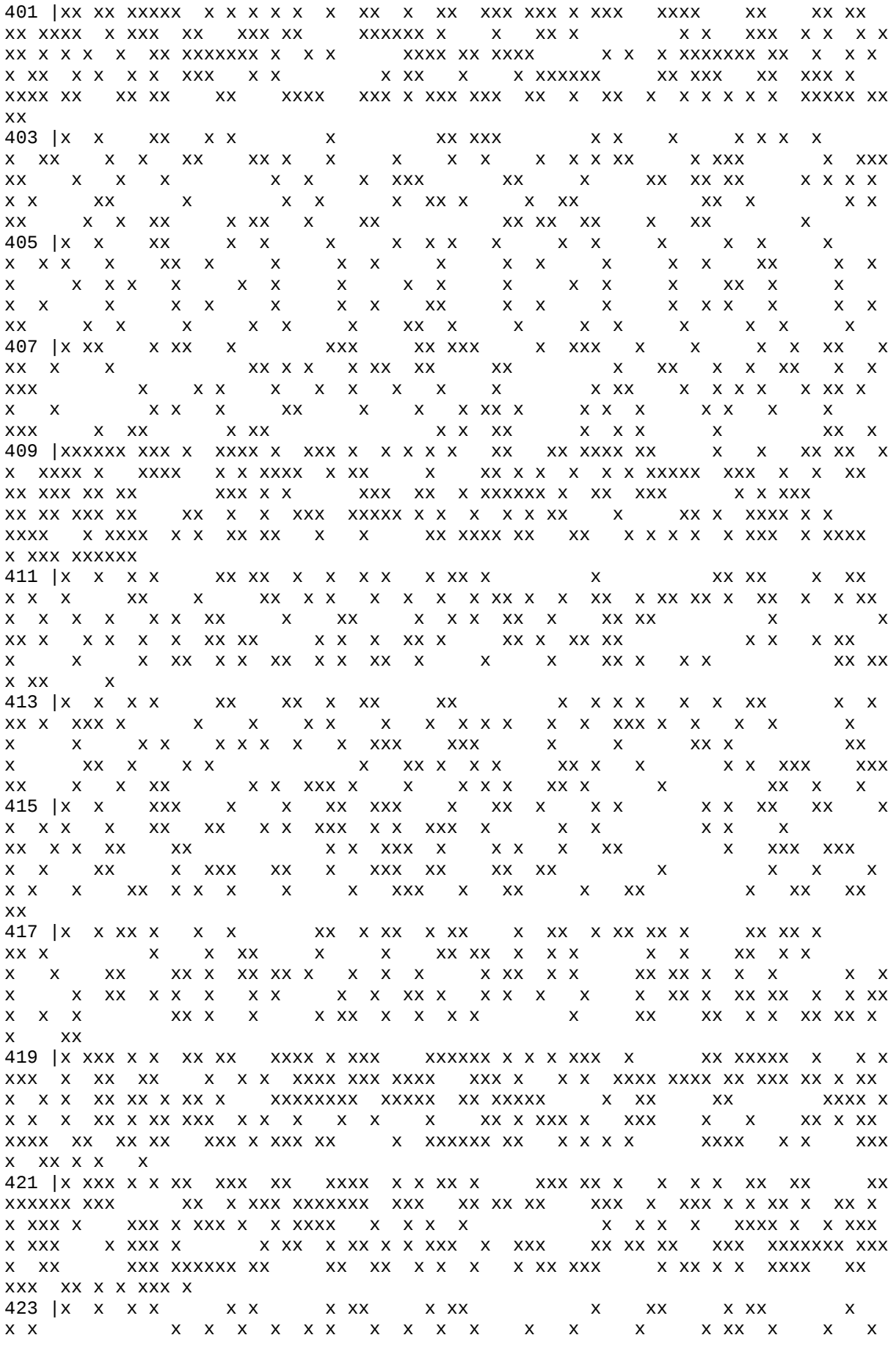
En effet, les égalités suivantes sont vérifiées :

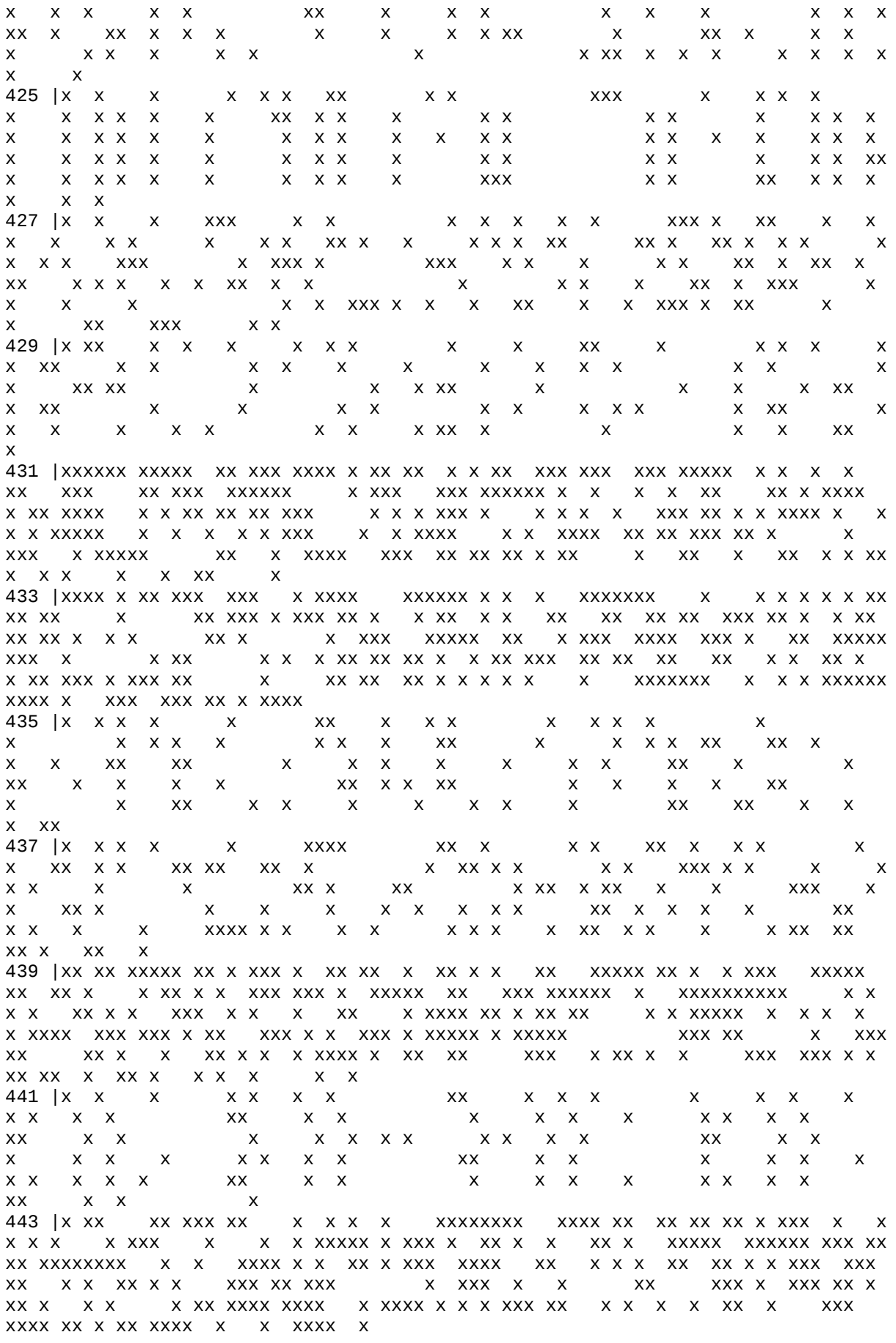
$$\begin{aligned}
25^2 - 6 \times 101 - 19 &= 0 \\
11^2 - 1 \times 101 - 20 &= 0 \\
18^2 - 3 \times 101 - 21 &= 0 \\
27^2 - 7 \times 101 - 22 &= 0 \\
15^2 - 2 \times 101 - 23 &= 0 \\
23^2 - 5 \times 101 - 24 &= 0 \\
5^2 - 0 \times 101 - 25 &= 0
\end{aligned}$$

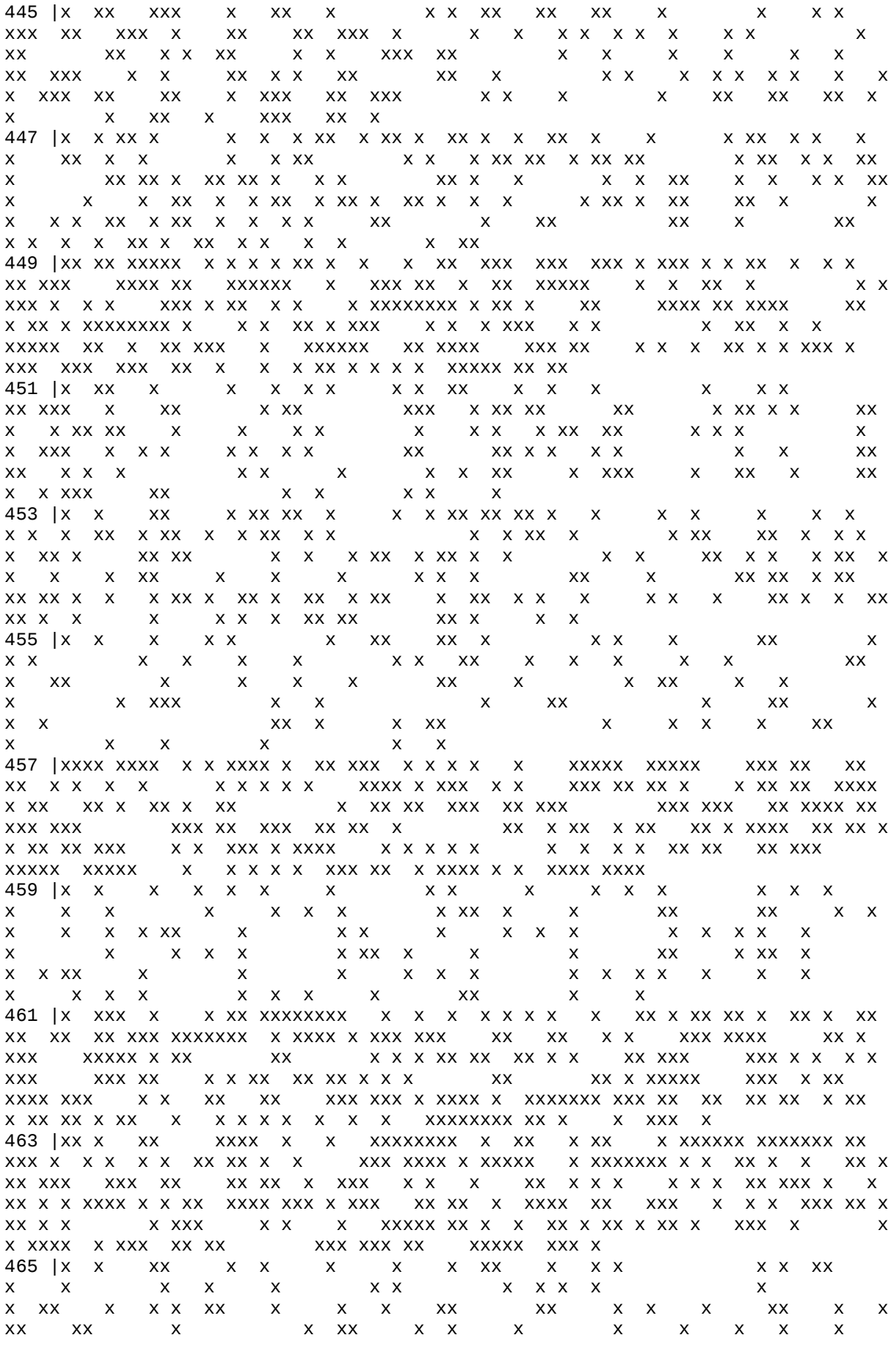
En ordonnant ces équations selon les carrés, on peut considérer que p est presque toujours premier s'il existe une succession de 4 carrés $(x_0)^2,\ (x_1)^2,\ (x_2)^2,\ (x_3)^2$, accompagnés de 4 coefficients $k_0,\ k_1,\ k_2,\ k_3$ et une variable x tels que

