Primalité de nombres, comptage de lettres, régularités.

Doubles de pairs entre 2 nombres premiers, comptage de lettres, régularités.

Toujours trouver un nouveau couple de nombres premiers les plus proches possible.

Ecriture p-adique, écriture en base p.

Matrice 2×2 ne contenant que des $1/2$.

Petit pont vers la mécanique quantique.

Trouver des opérateurs qui vérifient les règles souhaitées.

Entrechocs, entrelacs.

Transitions.

Matrices gigognes.

Tourner en rond.

Sommes de 2 carrés.

Rectangles.

Pgcd, classique ou tropical.

Entrelacs premiers.

Cromagnon child.

Tore ∞-dimensionnel.

G comme Gödel.

Programme préféré : les nombres premiers annulent une somme de cosinus.

Coder.

Tamis.

Quadrilatère quelconque, carre.

Petit pont entre grilles de divisibilité et D_4.

Matrices de passage entre les différents états.

Polygones et circuits dans des graphes.

Images.

Programmes de l'approche par les mots.

Programmes 4 carrés, 3 triangles, et Euréka de Gauss.

Espace et mon opérateur.

Etudier des nombres d'écarts.

Formule récurrente d'Euler pour le calcul de la somme des diviseurs.

transparents montrant des images.

Nombre de résidus quadratiques d'un nombre entier inférieurs à sa moitié.

Plus de la moitié ?.

De visu.

Tables de résidus quadratiques des modules 3 à 51.

Nombre de résidus quadratiques d'un nombre entier inférieurs à sa moitié.

Nombres de résidus quadratiques des nombres premiers ou composés.

Questions de fin d'été.

Indices de Gauss.

Nombres de résidus cubiques, biquadratiques, quintiques et sixtiques des nombres premiers ou composés.

Racines, chemins pour atteindre l'unité, cardinaux.

Pgcd et diagonales de booléens.

Pgcd et trajets de booléens.

Table de la relation “premier à”.

Papier pointé.

Une formule récurrente pour l’indicateur d’Euler trouvée sur la toile.

Suites arythmiques.

Couleurs Alain Connes “three classes of notes”.

Compositions.

Traverser un carré.

Courbes et points entiers.

Essai : graphe des produits d’entiers.

Primalité de nombres, comptage de lettres, régularités (Denise Vella-Chemla, 1.1.2016)

Il s'agit d'étudier si certains comptages de lettres, codant certaines propriétés de nombres, permettraient de mettre au jour des régularités, qui amèneraient la possibilité d'effectuer certaines déductions.

On rappelle que deux nombres premiers jumeaux ont pour différence 2. Par exemple, 3 et 5 sont des nombres premiers jumeaux, 41 et 43 en sont également.

On définit deux fonctions $pp(n)$ (pp pour *prec_premier*) et $sp(n)$ (sp pour *succ_premier*) qui associent à un nombre pair n deux booléens de primalité selon que $n-1$ et $n+1$ sont premiers ou non. Par convention, le booléen 0 signifie *premier* et le booléen 1 signifie *composé*. Par exemple, $pp(8) = 0$ car $8 - 1 = 7$ est premier tandis que $sp(8) = 1$ car $8 + 1 = 9$ est composé.

On définit $l(n)$ la lettre associée à un nombre pair n qui vaut :

- a si $pp(n) = 0$ et $sp(n) = 0$ (ex : $l(4) = l(18) = a$) ;
- b si $pp(n) = 0$ et $sp(n) = 1$ (ex : $l(8) = l(24) = b$) ;
- c si $pp(n) = 1$ et $sp(n) = 0$ (ex : $l(10) = l(22) = c$) ;
- d si $pp(n) = 1$ et $sp(n) = 1$ (ex : $l(26) = l(34) = d$).

On définit 4 variables $X_a(n), X_b(n), X_c(n)$ et $X_d(n)$ de la façon suivante :

- $X_a(n) = \#\{x \text{ pair et } 3 \leq x \leq n \text{ et } l(x) = a\}$
  ($X_a(n)$ compte le nombre de couples de nombres premiers jumeaux inférieurs ou égaux à $n + 1$) ;
- $X_b(n) = \#\{x \text{ pair et } 3 \leq x \leq n \text{ et } l(x) = b\}$;
- $X_c(n) = \#\{x \text{ pair et } 3 \leq x \leq n \text{ et } l(x) = c\}$;
- $X_d(n) = \#\{x \text{ pair et } 3 \leq x \leq n \text{ et } l(x) = d\}$.

On introduit la notation $pi(n)$ qui compte le nombre de nombres premiers impairs inférieurs à n.

Sont fournies dans un tableau en fin de note les valeurs des variables pour les nombres de 4 à 100.

On constate les régularités suivantes :

1) pour les nombres n de lettre a ou b, $pi(n) = pi(n-2) + 1$ (en effet, pour ces nombres n, $pp(n) = 0$, i.e. $n - 1$ est premier mais $n - 1$ n'a pas été compté comme nombre premier par $pi(n - 2)$, il faut donc ajouter 1 à $pi(n - 2)$ pour obtenir $pi(n)$) ;
2) pour les nombres n de lettre c ou d, $pi(n) = pi(n - 2)$ (pour la raison opposée à celle fournie dans la parenthèse ci-dessus) ;
3) pour les nombres n de lettre a ou c, $pi(n) = X_a(n) + X_c(n)$ et $X_b(n) = X_c(n)$ (et donc $pi(n) = X_a(n) + X_b(n)$) ; l'égalité $pi(n) = X_a(n) + X_c(n)$ se comprend aisément en montrant sur deux exemples qu'il y a autant de nombres premiers que de lettres qui se trouvent à leur gauche et qui sont des lettres a ou des lettres c (moyennant le passage imaginaire de la lettre c à gauche de $n + 1$ devant le nombre 3 qui n'a pas de lettre à sa gauche - on a coloré les nombres premiers en rouge et les lettres qui se trouvent à leur gauche en bleu).

   Illustration de $pi(18) = 6 = X_a(18) + X_c(18) = 4 + 2$:

   3 a 5 a 7 b 9 c 11 a 13 b 15 c 17 a (19)

   Illustration de $pi(28) = 8 = X_a(28) + X_c(28) = 4 + 4$:

   3 a 5 a 7 b 9 c 11 a 13 b 15 c 17 a 19 b 21 c 23 b 25 d 27 c (29)

Pour comprendre pourquoi $X_b(n) = X_c(n)$ pour les nombres de lettre a ou c, il s'agit de voir chaque lettre b comme signalant en quelque sorte l'entrée dans une séquence de nombres composés impairs successifs et chaque lettre c comme signalant la sortie d'une telle séquence (des sortes de parenthèses ouvrantes et fermantes se correspondant). Notons d'une même couleur les deux lettres b et c se correspondant sur l'exemple de 28 vu plus haut.