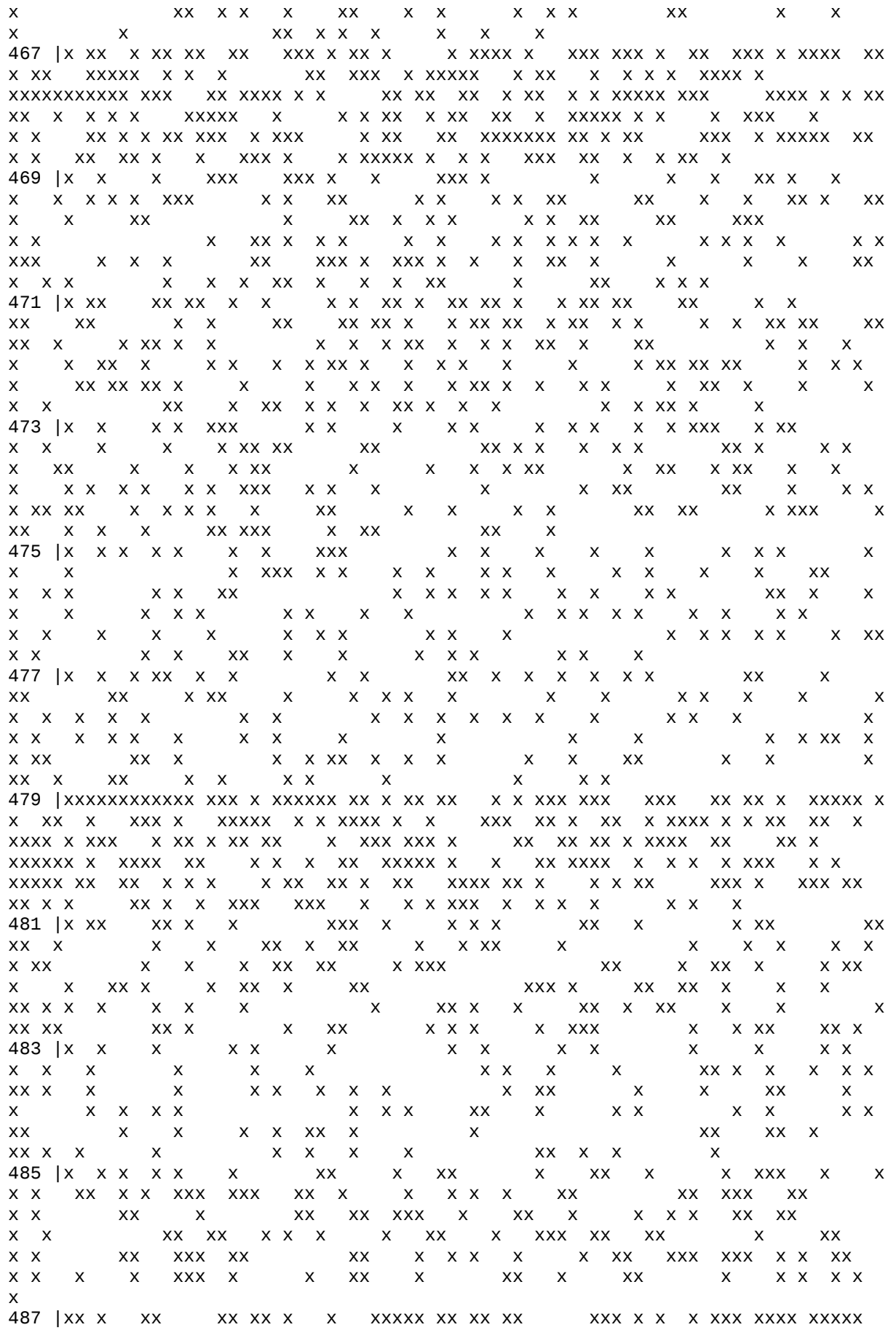
$$\begin{aligned}
(x_0)^2 &= k_0 \times p + x + 0, \\
(x_1)^2 &= k_1 \times p + x + 1, \\
(x_2)^2 &= k_2 \times p + x + 2, \\
(x_3)^2 &= k_3 \times p + x + 3.
\end{aligned}$$

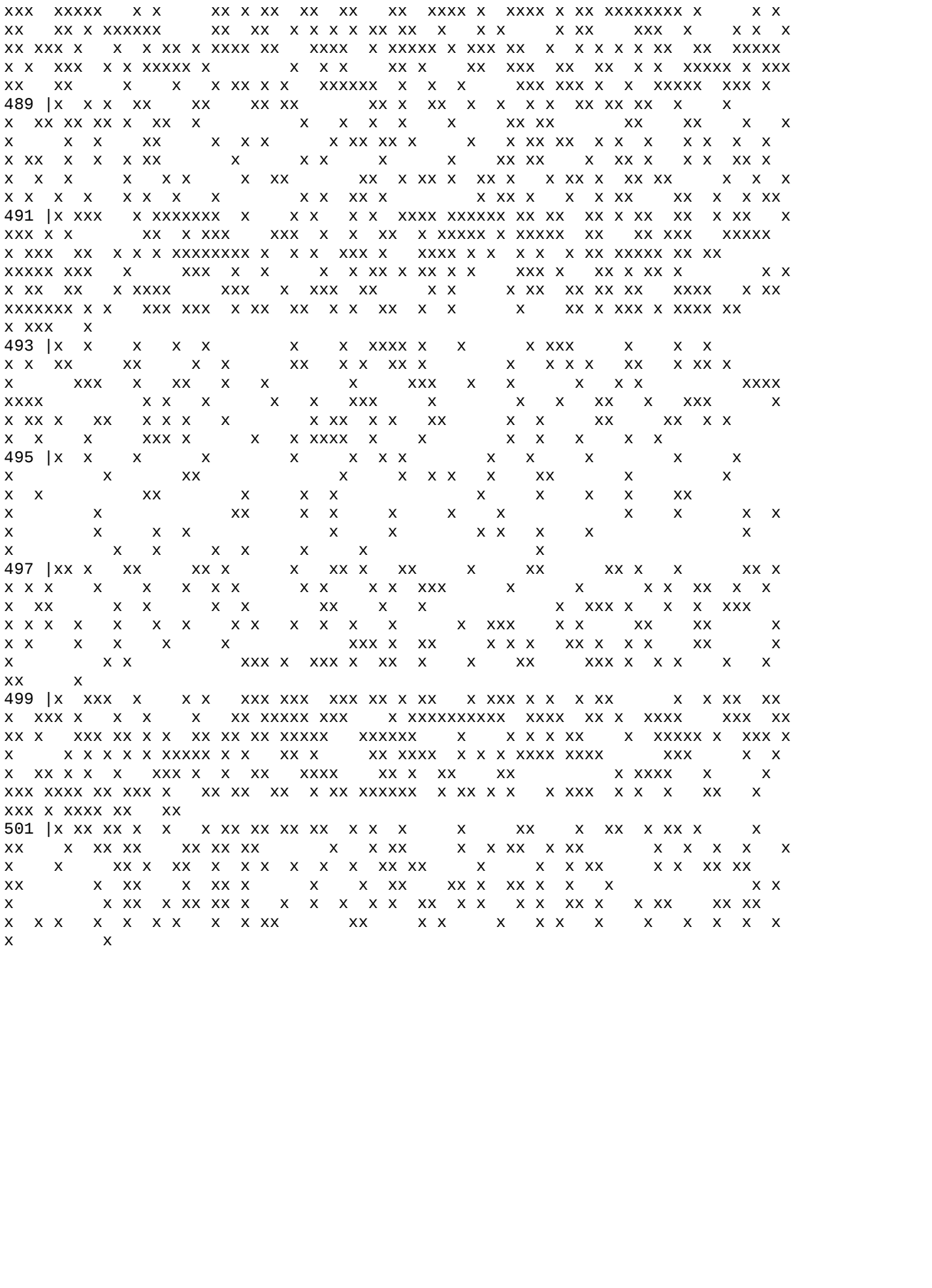
Dommage que 149 et 193 gâchent tout, c'était joli.
En programmant davantage, on infirme aussi la conjecture "il n'y a jamais plus de 3 nombres entiers consécutifs résidus quadratiques d'un nombre composé" par le contre-exemple 391, qui est un nombre composé, et dont 185, 186, 187 et 188 sont résidus quadratiques tous les 4.











Tautologies (Denise Vella-Chemla, 22/11/2017)

On voudrait revenir sur le fait que les nombres premiers établissent certaines relations entre d'autres nombres.

Habituellement, on dit qu'un nombre est premier si seuls 1 et lui-même le divisent. Un nombre composé a un diviseur différent de 1 et lui-même. 15 est composé parce que 3 le divise.

Mais on pourrait aussi dire que 15 est composé parce que 3 divise 12, c'est équivalent au fait que 3 divise 15 puisque 12 est le complémentaire de 3 à 15, c'est surprenant parce qu'on énonce quelque chose sur 15 en parlant d'une relation entre 2 autres nombres que 15.

On pourrait aussi dire que 13 est premier parce que 2 ne divise pas 11 et 3 ne divise pas 10 et 4 ne divise pas 9 et 5 ne divise pas 8 et 6 ne divise pas 7, 13 est premier parce qu'aucun nombre de 2 à 6 ne divise son complémentaire à 13. Mais c'est fastidieux et on a l'habitude d'utiliser l'expression la plus courte possible, qui pourrait être qu'aucun nombre de 2 à 6 ne divise 13, mais que l'on raccourcit encore en disant qu'aucun nombre inférieur à la racine carrée de 13 ne le divise, i.e. ni 2 ni 3 ne divisent 13.