Illustration de $X_b(28) = X_c(28) = 4$:

$$3\ a\ 5\ a\ 7\ b\ 9\ c\ 11\ a\ 13\ b\ 15\ c\ 17\ a\ 19\ b\ 21\ c\ 23\ b\ 25\ d\ 27\ c\ 29$$

Pour les nombres de lettre b ou d, la compréhension est aisée en notant simplement qu'il manque la dernière parenthèse fermante, rendant le nombre $X_b(n)$ de b supérieur de 1 au nombre $X_c(n)$ de c ;

4) pour les nombres n de lettre b ou d, $pi(n) = X_a(n) + X_c(n) + 1$ et $X_b(n) = X_c(n) + 1$ (et donc $pi(n) = X_a(n) + X_b(n)$; le raisonnement est le même que ci-dessus, avec la nécessité d'ajouter 1 pour compter le fait que 3 est premier) ;

5) $X_a(n) + X_b(n) + X_c(n) + X_d(n) = \dfrac{n-2}{2}$ (il s'agit simplement ici de compter le nombre total de lettres, qui augmente de 1 à chaque nouveau nombre pair).

n	$l(n)$	$X_a(n)$	$X_b(n)$	$X_c(n)$	$X_d(n)$	$pi(n)$	$pi_{jum}(n)$	$\frac{n-2}{2}$
4	a	1	0	0	0	1	1	1
6	a	2	0	0	0	2	2	2
8	b	2	1	0	0	3	2	3
10	c	2	1	1	0	3	2	4
12	a	3	1	1	0	4	3	5
14	b	3	2	1	0	5	3	6
16	c	3	2	2	0	5	3	7
18	a	4	2	2	0	6	4	8
20	b	4	3	2	0	7	4	9
22	c	4	3	3	0	7	4	10
24	b	4	4	3	0	8	4	11
26	d	4	4	3	1	8	4	12
28	c	4	4	4	1	8	4	13
30	a	5	4	4	1	9	5	14
32	b	5	5	4	1	10	5	15
34	d	5	5	4	2	10	5	16
36	c	5	5	5	2	10	5	17
38	b	5	6	5	2	11	5	18
40	c	5	6	6	2	11	5	19
42	a	6	6	6	2	12	6	20
44	b	6	7	6	2	13	6	21
46	c	6	7	7	2	13	6	22
48	b	6	8	7	2	14	6	23
50	d	6	8	7	3	14	6	24
52	c	6	8	8	3	14	6	25
54	b	6	9	8	3	15	6	26
56	d	6	9	8	4	15	6	27
58	c	6	9	9	4	15	6	28
60	a	7	9	9	4	16	7	29
62	b	7	10	9	4	17	7	30
64	d	7	10	9	5	17	7	31
66	c	7	10	10	5	17	7	32
68	b	7	11	10	5	18	7	33
70	c	7	11	11	5	18	7	34
72	a	8	11	11	5	19	8	35
74	b	8	12	11	5	20	8	36
76	d	8	12	11	6	20	8	37
78	c	8	12	12	6	20	8	38
80	b	8	13	12	6	21	8	39
82	c	8	13	13	6	21	8	40
84	b	8	14	13	6	22	8	41
86	d	8	14	13	7	22	8	42
88	c	8	14	14	7	22	8	43
90	b	8	15	14	7	23	8	44
92	d	8	15	14	8	23	8	45
94	d	8	15	14	9	23	8	46
96	c	8	15	15	9	23	8	47
98	b	8	16	15	9	24	8	48
100	c	8	16	16	9	24	8	49

Doubles de pairs entre 2 nombres premiers, comptage de lettres, régularités (Denise Vella-Chemla, 3.1.2016)

Il s'agit d'étudier si certains comptages de lettres, codant certaines propriétés de nombres, permettraient de mettre au jour des régularités, qui amèneraient la possibilité d'effectuer certaines déductions.

On rappelle que deux nombres premiers jumeaux ont pour différence 2. Par exemple, 3 et 5 sont des nombres premiers jumeaux, 41 et 43 en sont également.

On a tenté, dans une note récente, d'utiliser un nouveau codage par booléens de propriétés de primalité en cherchant si ce codage était avantageux pour étudier la conjecture des nombres premiers jumeaux mais ce codage ne semblait rien apporter d'intéressant. Du coup, on a essayé de trouver des régularités dans un tableau qu'on avait utilisé lors d'un travail autour de la conjecture de Goldbach et il s'avère que le tableau en question recélait des régularités qui semblent permettre de caractériser les doubles de nombres premiers jumeaux. Il faudrait démontrer ces régularités, et étudier si elles permettraient (seules ou en leur ajoutant d'autres régularités identifiées précédemment) de déduire qu'il y a une infinité de couples de nombres premiers jumeaux.

On note $X_b(n)$ le nombre de décompositions de n de la forme *composé + premier* et $X_d(n)$ le nombre de décompositions de n de la forme *composé + composé* (on rappelle qu'on ne s'intéresse qu'aux décompositions d'un nombre pair comme somme de 2 nombres impairs avec le premier sommant inférieur ou égal au second et les 2 sommants supérieurs ou égaux à 3 ; par exemple, 18 a 4 décompositions $3+15$ de la forme *premier+composé*, $5+13$ et $7+11$ de la forme *premier+premier* et $9+9$ de la forme *composé+composé*).

On constate dans le tableau suivant que pour les nombres pairs n doubles d'un pair k entre 2 nombres premiers $k-1$ et $k+1$, et seulement pour eux (on les a colorés en bleu), il y a égalité des différences suivantes dans 5 lignes consécutives (annotées d'une croix) :

1) $|X_b(n-4) - X_b(n-6)| = |X_d(n-4) - X_d(n-6)|$,
2) $|X_b(n-2) - X_b(n-4)| = |X_d(n-2) - X_d(n-4)|$,
3) $|X_b(n) - X_b(n-2)| = |X_d(n) - X_d(n-2)|$,
4) $|X_b(n+2) - X_b(n)| = |X_d(n+2) - X_d(n)|$ et
5) $|X_b(n+4) - X_b(n+2)| = |X_d(n+4) - X_d(n+2)|$.

La colonne d'entête $\Delta_b(n)$ fournit la valeur de $|X_b(n) - X_b(n-2)|$ tandis que la colonne d'entête $\Delta_d(n)$ fournit la valeur de $|X_d(n) - X_d(n-2)|$.

n	$X_b(n)$	$X_d(n)$	$\Delta_b(n)$	$\Delta_d(n)$		n	$X_b(n)$	$X_d(n)$	$\Delta_b(n)$	$\Delta_d(n)$		n	$X_b(n)$	$X_d(n)$	$\Delta_b(n)$
18	0	1	0	1		46	2	1	0	0		74	4	3	2
20	1	0	1	1	×	48	0	3	2	2		76	4	3	0
22	1	0	0	0	×	50	2	2	2	1		78	2	6	2
24	0	1	1	1	×	52	3	1	1	1		80	5	3	3
26	1	0	1	1	×	54	1	4	2	3		82	5	3	0
28	1	0	0	0	×	56	4	1	3	3	×	84	1	7	4
30	0	2	1	2		58	3	2	1	1	×	86	5	3	4
32	2	0	2	2	×	60	0	5	3	3	×	88	5	3	0
34	1	1	1	1	×	62	4	1	4	4	×	90	0	9	5
36	0	2	1	1	×	64	2	3	2	2	×	92	6	3	6
38	2	0	2	2	×	66	1	5	1	2		94	5	4	1
40	1	1	1	1	×	68	5	1	4	4	×	96	2	7	3
42	0	3	1	2		70	3	4	2	3	×	98	6	4	4
44	2	1	2	2		72	2	5	1	1	×	100	4	6	2

Toujours trouver un nouveau couple de nombres premiers les plus proches possible (Denise Vella-Chemla, 8.2.16)

Il s'agit de démontrer que l'ensemble des couples de nombres premiers d'écart 2 est infini.

Le couple $(3, 5)$ fait partie de cet ensemble, ainsi que le couple $(41, 43)$.

Posons l'hypothèse que l'ensemble des couples de nombres premiers d'écart 2 est fini, i.e. qu'on a recensé tous les couples de tels nombres premiers (*les plus proches possible*).

Appelons le plus grand de ces couples (p_{petit}, p_{grand}).

Trouvons le plus petit entier naturel qui est solution de la disjonction combinatoire de systèmes de congruences suivante :

$$\begin{cases} x \equiv 0\ (6) \\ (x \equiv 0\ (5)) \vee (x \equiv 2\ (5)) \vee (x \equiv 3\ (5)) \\ (x \equiv 0\ (7)) \vee (x \equiv 2\ (7)) \vee (x \equiv 3\ (7)) \vee (x \equiv 4\ (7)) \vee (x \equiv 5\ (7)) \\ (x \equiv 0\ (11)) \vee (x \equiv 2\ (11)) \vee \ldots \vee (x \equiv 9\ (11)) \\ \ldots \\ (x \equiv 0\ (p_k)) \vee (x \equiv 2\ (p_k)) \vee \ldots \vee (x \equiv p_k - 2\ (p_k)) \\ \ldots \\ (x \equiv 0\ (p_{grand})) \vee (x \equiv 2\ (p_{grand})) \vee \ldots \vee (x \equiv p_{grand} - 2\ (p_{grand})) \end{cases}$$

Le théorème des restes chinois nous assure que chacun des systèmes de congruence de la disjonction de systèmes a une solution (les modules étant tous des nombres premiers).

On est ainsi à la recherche d'un nombre x multiple de 6 et congru à $0, 2, \ldots, p_k - 2$ selon tous les nombres premiers p_k compris au sens large entre 5 et p_{grand}. Appelons x_k le nombre auquel x doit être congru selon le module p_k.

Le nombre x est un nombre pair entre 2 nombres premiers d'écart 2.

En effet, le nombre qui le précède, appelons-le p'_{petit}, est congru à 1 (2), à 2 (3), et à $x_k - 1$ (p_k) pour tout p_k compris au sens large entre 5 et p_{grand}. Il est donc premier. Non. On n'est assuré qu'il est premier que s'il est compris entre p_{grand} et $(p_{grand})^2$, ce qui n'est pas forcément le cas, le théorème chinois garantissant seulement l'existence d'une solution inférieure à $\#p_{grand} = \prod_{p_k=2}^{p_{grand}} p_k$ (aussi appelée primorielle de p_{grand}) qui est très supérieure à $(p_{grand})^2$. Peut-être est-il possible de dire que la combinatoire des systèmes de congruence fournit $\prod_{5 \leqslant p_k \leqslant p_{grand}} (p_k - 2)$ solutions différentes et que l'une au moins de ces solutions doit obligatoirement appartenir à l'intervalle $[p_k, (p_k)^2]$ dans la mesure où $\frac{\prod p_k}{\prod (p_k - 2)}$ est toujours inférieur strictement à $(p_k)^2 - p_k$ mais un tel raisonnement ne peut se tenir que si l'on est sûr que les solutions sont bien équiréparties.

Le nombre qui le suit, appelons-le p'_{grand}, est quant à lui congru à 1 (2), à 1 (3), et à $x_k + 1$ (p_k) pour tout p_k compris au sens large entre 5 et p_{grand}. Il est donc premier également (même remarque : on n'est assuré de sa primalité que s'il est compris entre p_{grand} et $(p_{grand})^2$).

On a trouvé un nouveau couple (p'_{petit}, p'_{grand}) de nombres premiers d'écart 2, dont les deux nombres sont plus grands que p_{grand} qui était pourtant selon notre hypothèse le plus grand des nombres premiers les plus proches possible trouvé jusque là. L'hypothèse est contredite : on peut augmenter à l'infini la taille de l'ensemble des couples de nombres premiers les plus proches possible.

Ecriture p-adique, écriture en base p (Denise Vella-Chemla, 13.02.2016)

On écrit les nombres de 1 à 100 sous leur forme 2-adique, 3-adique, 5-adique et 7-adique. Les nombres premiers p (en bleu) ont évidemment leur "dernier caractère" non nul dans toutes les écritures autres que p-adique ; il s'agit du coefficient de la puissance nulle de p, noté à droite, comme dans la numération décimale. On ne notera pas par ... la répétition infinie d'un nombre dans son écriture p-adique, sur la gauche au début de chaque écriture entre crochets.