12	11	10	9	8	7
1	2	3	4	5	6

Un nombre p premier est caractérisé par le fait qu'il a exactement $\frac{p-1}{2}$ résidus quadratiques (les nombres premiers maximisent le nombre de résidus quadratiques, tous les nombres de 1 à $\frac{p-1}{2}$ ayant des carrés différents modulo p).

Pour les nombres composés, soit il y a des redondances parmi les carrés, soit il y a des carrés nuls (par exemple pour 9), ce qui dans les deux cas rend le nombre de résidus quadratiques strictement inférieur à $\frac{p-1}{2}$.

14	13	12	11	10	9	8
1	2	3	4	5	6	7
1	4	9	1	10	6	4

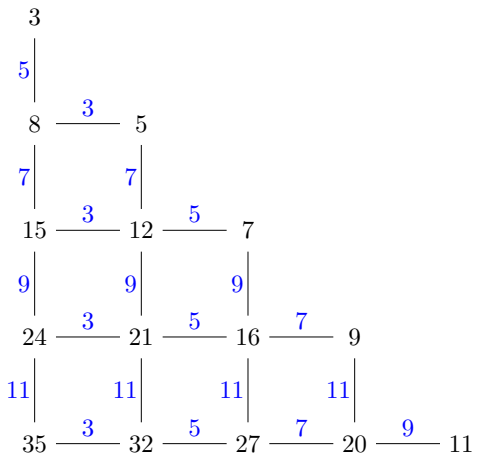
On voit dans la table que, selon le module 15, 4 et 1 ont même carré, ou bien encore 7 et 2. En effet, 15 divise $4^2 - 1^2 = (4-1)(4+1) = 3 \times 5$ ou bien 15 divise $7^2 - 2^2 = (7-2)(7+2) = 5 \times 9$.

Ca semble un peu particulier de dire que 15 est composé parce qu'il divise 3×5 ou encore parce qu'il divise 5×9 mais le fait est là, tous ces énoncés sont équivalents : 15 divise un produit de la forme $(a-b)(a+b)$ avec $1 \leqslant a < b \leqslant \frac{15-1}{2}$, ce qui équivaut au fait que 15 n'a pas $\frac{15-1}{2}$ résidus quadratiques, ce qui équivaut au fait que 15 est composé. Une redondance de carrés est équivalente à la composition du nombre mais une non-redondance de carrés ne garantit pas que le nombre est premier (existent deux carrés égaux modulo 15 et 15 est composé mais tous les carrés sont différents pour 6 ou pour 9 et 6 est composé, ou 9 est composé aussi).

On peut être exhaustif et envisager toutes les redondances éventuelles pour 13 (il y en a 21) :

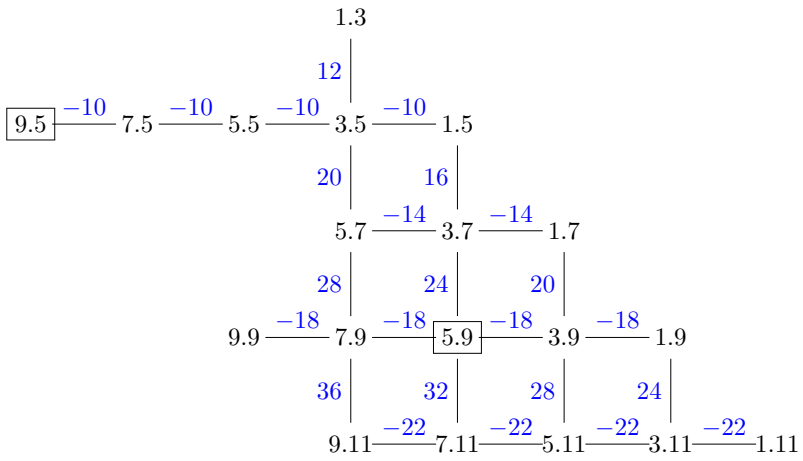
$(1,2) \rightarrow 1 \times 3 = 3$
$(1,3) \rightarrow 2 \times 4 = 8$ $(2,3) \rightarrow 1 \times 5 = 5$
$(1,4) \rightarrow 3 \times 5 = 15$ $(2,4) \rightarrow 2 \times 6 = 12$ $(3,4) \rightarrow 1 \times 7 = 7$
$(1,5) \rightarrow 4 \times 6 = 24$ $(2,5) \rightarrow 3 \times 7 = 21$ $(3,5) \rightarrow 2 \times 8 = 16$ $(4,5) \rightarrow 1 \times 9 = 9$
$(1,6) \rightarrow 5 \times 7 = 35$ $(2,6) \rightarrow 4 \times 8 = 32$ $(3,6) \rightarrow 3 \times 9 = 27$ $(4,6) \rightarrow 2 \times 10 = 20$ $(5,6) \rightarrow 1 \times 11 = 11$

13 est premier car il ne divise aucun des produits : il s'agit de produits de deux nombres différents, compris entre 1 et 11, et de différence paire. Notons dans le diagramme ci-dessous les écarts entre ces produits :



On rencontre un problème ici car, si on arrive à éliminer les nombres composés ou puissances de premiers, caractérisés par le fait que l'un des carrés est nul lorsqu'on les prend comme modules, on n'arrive pas à distinguer les doubles de premiers des nombres premiers eux-mêmes, pour qui tous les carrés sont différents et non nuls.

Diagramme de produits (Denise Vella-Chemla, 25/11/2017)



Les produits $a.b$ et $b.a$ dans ce diagramme (voir 5.9 et 9.5 encadrés) sont sommets de rectangles de longueur $\Delta = |b - a|$ et largeur $\Delta/2$. On peut observer les nombres écrits sur les traits de passages, qui sont des différences, des sortes de dérivées de fonctions, et que l'on peut lier entre eux en calculant des différences de différences, sortes de dérivées secondes[1]. Les verticales du diagramme contiennent des couples à différence de coordonnées constante.

Les nombres premiers ont pour caractéristique de n'avoir que 2 points leur correspondant dans ce diagramme : les points $1.p$ et $p.1$.

[1] ici, $+8$ pour les verticales, et identité pour les horizontales. Peut-être y aurait-il un lien avec la formule de Galois $E'F'' - E''F' = \frac{\pi}{2}\sqrt{-1}$

Carrés points fixes des nombres composés (Denise Vella-Chemla, 29/11/2017)

On découvre à la recherche de points fixes dans les tables de résiduosité quadratique qu'on peut distinguer les nombres composés n avec ou sans facteur carré en cherchant deux carrés particuliers modulo n de la façon suivante :

- si n est un nombre composé qui n'est pas une puissance de premier, on trouve toujours modulo n deux entiers consécutifs a et $a+1$, inférieurs ou égaux à $\left\lfloor \frac{n-1}{2} \right\rfloor$ qui ont pour carré l'un lui-même et l'autre son complément à n ; n divise le produit de ces deux nombres ; les deux nombres consécutifs en question vérifient deux équations quadratiques équivalentes modulo n ;
- si n est un nombre composé puissance de premier, un nombre inférieur ou égal à $\left\lfloor \frac{n-1}{2} \right\rfloor$ est de carré nul et on ne semble pas trouver de points fixes tels que notés ci-dessus.

On fournit ci-dessous les nombres consécutifs pour les composés sans facteur carré inférieurs à 100.

$15 : 5, 6$
$21 : 6, 7$
$33 : 11, 12$
$35 : 14, 15$
$39 : 12, 13$
$45 : 9, 10$
$51 : 17, 18$
$55 : 10, 11$
$57 : 18, 19$
$65 : 25, 26$
$69 : 23, 24$
$77 : 21, 22$
$85 : 34, 35$
$87 : 29, 30$
$91 : 13, 14$
$93 : 30, 31$
$95 : 19, 20$

Par programme, on vérifie que :

- les nombres premiers (qu'ils soient de la forme $4k+1$ ou $4k+3$) n'ont pas de carrés points fixes ; si on identifie x à $p-x$ (si on quotiente par une relation $x \equiv p-x$), modulo les premiers $4k+3$, l'élévation au carré réalise simplement une permutation des nombres inférieurs ou égaux à $(p-1)/2$ tandis que modulo les premiers $4k+1$, l'élévation au carré associe une même image aux nombres 2 par 2 (modulo 11, on a la permutation $\{1 \to 1, 2 \to 4, 3 \to 2, 4 \to 5, 5 \to 3\}$ tandis que modulo 17, on a $\{1 \to 1, 2 \to 4, 3 \to 8, 4 \to 1, 5 \to 8, 6 \to 2, 7 \to 2, 8 \to 4\}$ (i.e. 1 et 4 ont même image, 2 et 8 ont même image, 3 et 5 idem, et 6 et 7 idem) ;
- les nombres composés peuvent être classés selon trois sortes différentes ; les puissances d'un seul premier modulo lesquelles un nombre au moins est de carré nul mais modulo lesquelles il n'y a aucun carré fixe ; les puissances produits de plusieurs premiers modulo lesquelles un nombre au moins est de carré nul et modulo lesquelles certains carrés sont fixes (et vont deux par deux nombres consécutifs) et enfin, les nombres composés n'ayant aucun facteur carré modulo lesquels il y aura des nombres fixes par l'élévation au carré (allant par deux consécutivement) mais modulo lesquels aucun nombre ne sera de carré nul.

```
#include <iostream>
#include <cmath>

int tabfacteurs[2070], tabpuiss[2070], tabexpo[2070] ;

int prime(int atester)
{
  bool pastrouve=true;
  unsigned long k = 2;

  if (atester == 1) return 0;
  if (atester == 2) return 1;
  if (atester == 3) return 1;
  if (atester == 5) return 1;
  if (atester == 7) return 1;
  while (pastrouve)
    {
    if ((k * k) > atester) return 1;
    else
      if ((atester % k) == 0) {
      return 0 ;
      }
      else k++;
    }
}

int main (int argc, char* argv[])
{
  int i, comptelesptsfixes, nbmaxfixes, k, j, p, nbdiv, nbdivp, tempo, expo,
tmp, somme, nbredondances, sommeexpo ;
  bool boolpremier ;

  nbmaxfixes = 0 ;
  for (i=3 ; i <= 2020 ; i=i+2)
    //if (not(prime(i)))
      {
      comptelesptsfixes = 0 ;
      std::cout << "\n" << i << " : \n" ;
      tabfacteurs[i] = 1 ;
      tabpuiss[i] = 1 ;
      tabexpo[i] = 1 ;
      somme = 0 ;
      tempo = i ; p = i/2 ;
      nbdiv = 1 ;
      nbdivp = 0 ;
      if (prime(tempo))
        {
          tabfacteurs[1] = tempo ;
          tabpuiss[1] = tempo ;
          tabexpo[1] = 1 ;
        }
      else while ((tempo > 1) && (p > 1))
             {
             if ((prime(p)) && ((tempo%p) == 0))
               {
                 tabfacteurs[nbdiv] = p ;
                 nbdiv = nbdiv+1 ;
                 tempo = tempo/p ;
               }
             p=p-1 ;
             }
      if (not(prime(i))) nbdiv=nbdiv-1 ;
      if ((nbdiv == 1) && (prime(i)))
        {
```

```
    tabpuiss[1] = i ;
    tabexpo[1] = 1 ;
  }
else if ((nbdiv == 1) && (not(prime(i))))
  {
    tempo = tabfacteurs[1] ;
    tabpuiss[1] = i ;
    expo = 1 ;
    while (tempo < i)
      {
      tempo=tempo*tabfacteurs[1] ;
      expo = expo+1 ;
      }
    tabexpo[1] = expo ;
  }
else if (nbdiv > 1)
  {
    for (k = 1 ; k <= nbdiv ; ++k)
      {
      tempo = tabfacteurs[k] ;
      expo = 1 ;
      while (((i % tempo) == 0) && (tempo < i))
        {
          tempo=tempo*tabfacteurs[k] ;
          expo = expo+1 ;
        }
      tabpuiss[k] = tempo/tabfacteurs[k] ;
      tabexpo[k] = expo-1 ;
      }
  }
for (k = 1 ; k <= nbdiv ; ++k)
  {
    std::cout << tabfacteurs[k] << "^" ;
    std::cout << tabexpo[k] << "." ;
  }
std::cout << "\n" ;
k = 2 ;
while (k <= (i-1)/2)
  {
    //std::cout << "j etudie " << i << "\n" ;
    if (((k*k)%i) == 0)
      std::cout << k << " de carre nul. \n" ;
    else if ((((k*k)%i) == k) || (((k*k)%i) == (i-k)))
      {
      std::cout << k << "->" ;
      if ((k*k)%i < (i-1)/2)
        {
          std::cout << "en bas (" << (k*k)/i << ") " ;
          std::cout << (k*k)%i << "\n" ;
        }
      else
        {
          std::cout << "en haut (" << (k*k)/i << ") " ;
          std::cout << i-(k*k)%i << "\n" ;
        }
      comptelesptsfixes = comptelesptsfixes+2 ;
      }
    k=k+1 ;
  }
if (comptelesptsfixes > nbmaxfixes)
  {
    nbmaxfixes = comptelesptsfixes ;
    std::cout << "le plus de pts fixes.\n" ;
  }
```

```
        }
    }
```

Nombre de solutions de l'équation $x^2 = x \ (mod\ n)$ pour n impair (3/12/2017)

Soit n un nombre impair alors le nombre de solutions de l'équation $x^2 = x \ (mod\ n)$ est égal à 2^k avec k le nombre de facteurs premiers de la factorisation de n.

On a $n = \prod_k p_j^{\alpha_j}$. $\mathbb{Z}/n\mathbb{Z}$ est isomorphe au produit des $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$. Les solutions de l'équation $x^2 = x \ (mod\ n)$ sont données en prenant pour chaque p_j une solution de l'équation $x^2 = x$ dans l'anneau $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$. Il y en a 2 : 0 et 1. Pour trouver les solutions dans $\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z}$, on regarde le résidu r dans $\mathbb{F}_{p_j}$. Comme $\mathbb{F}_{p_j}$ est un corps, $r = 0$ ou $r = 1$.

- si $r = 0$, $x = 0$ car la valuation v de x (la plus petite puissance de p_j qui divise x) ne peut être égale à $2v$ sans être nulle ;
- si $r = 1$, on écrit $x = 1 + y$ et on a $(1 + y)^2 = 1 + y$ d'où $y^2 + y = 0$ et on a $y = 0$ car la valuation amène à une contradiction si y n'est pas nul.

```
from math import *
from numpy import *
import numpy as np

def prime(atester):
  pastrouve = True
  k = 2
  if (atester == 1): return False
  if (atester == 2): return True
  if (atester == 3): return True
  if (atester == 5): return True
  if (atester == 7): return True
  while (pastrouve):
    if ((k * k) > atester):
        return True
    else:
        if ((atester % k) == 0):
            return False
        else: k=k+1

tabfacteurs=np.zeros((1000),dtype='i')
tabpuiss=np.zeros((1000),dtype='i')
tabexpo=np.zeros((1000),dtype='i')
nbmaxfixes = 0 ;
for i in range(3,1000,2):
   comptelesptsfixes = 0
   tabfacteurs[i] = 1
   tabpuiss[i] = 1
   tabexpo[i] = 1
   somme = 0
   tempo = i
   p = i/2
   nbdiv = 1
   nbdivp = 0
   print(' ')
   if (prime(tempo)):
      print(str(tempo)+" est premier.")
      tabfacteurs[1] = tempo
      tabpuiss[1] = tempo
      tabexpo[1] = 1
   while ((tempo > 1) and (p > 1)):
      if ((prime(p)) and ((tempo%p) == 0)):
        tabfacteurs[nbdiv] = p
        nbdiv = nbdiv+1
        tempo = tempo/p
      p=p-1
   if (not(prime(i))):
     nbdiv=nbdiv-1
   if ((nbdiv == 1) and (prime(i))):
     tabpuiss[1] = i
     tabexpo[1] = 1
   elif ((nbdiv == 1) and (not(prime(i)))):
     tempo = tabfacteurs[1]
     tabpuiss[1] = i
     expo = 1
     while (tempo < i):
       tempo=tempo*tabfacteurs[1] ;
       expo = expo+1
     tabexpo[1] = expo
   elif (nbdiv > 1):
     for k in range(1,nbdiv+1,1):
       tempo = tabfacteurs[k]
       expo = 1
       while (((i%tempo) == 0) and (tempo < i)):
```

```
      tempo=tempo*tabfacteurs[k]
    expo = expo+1
    tabpuiss[k] = tempo/tabfacteurs[k]
    tabexpo[k] = expo-1
machaine = ""
for k in range(1,nbdiv+1,1):
  machaine+=str(tabfacteurs[k])+"^"+str(tabexpo[k])+"."
print(str(i)+' = '+machaine)

#partie x^2=x
k = 0
while (k <= i-1):
  machaine=""
  if (((k*k)%i) == 0):
    if (k == 0):
      print("0 fixe")
      comptelesptsfixes = comptelesptsfixes+1
    else :
      print(str(k)+" de carre nul.")
  elif (((k*k) % i) == k):
    machaine+=str(k)+" fixe "
    print(machaine)
    comptelesptsfixes = comptelesptsfixes+1
  k=k+1
  resal = comptelesptsfixes
print("Nombre de points fixes "+str(resal))
```

Nombre de solutions de l'équation $x^2 = 1\ (mod\ n)$ pour n impair (Denise Vella-Chemla, 4/12/2017)

Les nombres premiers et leurs puissances sont les seuls nombres impairs modulo lesquels la seule racine de 1 est 1.

Selon (modulo) les modules impairs composés notés n qui ne sont pas des puissances de premiers, le nombre de racines de 1 modulo n comprises entre 1 et $n-1$ est 2^k avec k le nombre de facteurs premiers de la factorisation de n.

L'explication conceptuelle de ce phénomène est trouvée en considérant que résoudre l'équation $x^2 = 1\ (mod\ n)$ est équivalent à résoudre l'équation $(x-1)(x+1) = 1\ (mod\ n)$, i.e. à trouver dans la réunion des facteurs des factorisations de $x-1$ et $x+1$ l'ensemble complet des facteurs de n. On imagine qu'il y a autant de manières différentes de réaliser cette "séparation des facteurs de n" en deux ensembles, l'un inclus dans l'ensemble des facteurs de $x-1$ et l'autre inclus dans l'ensemble des facteurs de $x+1$ que d'affecter des booléens, autant que de facteurs différents de n, chacun de ces booléens valant 0 ou 1 selon que le facteur va être retrouvé dans la décomposition de $x-1$ ou dans celle de $x+1$. C'est pour cette raison que le nombre de racines de 1 modulo n comprises entre 1 et $n-1$ est 2^k avec k le nombre de facteurs premiers de la factorisation de n.

Nombre de solutions de l'équation $x^2 = 1\ (mod\ n)$ pour n impair (Denise Vella-Chemla, 4/12/2017)

Les nombres premiers et leurs puissances sont les seuls nombres impairs modulo lesquels 1 a deux racines carrées : 1 et -1.

Selon (modulo) les modules impairs composés notés n qui ne sont pas des puissances de premiers, le nombre de racines de 1 modulo n comprises entre 1 et $n-1$ est 2^k avec k le nombre de facteurs premiers de la factorisation de n.

L'explication conceptuelle de ce phénomène est trouvée en considérant que résoudre l'équation $x^2 = 1\ (mod\ n)$ est équivalent à résoudre l'équation $(x-1)(x+1) = 1\ (mod\ n)$, i.e. à trouver dans la réunion des facteurs des factorisations de $x-1$ et $x+1$ l'ensemble complet des facteurs de n. On imagine qu'il y a autant de manières différentes de réaliser cette "séparation des facteurs de n" en deux ensembles, l'un inclus dans l'ensemble des facteurs de $x-1$ et l'autre inclus dans l'ensemble des facteurs de $x+1$ que d'affecter des booléens, autant que de facteurs différents de n, chacun de ces booléens valant 0 ou 1 selon que le facteur va être retrouvé dans la décomposition de $x-1$ ou dans celle de $x+1$. C'est pour cette raison que le nombre de racines de 1 modulo n comprises entre 1 et $n-1$ semble au premier abord être égal à 2^k avec k le nombre de facteurs premiers de la factorisation de n.

L'analyse des racines carrées modulaires de 1 pour le nombre $n = 66563$ montre qu'il faut bien différencier la factorisation du prédécesseur de 66563 (66562) de celle du successeur de 66563 (66564) (i.e. l'ordre dans lequel sont considérés ces deux nombres n'est pas indifférent).

$66563 = 7.37.257$ a une factorisation contenant trois facteurs premiers distincts.
Les racines de 1 modulo 66563 sont 258, 28526, 28785, 37778, 38037 et 66305.
Ecrivons les factorisations des prédécesseurs et successeurs de ces nombres pour comprendre l'association des $2^3 = 8$ chaînes de 3 booléens aux racines de 1 (i.e. à leur prédécesseur et successeur) : le premier booléen des chaînes correspond à l'appartenance de 7 à la factorisation du prédécesseur, le second booléen à l'appartenance de 37 à la factorisation du prédécesseur et le troisième à l'appartenance de 257 à la factorisation du prédécesseur :
257 et $259 = 7.37$ correspondent à la chaîne de 3 booléens 001 (257 "est à gauche").
$28525 = 5^2.7.163$ et $28527 = 3.37.257$ correspondent à la chaîne 100 (7 "est à gauche").
$28784 = 2^4.7.257$ et $28786 = 2.37.389$ correspondent à la chaîne 101 (7 et 257 "sont à gauche").
$37777 = 37.1021$ et $37779 = 3.7^2.257$ correspondent à la chaîne 010 (37 "est à gauche").
$38036 = 2^2.37.257$ et $38038 = 2.7.11.13.19$ correspondent à la chaîne 011 (37 et 257 "sont à gauche").
$66304 = 2^8.7.37$ et $66306 = 2.3.43.257$ correspondent à la chaîne 110 (7 et 37 "sont à gauche").