n	2-*adique*	3-*adique*	5-*adique*	7-*adique*	n	2-*adique*	3-*adique*	5-*adique*	7-*adique*
1	[1]	[1]	[1]	[1]	51	[51, 19, 3, 3, 3, 1]	[51, 24, 6, 0]	[51, 1, 1]	[51, 2, 2]
2	[2, 0]	[2]	[2]	[2]	52	[52, 20, 4, 4, 0, 0]	[52, 25, 7, 1]	[52, 2, 2]	[52, 3, 3]
3	[3, 1]	[3, 0]	[3]	[3]	53	[53, 21, 5, 5, 1, 1]	[53, 26, 8, 2]	[53, 3, 3]	[53, 4, 4]
4	[4, 0, 0]	[4, 1]	[4]	[4]	54	[54, 22, 6, 6, 2, 0]	[54, 0, 0, 0]	[54, 4, 4]	[54, 5, 5]
5	[5, 1, 1]	[5, 2]	[5, 0]	[5]	55	[55, 23, 7, 7, 3, 1]	[55, 1, 1, 1]	[55, 5, 0]	[55, 6, 6]
6	[6, 2, 0]	[6, 0]	[6, 1]	[6]	56	[56, 24, 8, 0, 0, 0]	[56, 2, 2, 2]	[56, 6, 1]	[56, 7, 0]
7	[7, 3, 1]	[7, 1]	[7, 2]	[7, 0]	57	[57, 25, 9, 1, 1, 1]	[57, 3, 3, 0]	[57, 7, 2]	[57, 8, 1]
8	[8, 0, 0, 0]	[8, 2]	[8, 3]	[8, 1]	58	[58, 26, 10, 2, 2, 0]	[58, 4, 4, 1]	[58, 8, 3]	[58, 9, 2]
9	[9, 1, 1, 1]	[9, 0, 0]	[9, 4]	[9, 2]	59	[59, 27, 11, 3, 3, 1]	[59, 5, 5, 2]	[59, 9, 4]	[59, 10, 3]
10	[10, 2, 2, 0]	[10, 1, 1]	[10, 0]	[10, 3]	60	[60, 28, 12, 4, 0, 0]	[60, 6, 6, 0]	[60, 10, 0]	[60, 11, 4]
11	[11, 3, 3, 1]	[11, 2, 2]	[11, 1]	[11, 4]	61	[61, 29, 13, 5, 1, 1]	[61, 7, 7, 1]	[61, 11, 1]	[61, 12, 5]
12	[12, 4, 0, 0]	[12, 3, 0]	[12, 2]	[12, 5]	62	[62, 30, 14, 6, 2, 0]	[62, 8, 8, 2]	[62, 12, 2]	[62, 13, 6]
13	[13, 5, 1, 1]	[13, 4, 1]	[13, 3]	[13, 6]	63	[63, 31, 15, 7, 3, 1]	[63, 9, 0, 0]	[63, 13, 3]	[63, 14, 0]
14	[14, 6, 2, 0]	[14, 5, 2]	[14, 4]	[14, 0]	64	[64, 0, 0, 0, 0, 0, 0]	[64, 10, 1, 1]	[64, 14, 4]	[64, 15, 1]
15	[15, 7, 3, 1]	[15, 6, 0]	[15, 0]	[15, 1]	65	[65, 1, 1, 1, 1, 1, 1]	[65, 11, 2, 2]	[65, 15, 0]	[65, 16, 2]
16	[16, 0, 0, 0, 0]	[16, 7, 1]	[16, 1]	[16, 2]	66	[66, 2, 2, 2, 2, 2, 0]	[66, 12, 3, 0]	[66, 16, 1]	[66, 17, 3]
17	[17, 1, 1, 1, 1]	[17, 8, 2]	[17, 2]	[17, 3]	67	[67, 3, 3, 3, 3, 3, 1]	[67, 13, 4, 1]	[67, 17, 2]	[67, 18, 4]
18	[18, 2, 2, 2, 0]	[18, 0, 0]	[18, 3]	[18, 4]	68	[68, 4, 4, 4, 4, 0, 0]	[68, 14, 5, 2]	[68, 18, 3]	[68, 19, 5]
19	[19, 3, 3, 3, 1]	[19, 1, 1]	[19, 4]	[19, 5]	69	[69, 5, 5, 5, 5, 1, 1]	[69, 15, 6, 0]	[69, 19, 4]	[69, 20, 6]
20	[20, 4, 4, 0, 0]	[20, 2, 2]	[20, 0]	[20, 6]	70	[70, 6, 6, 6, 6, 2, 0]	[70, 16, 7, 1]	[70, 20, 0]	[70, 21, 0]
21	[21, 5, 5, 1, 1]	[21, 3, 0]	[21, 1]	[21, 0]	71	[71, 7, 7, 7, 7, 3, 1]	[71, 17, 8, 2]	[71, 21, 1]	[71, 22, 1]
22	[22, 6, 6, 2, 0]	[22, 4, 1]	[22, 2]	[22, 1]	72	[72, 8, 8, 8, 0, 0, 0]	[72, 18, 0, 0]	[72, 22, 2]	[72, 23, 2]
23	[23, 7, 7, 3, 1]	[23, 5, 2]	[23, 3]	[23, 2]	73	[73, 9, 9, 9, 1, 1, 1]	[73, 19, 1, 1]	[73, 23, 3]	[73, 24, 3]
24	[24, 8, 0, 0, 0]	[24, 6, 0]	[24, 4]	[24, 3]	74	[74, 10, 10, 10, 2, 2, 0]	[74, 20, 2, 2]	[74, 24, 4]	[74, 25, 4]
25	[25, 9, 1, 1, 1]	[25, 7, 1]	[25, 0, 0]	[25, 4]	75	[75, 11, 11, 11, 3, 3, 1]	[75, 21, 3, 0]	[75, 0, 0]	[75, 26, 5]
26	[26, 10, 2, 2, 0]	[26, 8, 2]	[26, 1, 1]	[26, 5]	76	[76, 12, 12, 12, 4, 0, 0]	[76, 22, 4, 1]	[76, 1, 1]	[76, 27, 6]
27	[27, 11, 3, 3, 1]	[27, 0, 0, 0]	[27, 2, 2]	[27, 6]	77	[77, 13, 13, 13, 5, 1, 1]	[77, 23, 5, 2]	[77, 2, 2]	[77, 28, 0]
28	[28, 12, 4, 0, 0]	[28, 1, 1, 1]	[28, 3, 3]	[28, 0]	78	[78, 14, 14, 14, 6, 2, 0]	[78, 24, 6, 0]	[78, 3, 3]	[78, 29, 1]
29	[29, 13, 5, 1, 1]	[29, 2, 2, 2]	[29, 4, 4]	[29, 1]	79	[79, 15, 15, 15, 7, 3, 1]	[79, 25, 7, 1]	[79, 4, 4]	[79, 30, 2]
30	[30, 14, 6, 2, 0]	[30, 3, 3, 0]	[30, 5, 0]	[30, 2]	80	[80, 16, 16, 0, 0, 0, 0]	[80, 26, 8, 2]	[80, 5, 0]	[80, 31, 3]
31	[31, 15, 7, 3, 1]	[31, 4, 4, 1]	[31, 6, 1]	[31, 3]	81	[81, 17, 17, 1, 1, 1, 1]	[81, 0, 0, 0, 0]	[81, 6, 1]	[81, 32, 4]
32	[32, 0, 0, 0, 0, 0]	[32, 5, 5, 2]	[32, 7, 2]	[32, 4]	82	[82, 18, 18, 2, 2, 2, 0]	[82, 1, 1, 1, 1]	[82, 7, 2]	[82, 33, 5]
33	[33, 1, 1, 1, 1, 1]	[33, 6, 6, 0]	[33, 8, 3]	[33, 5]	83	[83, 19, 19, 3, 3, 3, 1]	[83, 2, 2, 2, 2]	[83, 8, 3]	[83, 34, 6]
34	[34, 2, 2, 2, 2, 0]	[34, 7, 7, 1]	[34, 9, 4]	[34, 6]	84	[84, 20, 20, 4, 4, 0, 0]	[84, 3, 3, 3, 0]	[84, 9, 4]	[84, 35, 0]
35	[35, 3, 3, 3, 3, 1]	[35, 8, 8, 2]	[35, 10, 0]	[35, 0]	85	[85, 21, 21, 5, 5, 1, 1]	[85, 4, 4, 4, 1]	[85, 10, 0]	[85, 36, 1]
36	[36, 4, 4, 4, 0, 0]	[36, 9, 0, 0]	[36, 11, 1]	[36, 1]	86	[86, 22, 22, 6, 6, 2, 0]	[86, 5, 5, 5, 2]	[86, 11, 1]	[86, 37, 2]
37	[37, 5, 5, 5, 1, 1]	[37, 10, 1, 1]	[37, 12, 2]	[37, 2]	87	[87, 23, 23, 7, 7, 3, 1]	[87, 6, 6, 6, 0]	[87, 12, 2]	[87, 38, 3]
38	[38, 6, 6, 6, 2, 0]	[38, 11, 2, 2]	[38, 13, 3]	[38, 3]	88	[88, 24, 24, 8, 0, 0, 0]	[88, 7, 7, 7, 1]	[88, 13, 3]	[88, 39, 4]
39	[39, 7, 7, 7, 3, 1]	[39, 12, 3, 0]	[39, 14, 4]	[39, 4]	89	[89, 25, 25, 9, 1, 1, 1]	[89, 8, 8, 8, 2]	[89, 14, 4]	[89, 40, 5]
40	[40, 8, 8, 0, 0, 0]	[40, 13, 4, 1]	[40, 15, 0]	[40, 5]	90	[90, 26, 26, 10, 2, 2, 0]	[90, 9, 9, 0, 0]	[90, 15, 0]	[90, 41, 6]
41	[41, 9, 9, 1, 1, 1]	[41, 14, 5, 2]	[41, 16, 1]	[41, 6]	91	[91, 27, 27, 11, 3, 3, 1]	[91, 10, 10, 1, 1]	[91, 16, 1]	[91, 42, 0]
42	[42, 10, 10, 2, 2, 0]	[42, 15, 6, 0]	[42, 17, 2]	[42, 0]	92	[92, 28, 28, 12, 4, 0, 0]	[92, 11, 11, 2, 2]	[92, 17, 2]	[92, 43, 1]
43	[43, 11, 11, 3, 3, 1]	[43, 16, 7, 1]	[43, 18, 3]	[43, 1]	93	[93, 29, 29, 13, 5, 1, 1]	[93, 12, 12, 3, 0]	[93, 18, 3]	[93, 44, 2]
44	[44, 12, 12, 4, 0, 0]	[44, 17, 8, 2]	[44, 19, 4]	[44, 2]	94	[94, 30, 30, 14, 6, 2, 0]	[94, 13, 13, 4, 1]	[94, 19, 4]	[94, 45, 3]
45	[45, 13, 13, 5, 1, 1]	[45, 18, 0, 0]	[45, 20, 0]	[45, 3]	95	[95, 31, 31, 15, 7, 3, 1]	[95, 14, 14, 5, 2]	[95, 20, 0]	[95, 46, 4]
46	[46, 14, 14, 6, 2, 0]	[46, 19, 1, 1]	[46, 21, 1]	[46, 4]	96	[96, 32, 0, 0, 0, 0, 0]	[96, 15, 15, 6, 0]	[96, 21, 1]	[96, 47, 5]
47	[47, 15, 15, 7, 3, 1]	[47, 20, 2, 2]	[47, 22, 2]	[47, 5]	97	[97, 33, 1, 1, 1, 1, 1]	[97, 16, 16, 7, 1]	[97, 22, 2]	[97, 48, 6]
48	[48, 16, 0, 0, 0, 0]	[48, 21, 3, 0]	[48, 23, 3]	[48, 6]	98	[98, 34, 2, 2, 2, 2, 0]	[98, 17, 17, 8, 2]	[98, 23, 3]	[98, 0, 0]
49	[49, 17, 1, 1, 1, 1]	[49, 22, 4, 1]	[49, 24, 4]	[49, 0, 0]	99	[99, 35, 3, 3, 3, 3, 1]	[99, 18, 18, 0, 0]	[99, 24, 4]	[99, 1, 1]
50	[50, 18, 2, 2, 2, 0]	[50, 23, 5, 2]	[50, 0, 0]	[50, 1, 1]	100	[100, 36, 4, 4, 4, 0, 0]	[100, 19, 19, 1, 1]	[100, 0, 0]	[100, 2, 2]