Remarque : Les nombres de carré modulaire fixe et les nombres de carré modulaire 1 se déduisent les uns des autres par la transformation $y = 2x - 1$ et sa transformation inverse $x = \frac{y+1}{2}$ ainsi :

- si $x^2 = x$ et $y = 2x - 1$ alors $x^2 - x = 0$ et $y^2 = 4x^2 - 4x + 1 = 4(x^2 - x) + 1 = 1$;
- si $y^2 = 1$ et $x = \frac{y+1}{2}$ alors $x^2 = \left(\frac{y+1}{2}\right)^2 = \frac{1+2y+y^2}{4} = \frac{2+2y}{4} = \frac{1+y}{2} = x$.

Exemples :
1) $12^2 = 12\ (mod\ 33) \iff 23^2 = 1\ (mod\ 33)$.
2) $19^2 = 1\ (mod\ 45) \iff 10^2 = 10\ (mod\ 45)$.

Nombre de solutions de l'équation $x^4 \equiv 1\ (mod\ n)$ pour n impair (Denise Vella-Chemla, 15/12/2017)

On compte les racines comprises entre 1 et $n-1$ de l'équation modulaire $x^4 \equiv 1\ (mod\ n)$. On note les entiers n pour lesquels le nombre de racines augmente strictement.

Il y a :

- ⋆ 2 solutions pour $n = 3$;
- ⋆ 4 solutions pour $n = 5$;
- ⋆ 8 solutions pour $n = 15 = 3.5$;
- ⋆ 16 solutions pour $n = 65 = 13.5$;
- ⋆ 32 solutions pour $n = 195 = 13.5.3$;
- ⋆ 64 solutions pour $n = 1105 = 17.13.5$;
- ⋆ 128 solutions pour $n = 3315 = 17.13.5.3$;

Note : ci-dessous, on utilisera toujours la lettre k mais il faudrait idéalement utiliser des k', k'', k''', etc.

On comprend les augmentations strictes ainsi ; on observe les facteurs des factorisations successives : $4k+3$ pour 3, $4k+1$ pour 5, $(4k+1).(4k+3)$ pour 15, 2 facteurs $4k+1$ pour 65, 2 facteurs $4k+1$ et un facteur $4k+3$ pour 195, 3 facteurs $4k+1$ pour 1105 et 3 facteurs $4k+1$ et un facteur $4k+3$ pour 3315. Il semble donc qu'il y ait augmentation stricte soit lors de l'ajout d'un facteur $4k+3$, soit lors de la transformation d'un facteur $4k+3$ en un facteur $4k+1$.

Pourquoi y-a-t-il deux fois plus de racines biquadratiques de 1 quand on passe d'un facteur $4k+3$ à un facteur $4k+1$?

-1 est un carré modulo tout nombre premier de la forme $4k+1$ mais n'est pas un carré modulo tout nombre premier de la forme $4k+3$. De ce fait, les nombres qui ont comme carré -1 sont racines de l'équation $x^4 \equiv 1\ (mod\ p)$ des seuls nombres premiers p de la forme $4k+1$ mais ne sont pas racines de cette équation pour les nombres premiers p de la forme $4k+3$. Le nombre de solutions de l'équation $x^4 \equiv 1\ (mod\ p)$ est égal à 2 pour les nombres premiers de la forme $4k+3$ tandis qu'il est égal à 4 pour les nombres premiers de la forme $4k+1$.

On obtient le nombre de solutions de l'équation $x^4 \equiv 1\ (mod\ n)$ pour un nombre n composé en comptant le nombre de facteurs de chaque sorte ($4k+1$ ou $4k+3$) dans sa factorisation $n = \prod_k p_k^{\alpha_k}$ et en multipliant les nombres de solutions dans les différents anneaux $\mathbb{Z}/p_k^{\alpha_k}\mathbb{Z}$ entre eux. La formule générale pour le nombre de racines quatrièmes de 1 dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ est :

$$4 \times \ nombre\ de\ facteurs\ de\ la\ forme\ 4k+1\ de\ n\ +\ 2 \times \ nombre\ de\ facteurs\ de\ la\ forme\ 4k+3\ de\ n.$$

Résultats de mathématiques expérimentales

On réutilise notre programme Python pour calculer les augmentations strictes du nombre de racines troisièmes de 1 dans $\mathbb{Z}/n\mathbb{Z}$, n impair, puis du nombre de racines cinquièmes de 1, puis du nombre de points fixes $x^5 = x$ dans ces anneaux.

1) $x^3 = 1$

$3 \rightarrow 1$
$7 \rightarrow 3$
$63 \rightarrow 9$
$819 = 3.7.13 \rightarrow 27$
$15561 = 3.7.13.19 \rightarrow 81$

2) $x^5 = 1$

$3 \to 1$
$11 \to 5$
$275 = 5.11 \to 25$
$8525 = 5.11.31 \to 125$
$(69905 = 5.11.31.41 \to 125)$
$4963255 = 5.11.31.41.71 \to 625$
$501288755 = 5.11.31.41.71.101 \to 3125$

Note : On a mis 69905 parce qu'on était sûre que ça augmenterait strictement et ça ne l'a pas fait !

3) $x^5 = x$

On fait apparaître les primorielles en bleu.

$3 \to 2$
$5 \to 4$
$15 = 3.5 \to 14$
$65 = 5.13 \to 24$
$105 = 3.5.7 \to 44$
$195 = 3.5.13 \to 74$
$1105 = 5.13.17 \to 124$
$1155 = 3.5.7.11 \to 134$
$1365 = 3.5.7.13 \to 224$
$3315 = 3.5.13.17 \to 374$
$15015 = 3.5.7.11.13 \to 674$
$23205 = 3.5.7.13.17 \to 1124$

Nombre de solutions de l'équation $x^5 \equiv 1\ (mod\ n)$ (Denise Vella-Chemla, 15/12/2017)

On constate par programme qu'on peut distinguer les nombres premiers (ou leurs puissances) de dernier chiffre 1 des nombres composés partageant cette propriété en étudiant le nombre de solutions de l'équation $x^5 \equiv 1\ (mod\ n)$. En effet, dans $\mathbb{Z}/p\mathbb{Z}$ pour les nombres premiers p dont le dernier chiffre est 1 (ou pour leurs puissances), $p-1$ étant divisible par 5 (i.e. se terminant par 0), l'équation $x^5 \equiv 1\ (mod\ n)$ a 5 solutions. Cette même équation a une seule solution ($1^5 \equiv 1\ (mod\ n)$) pour les nombres composés (autres que des puissances de premiers) de dernier chiffre 1.

On constate aussi que modulo les nombres n qui sont soit des nombres premiers soit des puissances de nombres premiers et qui se terminent par 3, 7 ou 9, l'équation $x^{10} \equiv 1\ (mod\ n)$ a 2 solutions exactement.

On constate encore que modulo les nombres n qui sont soit des nombres premiers soit des puissances de nombres premiers et qui se terminent par 1, l'équation $x^{10} \equiv 1\ (mod\ n)$ a 10 solutions exactement.

Programme en python de calcul des solutions de $x^5 \equiv 1\ (mod\ n)$

```
from math import *
from numpy import *
import numpy as np

def prime(atester):
  pastrouve = True
  k = 2
  if (atester == 1): return False
  if (atester == 2): return True
  if (atester == 3): return True
  if (atester == 5): return True
  if (atester == 7): return True
  while (pastrouve):
    if ((k * k) > atester):
        return True
    else:
        if ((atester % k) == 0):
            return False
        else: k=k+1

tabfacteurs=np.zeros((200000),dtype='i')
tabpuiss=np.zeros((200000),dtype='i')
tabexpo=np.zeros((200000),dtype='i')
maxnbrac = 0
for i in range(3,2017,1):
   comptelesrac = 0
   tabfacteurs[i] = 1
   tabpuiss[i] = 1
   tabexpo[i] = 1
   somme = 0
   tempo = i
   p = i/2
   nbdiv = 1
   nbdivp = 0
   print(' ')
   if (prime(tempo)):
      print(str(tempo)+" est premier.")
      tabfacteurs[1] = tempo
      tabpuiss[1] = tempo
      tabexpo[1] = 1
```

```
  while ((tempo > 1) and (p > 1)):
     if ((prime(p)) and ((tempo\%p) == 0)):
       tabfacteurs[nbdiv] = p
       nbdiv = nbdiv+1
       tempo = tempo/p
     p=p-1
  if (not(prime(i))):
    nbdiv=nbdiv-1
  if ((nbdiv == 1) and (prime(i))):
    tabpuiss[1] = i
    tabexpo[1] = 1
  elif ((nbdiv == 1) and (not(prime(i)))):
    tempo = tabfacteurs[1]
    tabpuiss[1] = i
    expo = 1
    while (tempo < i):
      tempo=tempo*tabfacteurs[1] ;
      expo = expo+1
    tabexpo[1] = expo
  elif (nbdiv > 1):
    for k in range(1,nbdiv+1,1):
      tempo = tabfacteurs[k]
      expo = 1
      while (((i%tempo) == 0) and (tempo < i)):
        tempo=tempo*tabfacteurs[k]
  expo = expo+1
      tabpuiss[k] = tempo/tabfacteurs[k]
      tabexpo[k] = expo-1
  machaine = ""
  for k in range(1,nbdiv+1,1):
    machaine+=str(tabfacteurs[k])+"^"+str(tabexpo[k])+"."
  print(str(i)+' = '+machaine)

  k = 1
  while (k <= i-1):
     if (((k*k*k*k*k) % i) == 1):
        print(str(k)+" sol de x^5=1 (mod n).")
        comptelesrac = comptelesrac+1
     k=k+1
  print(str(comptelesrac)+" sol.")
  if (comptelesrac > maxnbrac):
     maxnbrac = comptelesrac
     print("le plus de rac.")
```