Si on écrit les nombres en base 2, 3, 5 ou 7 (l'écriture p-adique ci-dessus consiste à "cumuler les digits" de l'écriture en base p ci-dessous), les nombres premiers p sont également les nombres dont tous les derniers caractères p'-adiques sont non nuls avec $p' \neq p$.

n	*en base* 2	*en base* 3	*en base* 5	*en base* 7	n	*en base* 2	*en base* 3	*en base* 5	*en base* 7
1	01	01	01	01	51	0110011	01220	0201	0102
2	10	02	02	02	52	0110100	01221	0202	0103
3	011	10	03	03	53	0110101	01222	0203	0104
4	100	011	04	04	54	0110110	02000	0204	0105
5	0101	012	10	05	55	0110111	02001	0210	0106
6	0110	020	011	06	56	0111000	02002	0211	0110
7	0111	021	012	10	57	0111001	02010	0212	0111
8	1000	022	013	011	58	0111010	02011	0213	0112
9	01001	100	014	012	59	0111011	02012	0214	0113
10	01010	0101	020	013	60	0111100	02020	0220	0114
11	01011	0102	021	014	61	0111101	02021	0221	0115
12	01100	0110	022	015	62	0111110	02022	0222	0116
13	01101	0111	023	016	63	0111111	02100	0223	0120
14	01110	0112	024	020	64	1000000	02101	0224	0121
15	01111	0120	030	021	65	01000001	02102	0230	0122
16	10000	0121	031	022	66	01000010	02110	0231	0123
17	010001	0122	032	023	67	01000011	02111	0232	0124
18	010010	0200	033	024	68	01000100	02112	0233	0125
19	010011	0201	034	025	69	01000101	02120	0234	0126
20	010100	0202	040	026	70	01000110	02121	0240	0130
21	010101	0210	041	030	71	01000111	02122	0241	0131
22	010110	0211	042	031	72	01001000	02200	0242	0132
23	010111	0212	043	032	73	01001001	02201	0243	0133
24	011000	0220	044	033	74	01001010	02202	0244	0134
25	011001	0221	100	034	75	01001011	02210	0300	0135
26	011010	0222	0101	035	76	01001100	02211	0301	0136
27	011011	1000	0102	036	77	01001101	02212	0302	0140
28	011100	01001	0103	040	78	01001110	02220	0303	0141
29	011101	01002	0104	041	79	01001111	02221	0304	0142
30	011110	01010	0110	042	80	01010000	02222	0310	0143
31	011111	01011	0111	043	81	01010001	10000	0311	0144
32	100000	01012	0112	044	82	01010010	010001	0312	0145
33	0100001	01020	0113	045	83	01010011	010002	0313	0146
34	0100010	01021	0114	046	84	01010100	010010	0314	0150
35	0100011	01022	0120	050	85	01010101	010011	0320	0151
36	0100100	01100	0121	051	86	01010110	010012	0321	0152
37	0100101	01101	0122	052	87	01010111	010020	0322	0153
38	0100110	01102	0123	053	88	01011000	010021	0323	0154
39	0100111	01110	0124	054	89	01011001	010022	0324	0155
40	0101000	01111	0130	055	90	01011010	010100	0330	0156
41	0101001	01112	0131	056	91	01011011	010101	0331	0160
42	0101010	01120	0132	060	92	01011100	010102	0332	0161
43	0101011	01121	0133	061	93	01011101	010110	0333	0162
44	0101100	01122	0134	062	94	01011110	010111	0334	0163
45	0101101	01200	0140	063	95	01011111	010112	0340	0164
46	0101110	01201	0141	064	96	01100000	010120	0341	0165
47	0101111	01202	0142	065	97	01100001	010121	0342	0166
48	0110000	01210	0143	066	98	01100010	010122	0343	0200
49	0110001	01211	0144	100	99	01100011	010200	0344	0201
50	0110010	01212	0200	0101	100	01100100	010201	0400	0202

On essaie de comprendre l'action de la matrice M ci-dessous :

$$M = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Elle projette les vecteurs du plan sur la diagonale principale (de pente 45°).

Si on multiplie à droite et à gauche la matrice

$$M' = \begin{pmatrix} \frac{1}{3} & 0 \\ \\ 0 & \frac{2}{3} \end{pmatrix}$$

par M, on obtient :

$$MM'M = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \begin{pmatrix} \frac{1}{3} & 0 \\ \\ 0 & \frac{2}{3} \end{pmatrix} \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

En procédant de même avec :

$$M'' = \begin{pmatrix} \frac{1}{5} & 0 \\ \\ 0 & \frac{4}{5} \end{pmatrix}$$

on obtient :

$$MM''M = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

Effectivement, la forme de la matrice centrale :

$$M_p = \begin{pmatrix} \frac{1}{p} & 0 \\ \\ 0 & \frac{p-1}{p} \end{pmatrix}$$

a pour conséquence que :

$$MM_pM = \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

Pourquoi le contenu de la matrice centrale n'a-t-il aucune influence sur le résultat ?
Que font les 3 matrices ?
A quoi correspond cet état quasi-absorbant de la matrice M (cette indépendance du résultat obtenu de la matrice au milieu du produit si cette matrice est de la bonne forme) ?
Comment s'appelle une matrice qui contient le même élément partout ?

Petit pont vers la mécanique quantique (Denise Vella-Chemla, 20.3.2016)

Si on veut faire un lien entre l'approche que j'ai choisie et l'informatique quantique, il faut voir les 4 lettres comme correspondant aux 4 opérateurs intervenant dans l'algorithme quantique de Deutsch (se reporter à la page 3 du document http://denise.vella.chemla.free.fr/Deutsch-Shor-Algo-Quant.pdf où sont fournies les matrices en question).

Mais je crois que son approche est probabiliste alors que la mienne ne l'est pas : quand j'étudie les décompositions de Goldbach d'un nombre n, en mettant face à face les impairs complémentaires à n, et en associant à chacun d'entre eux un booléen de primalité, tout est complètement déterminé.

Les matrices 4×4 correspondant aux 4 lettres a, b, c, d sont :

$$M_a = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M_b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$M_c = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$M_d = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

N'importe quoi : ces matrices-là ne respectent pas "mes" règles :

$$aa \rightarrow a, ab \rightarrow b, ac \rightarrow a, ad \rightarrow b,$$
$$ba \rightarrow a, bb \rightarrow b, bc \rightarrow a, bd \rightarrow b,$$
$$ca \rightarrow c, cb \rightarrow d, cc \rightarrow c, cd \rightarrow d,$$
$$da \rightarrow c, db \rightarrow b, dc \rightarrow c, dd \rightarrow d.$$

J'essaie désespérément depuis trois jours en programmant de trouver des matrices, ne serait-ce que 2×2, puis 3×3 qui respectent ces règles et je n'en trouve pas.

Ce qui serait peut-être intéressant, c'est de considérer que les lettres a, b, c et d caractérisent l'évolution de l'état du booléen de primalité, quand on passe d'un impair à l'impair suivant (les pairs ne sont jamais premiers sauf 2). Ainsi, selon le théorème des nombres premiers, la première matrice serait affectée de la probabilité d'occurrence $(1/ln\ n)^2$ caractérisant les possibilités indépendantes d'avoir deux nombres impairs consécutifs premiers tous les deux, la seconde et la troisième matrices seraient affectées de la pondération $(1/ln\ n)(1 - 1/ln\ n)(= (1 - 1/ln\ n)(1/ln\ n))$ et la quatrième matrice serait affectée de la pondération $(1 - 1/ln\ n)^2$ et on ferait "tourner tout ça" de manière quantique pour voir si cela nous enseigne quelque chose sur l'ensemble des nombres premiers.

Trouver des opérateurs qui vérifient les règles souhaitées (Denise Vella-Chemla, 26.3.2016)

On trouve des exemples de matrices 2×2 qui vérifient les règles de réécriture qu'on a identifiées :

$$a = c = \begin{pmatrix} -1 & -2 \\ 1 & 2 \end{pmatrix}$$

$$b = d = \begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{array}{c} aa = a, ab = b, ac = a, ad = b, \\ ba = a, bb = b, bc = a, bd = b, \\ ca = c, cb = d, cc = c, cd = d, \\ da = c, db = d, dc = c, dd = d. \end{array}$$

Les 4 matrices sont idempotentes : elles sont égales à l'une de leur quelconque puissance.

On aimerait trouver d'autres exemples qui permettraient de distinguer a de c et b de d car a nous a servi à représenter les décompositions de n de la forme $premier + premier$ tandis que c a été utilisé pour représenter les décompositions de la forme $premier + composé$.

Entrechocs, entrelacs (Denise Vella-Chemla, 3.4.2016)

L'idée de cette note est de voir les nombres comme des particules.

On a une chaîne de booléens de primalité, sur laquelle on va effectuer des traitements, avec en tête des notions telles que le passage du temps ou le changement d'état.

La séquence de booléens qui code la primalité des entiers, commence pour les impairs de 3 à 49 par[1] :

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

On la concatène à elle-même et on choisit de la décaler à droite ainsi :

$$\begin{array}{cccccccccccccccccccccc} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & \ldots \\ & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \ldots \end{array}$$

On code alors par des lettres les doublons de booléens obtenus aux positions successives :

$$\begin{array}{cccccccccccccccccccccc} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & \ldots \\ & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \ldots \\ & a & a & c & b & a & c & b & a & c & b & c & d & b & a & c & d & b & c & b & a & c & \ldots \end{array}$$

Puis on réitère, en considérant les doublons de booléens contenant un booléen de la chaîne décalée courante et le booléen à la même position de la chaîne initiale.

$$\begin{array}{cccccccccccccccccccccc} 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & \ldots \\ & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & \ldots \\ & a & a & c & b & a & c & b & a & c & b & c & d & b & a & c & d & b & c & b & a & c & \ldots \\ & & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & \ldots \\ & & a & c & a & b & c & a & b & c & a & d & c & b & b & c & c & b & d & a & b & c & \ldots \\ & & & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & \ldots \\ & & & c & a & a & d & a & a & d & a & c & d & a & b & d & c & a & d & b & a & d & \ldots \\ & & & & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & \ldots \\ & & & & a & a & c & b & a & c & b & c & c & b & a & d & d & a & c & b & b & c & \ldots \end{array}$$

Ce faisant, on comprend qu'on a étudié les doublons de booléens directement issus de la chaîne initiale, selon qu'ils étaient à telle ou telle distance (ce qu'on appelle le décalage) les uns des autres.