Résultat du programme ci-dessus :

```
3 est premier.
3 = 3^1.
1 sol de x^5=1 (mod n).
1 sol.
le plus de rac.

4 = 2^2.
1 sol de x^5=1 (mod n).
1 sol.
```

```
5 est premier.
5 = 5^1.
1 sol de x^5=1 (mod n).
1 sol.

6 = 3^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

7 est premier.
7 = 7^1.
1 sol de x^5=1 (mod n).
1 sol.

8 = 2^3.
1 sol de x^5=1 (mod n).
1 sol.

9 = 3^2.
1 sol de x^5=1 (mod n).
1 sol.

10 = 5^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

11 est premier.
11 = 11^1.
1 sol de x^5=1 (mod n).
3 sol de x^5=1 (mod n).
4 sol de x^5=1 (mod n).
5 sol de x^5=1 (mod n).
9 sol de x^5=1 (mod n).
5 sol.
le plus de rac.

12 = 3^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.

13 est premier.
13 = 13^1.
1 sol de x^5=1 (mod n).
1 sol.

14 = 7^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

15 = 5^1.3^1.
1 sol de x^5=1 (mod n).
1 sol.

16 = 2^4.
1 sol de x^5=1 (mod n).
1 sol.

17 est premier.
17 = 17^1.
1 sol de x^5=1 (mod n).
1 sol.
```

```
18 = 3^2.2^1.
1 sol de x^5=1 (mod n).
1 sol.

19 est premier.
19 = 19^1.
1 sol de x^5=1 (mod n).
1 sol.

20 = 5^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.

21 = 7^1.3^1.
1 sol de x^5=1 (mod n).
1 sol.

22 = 11^1.2^1.
1 sol de x^5=1 (mod n).
3 sol de x^5=1 (mod n).
5 sol de x^5=1 (mod n).
9 sol de x^5=1 (mod n).
15 sol de x^5=1 (mod n).
5 sol.

23 est premier.
23 = 23^1.
1 sol de x^5=1 (mod n).
1 sol.

24 = 3^1.2^3.
1 sol de x^5=1 (mod n).
1 sol.

25 = 5^2.
1 sol de x^5=1 (mod n).
6 sol de x^5=1 (mod n).
11 sol de x^5=1 (mod n).
16 sol de x^5=1 (mod n).
21 sol de x^5=1 (mod n).
5 sol.

26 = 13^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

27 = 3^3.
1 sol de x^5=1 (mod n).
1 sol.

28 = 7^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.

29 est premier.
29 = 29^1.
1 sol de x^5=1 (mod n).
1 sol.

30 = 5^1.3^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.
```

```
31 est premier.
31 = 31^1.
1 sol de x^5=1 (mod n).
2 sol de x^5=1 (mod n).
4 sol de x^5=1 (mod n).
8 sol de x^5=1 (mod n).
16 sol de x^5=1 (mod n).
5 sol.

32 = 2^5.
1 sol de x^5=1 (mod n).
1 sol.

33 = 11^1.3^1.
1 sol de x^5=1 (mod n).
4 sol de x^5=1 (mod n).
16 sol de x^5=1 (mod n).
25 sol de x^5=1 (mod n).
31 sol de x^5=1 (mod n).
5 sol.

34 = 17^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

35 = 7^1.5^1.
1 sol de x^5=1 (mod n).
1 sol.

36 = 3^2.2^2.
1 sol de x^5=1 (mod n).
1 sol.

37 est premier.
37 = 37^1.
1 sol de x^5=1 (mod n).
1 sol.

38 = 19^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

39 = 13^1.3^1.
1 sol de x^5=1 (mod n).
1 sol.

40 = 5^1.2^3.
1 sol de x^5=1 (mod n).
1 sol.

41 est premier.
41 = 41^1.
1 sol de x^5=1 (mod n).
10 sol de x^5=1 (mod n).
16 sol de x^5=1 (mod n).
18 sol de x^5=1 (mod n).
37 sol de x^5=1 (mod n).
5 sol.

42 = 7^1.3^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.
```

```
43 est premier.
43 = 43^1.
1 sol de x^5=1 (mod n).
1 sol.

44 = 11^1.2^2.
1 sol de x^5=1 (mod n).
5 sol de x^5=1 (mod n).
9 sol de x^5=1 (mod n).
25 sol de x^5=1 (mod n).
37 sol de x^5=1 (mod n).
5 sol.

45 = 5^1.3^2.
1 sol de x^5=1 (mod n).
1 sol.

46 = 23^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

47 est premier.
47 = 47^1.
1 sol de x^5=1 (mod n).
1 sol.

48 = 3^1.2^4.
1 sol de x^5=1 (mod n).
1 sol.

49 = 7^2.
1 sol de x^5=1 (mod n).
1 sol.

50 = 5^2.2^1.
1 sol de x^5=1 (mod n).
11 sol de x^5=1 (mod n).
21 sol de x^5=1 (mod n).
31 sol de x^5=1 (mod n).
41 sol de x^5=1 (mod n).
5 sol.

51 = 17^1.3^1.
1 sol de x^5=1 (mod n).
1 sol.

52 = 13^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.

53 est premier.
53 = 53^1.
1 sol de x^5=1 (mod n).
1 sol.

54 = 3^3.2^1.
1 sol de x^5=1 (mod n).
1 sol.
```

```
55 = 11^1.5^1.
1 sol de x^5=1 (mod n).
16 sol de x^5=1 (mod n).
26 sol de x^5=1 (mod n).
31 sol de x^5=1 (mod n).
36 sol de x^5=1 (mod n).
5 sol.

56 = 7^1.2^3.
1 sol de x^5=1 (mod n).
1 sol.

57 = 19^1.3^1.
1 sol de x^5=1 (mod n).
1 sol.

58 = 29^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

59 est premier.
59 = 59^1.
1 sol de x^5=1 (mod n).
1 sol.

60 = 5^1.3^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.

61 est premier.
61 = 61^1.
1 sol de x^5=1 (mod n).
9 sol de x^5=1 (mod n).
20 sol de x^5=1 (mod n).
34 sol de x^5=1 (mod n).
58 sol de x^5=1 (mod n).
5 sol.

62 = 31^1.2^1.
1 sol de x^5=1 (mod n).
33 sol de x^5=1 (mod n).
35 sol de x^5=1 (mod n).
39 sol de x^5=1 (mod n).
47 sol de x^5=1 (mod n).
5 sol.

63 = 7^1.3^2.
1 sol de x^5=1 (mod n).
1 sol.

64 = 2^6.
1 sol de x^5=1 (mod n).
1 sol.

65 = 13^1.5^1.
1 sol de x^5=1 (mod n).
1 sol.
```

```
66 = 11^1.3^1.2^1.
1 sol de x^5=1 (mod n).
25 sol de x^5=1 (mod n).
31 sol de x^5=1 (mod n).
37 sol de x^5=1 (mod n).
49 sol de x^5=1 (mod n).
5 sol.

67 est premier.
67 = 67^1.
1 sol de x^5=1 (mod n).
1 sol.

68 = 17^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.

69 = 23^1.3^1.
1 sol de x^5=1 (mod n).
1 sol.

70 = 7^1.5^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

71 est premier.
71 = 71^1.
1 sol de x^5=1 (mod n).
5 sol de x^5=1 (mod n).
25 sol de x^5=1 (mod n).
54 sol de x^5=1 (mod n).
57 sol de x^5=1 (mod n).
5 sol.

72 = 3^2.2^3.
1 sol de x^5=1 (mod n).
1 sol.

73 est premier.
73 = 73^1.
1 sol de x^5=1 (mod n).
1 sol.

74 = 37^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

75 = 5^2.3^1.
1 sol de x^5=1 (mod n).
16 sol de x^5=1 (mod n).
31 sol de x^5=1 (mod n).
46 sol de x^5=1 (mod n).
61 sol de x^5=1 (mod n).
5 sol.

76 = 19^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.
```

```
77 = 11^1.7^1.
1 sol de x^5=1 (mod n).
15 sol de x^5=1 (mod n).
36 sol de x^5=1 (mod n).
64 sol de x^5=1 (mod n).
71 sol de x^5=1 (mod n).
5 sol.

78 = 13^1.3^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

79 est premier.
79 = 79^1.
1 sol de x^5=1 (mod n).
1 sol.

80 = 5^1.2^4.
1 sol de x^5=1 (mod n).
1 sol.

81 = 3^4.
1 sol de x^5=1 (mod n).
1 sol.

82 = 41^1.2^1.
1 sol de x^5=1 (mod n).
37 sol de x^5=1 (mod n).
51 sol de x^5=1 (mod n).
57 sol de x^5=1 (mod n).
59 sol de x^5=1 (mod n).
5 sol.

83 est premier.
83 = 83^1.
1 sol de x^5=1 (mod n).
1 sol.

84 = 7^1.3^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.

85 = 17^1.5^1.
1 sol de x^5=1 (mod n).
1 sol.

86 = 43^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

87 = 29^1.3^1.
1 sol de x^5=1 (mod n).
1 sol.

88 = 11^1.2^3.
1 sol de x^5=1 (mod n).
9 sol de x^5=1 (mod n).
25 sol de x^5=1 (mod n).
49 sol de x^5=1 (mod n).
81 sol de x^5=1 (mod n).
5 sol.
```

```
89 est premier.
89 = 89^1.
1 sol de x^5=1 (mod n).
1 sol.

90 = 5^1.3^2.2^1.
1 sol de x^5=1 (mod n).
1 sol.

91 = 13^1.7^1.
1 sol de x^5=1 (mod n).
1 sol.

92 = 23^1.2^2.
1 sol de x^5=1 (mod n).
1 sol.

93 = 31^1.3^1.
1 sol de x^5=1 (mod n).
4 sol de x^5=1 (mod n).
16 sol de x^5=1 (mod n).
64 sol de x^5=1 (mod n).
70 sol de x^5=1 (mod n).
5 sol.

94 = 47^1.2^1.
1 sol de x^5=1 (mod n).
1 sol.

95 = 19^1.5^1.
1 sol de x^5=1 (mod n).
1 sol.

96 = 3^1.2^5.
1 sol de x^5=1 (mod n).
1 sol.

97 est premier.
97 = 97^1.
1 sol de x^5=1 (mod n).
1 sol.

98 = 7^2.2^1.
1 sol de x^5=1 (mod n).
1 sol.

99 = 11^1.3^2.
1 sol de x^5=1 (mod n).
37 sol de x^5=1 (mod n).
64 sol de x^5=1 (mod n).
82 sol de x^5=1 (mod n).
91 sol de x^5=1 (mod n).
5 sol.
```

```
100 = 5^2.2^2.
1 sol de x^5=1 (mod n).
21 sol de x^5=1 (mod n).
41 sol de x^5=1 (mod n).
61 sol de x^5=1 (mod n).
81 sol de x^5=1 (mod n).
5 sol.

101 est premier.
101 = 101^1.
1 sol de x^5=1 (mod n).
36 sol de x^5=1 (mod n).
84 sol de x^5=1 (mod n).
87 sol de x^5=1 (mod n).
95 sol de x^5=1 (mod n).
5 sol.
```

Le programme ci-dessous teste qu'au moins jusqu'à 1515, modulo tous les nombres premiers dont le dernier chiffre est 3 (resp. modulo leurs puissances), l'équation $x^{10} \equiv 1 \ (mod \ p)$ (resp. l'équation $x^{10} \equiv 1 \ (mod \ p^k)$) a exactement deux solutions. On doit également vérifier que modulo aucun nombre composé autre qu'une puissance d'un nombre premier de dernier chiffre 1, l'équation en question a deux solutions exactement (faux positifs).

```
from math import *
from numpy import *
import numpy as np

def prime(atester):
  pastrouve = True
  k = 2
  if (atester == 1): return False
  if (atester == 2): return True
  if (atester == 3): return True
  if (atester == 5): return True
  if (atester == 7): return True
  while (pastrouve):
    if ((k * k) > atester):
        return True
    else:
        if ((atester % k) == 0):
            return False
        else: k=k+1
```

```
tabfacteurs=np.zeros((200000),dtype='i')
tabpuiss=np.zeros((200000),dtype='i')
tabexpo=np.zeros((200000),dtype='i')
maxnbrac = 0
for i in range(3,1515,1):
   comptelesrac = 0
   tabfacteurs[i] = 1
   tabpuiss[i] = 1
   tabexpo[i] = 1
   somme = 0
   tempo = i
   p = i/2
   nbdiv = 1
   nbdivp = 0
   print(' ')
   if (prime(tempo)):
      print(str(tempo)+" est premier.")
      tabfacteurs[1] = tempo
      tabpuiss[1] = tempo
      tabexpo[1] = 1

    while ((tempo > 1) and (p > 1)):
      if ((prime(p)) and ((tempo%p) == 0)):
        tabfacteurs[nbdiv] = p
        nbdiv = nbdiv+1
        tempo = tempo/p
      p=p-1

   if (not(prime(i))):
      nbdiv=nbdiv-1
   if ((nbdiv == 1) and (prime(i))):
     tabpuiss[1] = i
     tabexpo[1] = 1
   elif ((nbdiv == 1) and (not(prime(i)))):
     tempo = tabfacteurs[1]
     tabpuiss[1] = i
     expo = 1
     while (tempo < i):
       tempo=tempo*tabfacteurs[1] ;
       expo = expo+1
     tabexpo[1] = expo
   elif (nbdiv > 1):
     for k in range(1,nbdiv+1,1):
       tempo = tabfacteurs[k]
       expo = 1
       while (((i\%tempo) == 0) and (tempo < i)):
         tempo=tempo*tabfacteurs[k]
   expo = expo+1
       tabpuiss[k] = tempo/tabfacteurs[k]
       tabexpo[k] = expo-1
   machaine = ""
   for k in range(1,nbdiv+1,1):
     machaine+=str(tabfacteurs[k])+"^"+str(tabexpo[k])+"."
   print(str(i)+' = '+machaine)

   k = 1
   while (k <= i-1):
      if ((((((((((((((((((((k*k)\%i)*k)\%i)*k)\%i)*k)\%i)*k)\%i)*k)\%i)*k)\%i)*k)\%i)*k)\%i)== 1)
          :
        print(str(k)+" sol de x^{10}=1 (mod n).")
        comptelesrac = comptelesrac+1
      k=k+1
   print(str(comptelesrac)+" sol.")
```

```
   if ((prime(i)) and ((i \% 10) == 3) and (comptelesrac == 2)):
      print("youpi premier")
   elif (prime(i)) and ((i \% 10) == 3):
      print("rate premier")
   elif (((i \% 10) == 3) and (nbdiv == 1) and (comptelesrac != 2)):
      print("rate compose")
   elif ((i \% 10) == 3):
      print("youpi compose")
   if (comptelesrac > maxnbrac):
      maxnbrac = comptelesrac
      print("le plus de rac.")
```

Résultat du programme ci-dessus :

```
3 est premier.
3 = 3^1.
1 sol de x^{10}=1 (mod n).
2 sol de x^{10}=1 (mod n).
2 sol.
youpi premier
le plus de rac.

4 = 2^2.
1 sol de x^{10}=1 (mod n).
3 sol de x^{10}=1 (mod n).
2 sol.

5 est premier.
5 = 5^1.
1 sol de x^{10}=1 (mod n).
4 sol de x^{10}=1 (mod n).
2 sol.

6 = 3^1.2^1.
1 sol de x^{10}=1 (mod n).
5 sol de x^{10}=1 (mod n).
2 sol.

7 est premier.
7 = 7^1.
1 sol de x^{10}=1 (mod n).
6 sol de x^{10}=1 (mod n).
2 sol.
```

```
8 = 2^3.
1 sol de x^{10}=1 (mod n).
3 sol de x^{10}=1 (mod n).
5 sol de x^{10}=1 (mod n).
7 sol de x^{10}=1 (mod n).
4 sol.
le plus de rac.

9 = 3^2.
1 sol de x^{10}=1 (mod n).
8 sol de x^{10}=1 (mod n).
2 sol.

10 = 5^1.2^1.
1 sol de x^{10}=1 (mod n).
9 sol de x^{10}=1 (mod n).
2 sol.

11 est premier.
11 = 11^1.
1 sol de x^{10}=1 (mod n).
2 sol de x^{10}=1 (mod n).
3 sol de x^{10}=1 (mod n).
4 sol de x^{10}=1 (mod n).
5 sol de x^{10}=1 (mod n).
6 sol de x^{10}=1 (mod n).
7 sol de x^{10}=1 (mod n).
8 sol de x^{10}=1 (mod n).
9 sol de x^{10}=1 (mod n).
10 sol de x^{10}=1 (mod n).
10 sol.
le plus de rac.

12 = 3^1.2^2.
1 sol de x^{10}=1 (mod n).
5 sol de x^{10}=1 (mod n).
7 sol de x^{10}=1 (mod n).
11 sol de x^{10}=1 (mod n).
4 sol.

13 est premier.
13 = 13^1.
1 sol de x^{10}=1 (mod n).
12 sol de x^{10}=1 (mod n).
2 sol.
youpi premier

14 = 7^1.2^1.
1 sol de x^{10}=1 (mod n).
13 sol de x^{10}=1 (mod n).
2 sol.

15 = 5^1.3^1.
1 sol de x^{10}=1 (mod n).
4 sol de x^{10}=1 (mod n).
11 sol de x^{10}=1 (mod n).
14 sol de x^{10}=1 (mod n).
4 sol.
```

```
16 = 2^4.
1 sol de x^{10}=1 (mod n).
7 sol de x^{10}=1 (mod n).
9 sol de x^{10}=1 (mod n).
15 sol de x^{10}=1 (mod n).
4 sol.

17 est premier.
17 = 17^1.
1 sol de x^{10}=1 (mod n).
16 sol de x^{10}=1 (mod n).
2 sol.

18 = 3^2.2^1.
1 sol de x^{10}=1 (mod n).
17 sol de x^{10}=1 (mod n).
2 sol.

19 est premier.
19 = 19^1.
1 sol de x^{10}=1 (mod n).
18 sol de x^{10}=1 (mod n).
2 sol.

20 = 5^1.2^2.
1 sol de x^{10}=1 (mod n).
9 sol de x^{10}=1 (mod n).
11 sol de x^{10}=1 (mod n).
19 sol de x^{10}=1 (mod n).
4 sol.

21 = 7^1.3^1.
1 sol de x^{10}=1 (mod n).
8 sol de x^{10}=1 (mod n).
13 sol de x^{10}=1 (mod n).
20 sol de x^{10}=1 (mod n).
4 sol.

22 = 11^1.2^1.
1 sol de x^{10}=1 (mod n).
3 sol de x^{10}=1 (mod n).
5 sol de x^{10}=1 (mod n).
7 sol de x^{10}=1 (mod n).
9 sol de x^{10}=1 (mod n).
13 sol de x^{10}=1 (mod n).
15 sol de x^{10}=1 (mod n).
17 sol de x^{10}=1 (mod n).
19 sol de x^{10}=1 (mod n).
21 sol de x^{10}=1 (mod n).
10 sol.

23 est premier.
23 = 23^1.
1 sol de x^{10}=1 (mod n).
22 sol de x^{10}=1 (mod n).
2 sol.
youpi premier
```

```
24 = 3^1.2^3.
1 sol de x^{10}=1 (mod n).
5 sol de x^{10}=1 (mod n).
7 sol de x^{10}=1 (mod n).
11 sol de x^{10}=1 (mod n).
13 sol de x^{10}=1 (mod n).
17 sol de x^{10}=1 (mod n).
19 sol de x^{10}=1 (mod n).
23 sol de x^{10}=1 (mod n).
8 sol.

25 = 5^2.
1 sol de x^{10}=1 (mod n).
4 sol de x^{10}=1 (mod n).
6 sol de x^{10}=1 (mod n).
9 sol de x^{10}=1 (mod n).
11 sol de x^{10}=1 (mod n).
14 sol de x^{10}=1 (mod n).
16 sol de x^{10}=1 (mod n).
19 sol de x^{10}=1 (mod n).
21 sol de x^{10}=1 (mod n).
24 sol de x^{10}=1 (mod n).
10 sol.

26 = 13^1.2^1.
1 sol de x^{10}=1 (mod n).
25 sol de x^{10}=1 (mod n).
2 sol.

27 = 3^3.
1 sol de x^{10}=1 (mod n).
26 sol de x^{10}=1 (mod n).
2 sol.

28 = 7^1.2^2.
1 sol de x^{10}=1 (mod n).
13 sol de x^{10}=1 (mod n).
15 sol de x^{10}=1 (mod n).
27 sol de x^{10}=1 (mod n).
4 sol.

29 est premier.
29 = 29^1.
1 sol de x^{10}=1 (mod n).
28 sol de x^{10}=1 (mod n).
2 sol.

30 = 5^1.3^1.2^1.
1 sol de x^{10}=1 (mod n).
11 sol de x^{10}=1 (mod n).
19 sol de x^{10}=1 (mod n).
29 sol de x^{10}=1 (mod n).
4 sol.
```

Nombre de solutions de l'équation $x^{10} \equiv 1\ (mod\ n)$ en fonction du dernier chiffre de n (Denise Vella-Chemla, 22.12.2017)

Par programme, on a constaté les faits suivants que l'on énonce comme des conjectures :

- un nombre n qui se termine par 1 est un nombre premier ou une puissance d'un nombre premier se terminant par un 1 si et seulement si l'équation modulaire $x^{10} \equiv 1\ (mod\ n)$ a exactement 10 solutions ;
- un nombre n qui se termine par 3, 7 ou 9 est un nombre premier ou une puissance d'un nombre premier (se terminant par 3, 7, ou 9) si et seulement si l'équation modulaire $x^{10} \equiv 1\ (mod\ n)$ a exactement 2 solutions ;
- un nombre n qui se termine par 1 est une puissance d'un nombre premier se terminant par 3, 7, ou 9 si et seulement si l'équation modulaire $x^{10} \equiv 1\ (mod\ n)$ a exactement 2 solutions.

On a $x^{10} \equiv 1\ (mod\ n) \iff x^{10} - 1 \equiv 0\ (mod\ n)$.

Or $x^{10} - 1 = (x-1)(x+1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)$.