Si on considère que la chaîne initiale représente les états successifs d'une particule unique, on analyse en quelque sorte ce qui lui arrive lorsqu'elle passe de tel état e_i à tel état $e_{i+\Delta t}$. Une autre façon de voir est de considérer chaque entier comme une particule qui changerait d'état et qui aurait sa "ligne d'états" propre (représentée par une colonne ci-dessus).

Dans cette vision "multi-particules", on peut alors s'intéresser aux entrechocs ou collisions. Lorsque deux changements d'état ont lieu à proximité l'un de l'autre, ils ont pour conséquence un troisième changement d'état à l'instant immédiatement ultérieur (à proximité temporelle). On peut voir que ces liens entre changements d'état sont invariants. On les code par des règles.

$$\begin{array}{cccc} aa \to a & ba \to b & ca \to a & da \to b \\ ab \to a & bb \to b & cb \to a & db \to b \\ ac \to c & bc \to d & cc \to c & dc \to d \\ ad \to c & bd \to d & cd \to c & dd \to d \end{array}$$

Les règles ci-dessus sont obtenues en ne faisant que des décalages ("shift" en informatique) de la chaîne initiale. Si on s'autorise comme action sur les séquences de booléens, en plus des translations selon un certain décalage, le fait d'inverser complètement une chaîne de booléens (en utilisant la chaîne obtenue par symétrie-miroir) alors les règles deviennent :

$$\begin{array}{cccc} aa \to a & ba \to a & ca \to c & da \to c \\ ab \to b & bb \to b & cb \to d & db \to d \\ ac \to a & bc \to a & cc \to c & dc \to c \\ ad \to b & bd \to b & cd \to d & dd \to d \end{array}$$

[1] $3 \to 0$, $5 \to 0$, $7 \to 0$, $9 \to 1$, $11 \to 0$, $13 \to 0$, $15 \to 1$, ...

Ce sont ces règles-là qui nous ont permis de trouver l'explication qu'on cherchait au sujet de la conjecture de Goldbach, par de simples comptages d'occurrences de certaines lettres.

On a utilisé le mot "entrelacs" dans le titre car on observe bien la manière dont la symétrie-miroir a "entrelacé" les règles en intervertissant certaines lettres. Le mot "entrechocs" exprime lui le fait qu'on n'observe que les changements d'état proches, qui font penser à des collisions entre lettres. Mais il va sans dire que cette idée de collision provient du sens commun et qu'il n'y aurait, probabilistiquement parlant, pas lieu de s'intéresser à ces occurrences de lettres-là plutôt qu'à d'autres, qui seraient "temporellement" plus éloignées. Là aussi, le mot "temporellement" provient du sens commun. Il n'y a pas de temps ici, juste des lettres, données toutes d'un coup dans la globalité de notre champ de lettres, en n'ayant comme seule donnée initiale que la séquence des booléens de primalité. Dit plus brièvement, l'oracle sait "directement" si 145637807 est premier ou pas, puisqu'il a la connaissance de toutes les chaînes de causalité d'un coup.

Comment coder cela par des matrices, un peu à la manière de ce qui se fait en physique quantique ? Il faut trouver les probabilités des différents doublons de lettres : il y en a 16. On peut les coder dans une matrice de taille 4×4 ($p(xy)$ désigne la probabilité d'occurrence du doublon xy, on a vu qu'un doublon a toujours même conséquence, selon les règles invariantes de passage fournies plus haut) :

$$\begin{pmatrix} p(aa) & p(ab) & p(ac) & p(ad) \\ p(ba) & p(bb) & p(bc) & p(bd) \\ p(ca) & p(cb) & p(cc) & p(cd) \\ p(da) & p(db) & p(dc) & p(dd) \end{pmatrix}$$

Il faut garder à l'esprit qu'on pourrait augmenter l'information en calculant les probabilités d'occurrence d'une matrice de densité de "triplons" au lieu de doublons (*exemples de triplons* : $aaa, aab, aac, aad, aba, \ldots$). Cette matrice plus précise serait de taille $8 \times 8 = 64$, on remplacerait chacun des doublons (par exemple, le doublon aa) par une petite matrice 2×2 qui représenterait les probabilités d'occurrence des triplons aaa, aab, aac, aad.

Par programme, jusqu'à $13 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 = 30030$, on obtient la matrice des doublons :

$$\begin{pmatrix} 0 & 0 & 0 & 16\,585\,920 \\ 0 & 0 & 16\,585\,920 & 53\,308\,800 \\ 0 & 16\,591\,680 & 0 & 53\,308\,800 \\ 16\,585\,920 & 53\,227\,310 & 53\,290\,290 & 171\,300\,795 \end{pmatrix}$$

qu'on ramène à des proportions du nombre total de doublons :

$$\begin{pmatrix} 0 & 0 & 0 & 0.036793 \\ 0 & 0 & 0.036793 & 0.118258 \\ 0 & 0.036806 & 0 & 0.118258 \\ 0.036793 & 0.118077 & 0.118217 & 0.380005 \end{pmatrix}$$

La présence de 0 dans la matrice doit aisément s'expliquer : on a comptabilisé des disjonctions de critères de divisibilité satisfaits par des nombres séparés par les mêmes intervalles, selon des petits schémas comme celui-ci (représentant la transition ba, d'occurrence nulle dans la matrice) :

$$\begin{array}{ccc} b : x = 1 & \xrightarrow{+d} & y = 0 \\ \downarrow{\scriptstyle +1} & & \downarrow{\scriptstyle +1} \\ a : z = 0 & \xrightarrow{+d} & t = 0 \end{array}$$

Si par contre, on teste la primalité des entiers considérés, on obtient alors des matrices complètement remplies et symétriques (à erreurs près) comme celle-ci, calculée pour les entiers impairs inférieurs à 10000. Les totaux par ligne et par colonne sont proches.

$$\begin{pmatrix} 55611 & 290276 & 345326 & 1809753 \\ 290610 & 822809 & 1811656 & 5155669 \\ 344992 & 1809753 & 1134097 & 5994008 \\ 1809753 & 5155669 & 5994008 & 17161011 \end{pmatrix}$$

Plusieurs éléments ne sont pas satisfaisants : on devrait pouvoir ne fournir que les transitions d'un cran, les autres s'en déduisant par "fermeture" (élévation de la matrice à une certaine puissance). Mais on n'y arrive pas : la matrice qui code les transitions simples pour les impairs de 1 à 25 est :

$$\begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 0 & 3 & 0 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Le cumul de ses deux premières colonnes fournit le nombre de nombres premiers jusqu'à 25.

On aurait aimé qu'une puissance de cette matrice nous amène à celle-ci, qui code les transitions jusqu'à 30 (le cumul des 2 premières colonnes fournit $\pi(30)$) :

$$\begin{pmatrix} 1 & 3 & 0 & 0 \\ 0 & 0 & 3 & 1 \\ 3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

ou bien à celle-ci, qui code les transitions jusqu'à 50 :

$$\begin{pmatrix} 1 & 5 & 0 & 0 \\ 0 & 0 & 5 & 2 \\ 5 & 3 & 0 & 0 \\ 0 & 0 & 2 & 0 \end{pmatrix}$$

Mais bien-sûr, ça ne marche pas ; les puissances fournissent les transitions d'écart 4, puis d'écart 6, etc, sur la chaîne de booléens initiale mais ne permettent pas de l'étendre.