On oublie les solutions triviales 1 et $n-1$ qui annulent, l'une, le monôme $x-1$, et l'autre, le monôme $x+1$. On oublie également le polynôme alterné $x^4 - x^3 + x^2 - x + 1$ car il s'annule pour $n - x$ lorsque le polynôme $x^4 + x^3 + x^2 + x + 1$ s'annule pour x et on se concentre donc sur l'annulation de ce polynôme simple symétrique $x^4 + x^3 + x^2 + x + 1$. On cherche pourquoi il s'annule 4 fois pour un nombre premier p se terminant par 1 ou une puissance de nombre premier p^k se terminant par 1 alors qu'il ne s'annule jamais pour un nombre premier p se terminant par $3, 7$ ou 9 ou une puissance de nombre premier p^k se terminant par $3, 7$ ou 9. On ne réfléchit pas pour l'instant au fait que modulo un nombre composé n, l'équation modulaire $x^{10} \equiv 1\ (mod\ n)$ n'admet jamais 2 ou 10 solutions.

On résoud $x^4 + x^3 + x^2 + x + 1 = 0$ ainsi : on divise le polynôme par x^2. On obtient :

$$x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2} = 0$$

qu'on réécrit en :

$$\left(x^2 + \frac{1}{x^2}\right) + \left(x + \frac{1}{x}\right) + 1 = 0$$

(en mettant ensemble les premier et cinquième termes, ainsi que les second et quatrième termes).

On pose $X = x + \frac{1}{x}$.

L'équation se réécrit $X^2 + X - 1 = 0$. Le discriminant Δ_1 de cette nouvelle équation est égal à 5.

On a abouti aux 2 solutions suivantes pour X :

$$x + \frac{1}{x} = \frac{-1 \pm \sqrt{5}}{2}.$$

On multiplie les deux membres de l'égalité par x et on a à résoudre une autre équation du second degré :

$$x^2 + \frac{1 \pm \sqrt{5}}{2}x + 1 = 0$$

Le discriminant Δ_2 de cette seconde équation du second degré est égal à :

$$\Delta_2 = \frac{(1 \pm \sqrt{5})^2}{4} - 4 = \frac{1 \pm 2\sqrt{5} + 5 - 16}{4} = \frac{-5 \pm \sqrt{5}}{2}$$

Les deux solutions de cette seconde équation du second degré sont :

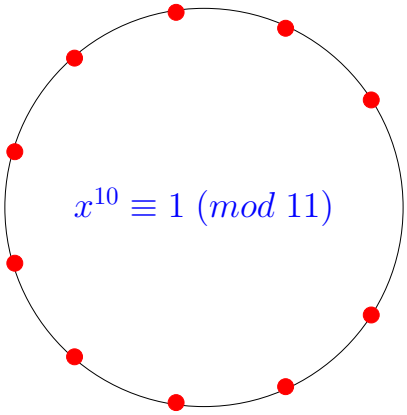
$$X = \frac{\frac{-1 \pm \sqrt{5}}{2} \pm \sqrt{\frac{-5 \pm \sqrt{5}}{2}}}{2}$$

Il n'y a aucune solution pour les nombres n de dernier chiffre 3 et 7 car modulo de tels nombres n, 5 n'est jamais un carré (i.e. n'a pas de racine carrée modulaire) dans $\mathbb{Z}/n\mathbb{Z}$.

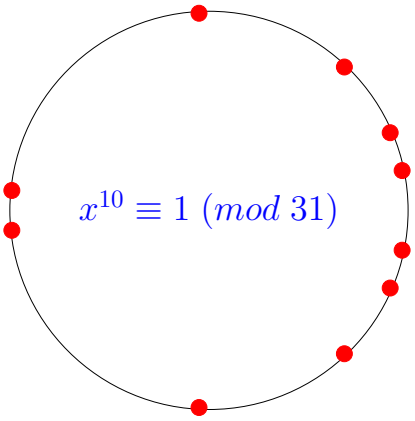
Mais pour les nombres n de dernier chiffre 1 ou 9, 5 admet toujours deux racines carrées (cf. annexe 2), il reste à comprendre pourquoi selon un module n de dernier chiffre 9, bien que 5 admette deux racines carrées modulaires, le polynôme $x^4 + x^3 + x^2 + x + 1$ ne peut cependant jamais être nul. Il faut aussi compléter le raisonnement pour les puissances d'un nombre premier plutôt que pour les nombres premiers simples.

Annexe 1 : Positionnement des solutions de l'équation $x^{10} \equiv 1 \ (mod\ p)$ *sur cercles modulaires pour* $p = 11, 31, 41, 61, 71$

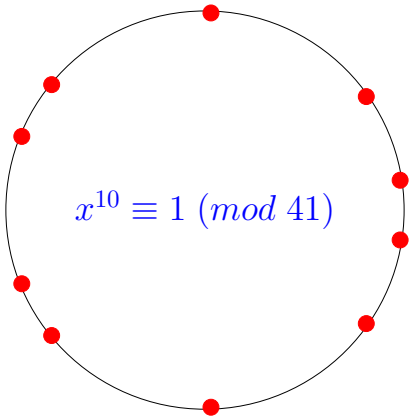
Solutions de $x^{10} \equiv 1 \ (mod\ 11)$: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10. 11 est premier. Il y a 10 solutions.



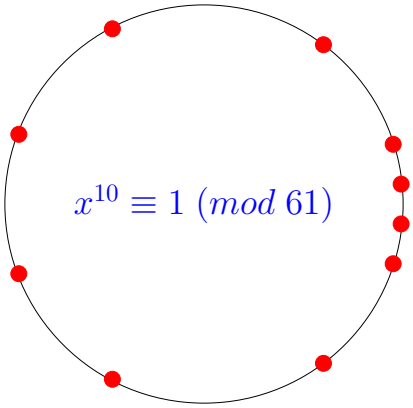
Solutions de $x^{10} \equiv 1 \ (mod\ 31)$: 1, 2, 4, 8, 15, 16, 23, 27, 29, 30. 31 est premier. Il y a 10 solutions.



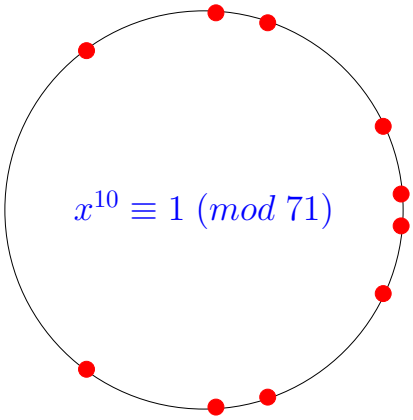
Solutions de $x^{10} \equiv 1 \ (mod\ 41)$: 1, 4, 10, 16, 18, 23, 25, 31, 37, 40. 41 est premier. Il y a 10 solutions.



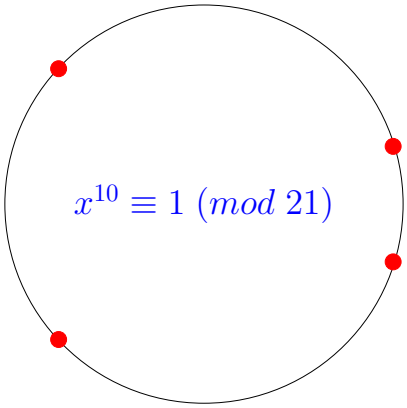
Solutions de $x^{10} \equiv 1 \ (mod\ 61)$: 1, 3, 9, 20, 27, 34, 41, 52, 58, 60. 61 est premier. Il y a 10 solutions.



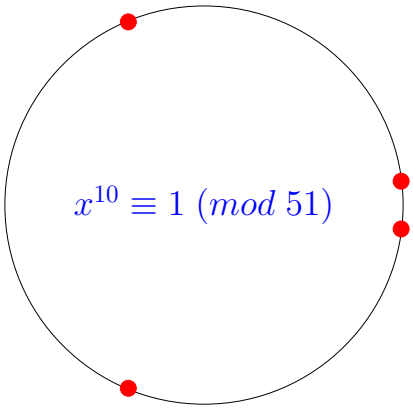
Solutions de $x^{10} \equiv 1 \ (mod\ 71)$: 1, 5, 14, 17, 25, 46, 54, 57, 66, 70. 71 est premier. Il y a 10 solutions.



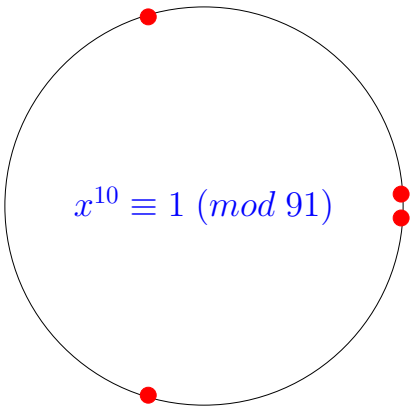
Solutions de $x^{10} \equiv 1 \ (mod\ 21)$: 1, 8, 13, 20. 21 est composé. Il y a 4 solutions.



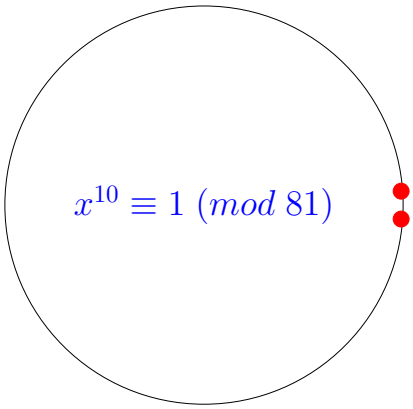
Solutions de $x^{10} \equiv 1 \ (mod\ 51)$: 1, 16, 35, 50. 51 est composé. Il y a 4 solutions.



Solutions de $x^{10} \equiv 1 \ (mod\ 91)$: 1, 27, 64, 90. 91 est composé. Il y a 4 solutions.



Solutions de $x^{10} \equiv 1\ (mod\ 81)$: 1, 80. 81 est composé, c'est une puissance d'un nombre premier se terminant par 3, l'équation n'a que deux solutions, les solutions triviales (de même par exemple, que l'équation $x^{10} \equiv 1\ (mod\ 49)$ (49 étant une puissance de 7), n'a que les deux solutions triviales 1 et 48).



Annexe 2 : Rappel des racines carrées modulaires de 5 pour les nombres n de dernier chiffre 1 ou 9 (obtenues par programme)

4 racine carrée de 5 (mod 11).
7 racine carrée de 5 (mod 11).

9 racine carrée de 5 (mod 19).
10 racine carrée de 5 (mod 19).

11 racine carrée de 5 (mod 29).
18 racine carrée de 5 (mod 29).

6 racine carrée de 5 (mod 31).
25 racine carrée de 5 (mod 31).

13 racine carrée de 5 (mod 41).
28 racine carrée de 5 (mod 41).

8 racine carrée de 5 (mod 59).
51 racine carrée de 5 (mod 59).

26 racine carrée de 5 (mod 61).
35 racine carrée de 5 (mod 61).

17 racine carrée de 5 (mod 71).
54 racine carrée de 5 (mod 71).

20 racine carrée de 5 (mod 79).
59 racine carrée de 5 (mod 79).

19 racine carrée de 5 (mod 89).
70 racine carrée de 5 (mod 89).