Transitions (Denise Vella-Chemla, 6.4.2016)

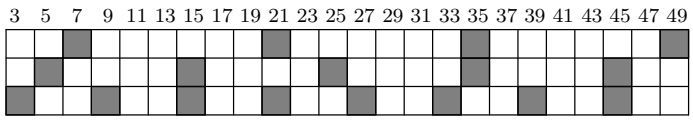
En ce moment, on essaie de comprendre les transitions. Ce qui pose souci par rapport à l'ensemble des nombres premiers, c'est le fait qu'on a le sentiment d'un certain déterminisme, qui cependant engendre du désordre. Et l'objectif est de modéliser ce déterminisme.

Il faut peut-être considérer de petites matrices 2×2 de la forme :

$$\begin{pmatrix} f_{aa} & f_{ab} \\ f_{ba} & f_{bb} \end{pmatrix}$$

avec $f_{ab} \neq f_{ba}$.

On revient sur nos grilles de divisibilité, qu'on a utilisées souvent pour comprendre la décomposition des nombres pairs en sommes de 2 nombres premiers (on ne s'occupe que des nombres impairs). Par exemple, la grille :



montre les nombres premiers jusqu'à 49 comme étant non-divisibles par 3, 5 et 7.

Concernant la divisibilité, on a en général en tête qu'un nombre a une chance sur 5 d'être divisible par 5 et 4 chances sur 5 de ne pas l'être. Il y a cependant une formulation plus précise, en terme de transitions, concernant la divisibilité par 5 (observer la seconde ligne de la grille) :

- une transition sur 5 fait passer d'un nombre divisible par 5 à un nombre non-divisible par 5 ;
- une transition sur 5 fait passer d'un nombre non-divisible par 5 à un nombre divisible par 5 ;
- 3 transitions sur 5 font passer d'un nombre non-divisible par 5 à un nombre non-divisible par 5 ;
- et enfin, aucune transition ne fait passer d'un nombre divisible par 5 à un autre le suivant juste.

On note cela par la matrice de passage suivante :

$$\begin{pmatrix} 0 & 1/5 \\ 1/5 & 3/5 \end{pmatrix}$$

Il faudrait combiner des matrices de la forme ci-dessous.

Matrice de divisibilité par 3 : $\begin{pmatrix} 0 & 1/3 \\ 1/3 & 1/3 \end{pmatrix}$

Matrice de divisibilité par 5 : $\begin{pmatrix} 0 & 1/5 \\ 1/5 & 3/5 \end{pmatrix}$

Matrice de divisibilité par 7 : $\begin{pmatrix} 0 & 1/7 \\ 1/7 & 5/7 \end{pmatrix}$

Matrice de divisibilité par p : $\begin{pmatrix} 0 & 1/p \\ 1/p & (p-2)/p \end{pmatrix}$

La combinaison des matrices de divisibilité par 3, 5 et 7 devrait représenter toutes les transitions possibles entre les différents nombres sachant que parmi eux, il s'en trouve un certain nombre qui sont divisibles par 3 ou bien par 5 ou bien par 7 (ce qui les empêche d'être premiers), d'autres ne sont divisibles que par l'un de 2 de ces nombres premiers sur les 3, d'autres seulement par 1 sur les 3, d'autres enfin par aucun. Le formalisme quantique devrait permettre de représenter toutes ces disjonctions de possibilités de transitions entre les différentes sortes de nombres.

Par exemple, le produit tensoriel entre les 2 premières matrices $\begin{pmatrix} 0 & 1/3 \\ 1/3 & 1/3 \end{pmatrix}$ et $\begin{pmatrix} 0 & 1/5 \\ 1/5 & 3/5 \end{pmatrix}$ permet d'obtenir la matrice :

$$\begin{pmatrix} 0\times 0 & 0\times 1/5 & 1/3\times 0 & 1/3\times 1/5 \\ 0\times 1/5 & 0\times 3/5 & 1/3\times 1/5 & 1/3\times 3/5 \\ 1/3\times 0 & 1/3\times 1/5 & 1/3\times 0 & 1/3\times 1/5 \\ 1/3\times 1/5 & /3\times 3/5 & 1/3\times 1/5 & 1/3\times 3/5 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1/15 \\ 0 & 0 & 1/15 & 3/15 \\ 0 & 1/15 & 0 & 1/15 \\ 1/15 & 3/15 & 1/15 & 3/15 \end{pmatrix}$$

de somme totale des probabilités valant bien 1.

La parité, si on avait voulu la prendre en considération, donne lieu à une matrice un peu différente des autres car elle a un 0 en bas à droite aussi.

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

Sa prise en compte aurait amené au produit tensoriel ci-dessous (on a sorti le dénominateur 30) :

$$\frac{1}{30}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 3 & 0 & 1 & 0 & 3 \\ 1 & 0 & 3 & 0 & 1 & 0 & 3 & 0 \end{pmatrix}$$

Matrices gigognes (Denise Vella-Chemla, 8.4.2016)

Cette note reprend simplement les matrices de la note Transitions ; elles sont gigognes du fait des produits qui opèrent tous les possibles.

Pour les transitions *"un pair succède à un impair, un impair succède à un pair"*, on a cette matrice :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

On omet le 1/2 devant.

On code les transitions *"un divisible par 3 est suivi par un non-divisible par 3 tandis qu'un non-divisible par 3 peut être suivi à égales proportions par un divisible ou par un non-divisible par 3"* par la matrice :

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

Les transitions pour la divisibilité par 5 sont notées dans la matrice :

$$\begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix}$$

Les transitions pour la divisibilité par 7 sont notées dans la matrice :

$$\begin{pmatrix} 0 & 1 \\ 1 & 5 \end{pmatrix}$$

Le produit tensoriel des 2 premières matrices vaut :

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Le produit des 3 premières matrices est égal à :

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

Le produit des 4 premières matrices est égal à :

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 3 & 1 & 3 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 3 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 5 & 0 & 0 & 1 & 5 \\ 0 & 1 & 0 & 3 & 0 & 1 & 0 & 3 \\ 1 & 5 & 3 & 15 & 1 & 5 & 3 & 15 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 5 & 3 & 15 \end{pmatrix}$$

Oublier la parité (divisibilité par 2) permet d'obtenir des matrices plus aisées à appréhender, les occurrences des nombres sont bien parallèles à la diagonale principale (ci-dessous, la matrice du produit des divisibilités par 3, 5, et 7).

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 3 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 5 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 1 & 5 & 3 & 15 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 5 & 0 & 0 & 1 & 5 \\ 0 & 1 & 0 & 3 & 0 & 1 & 0 & 3 \\ 1 & 5 & 3 & 15 & 1 & 5 & 3 & 15 \end{pmatrix}$$

Tourner en rond (Denise Vella-Chemla, 19.4.2016)

On essaie d'établir un lien entre nos petites idées et la fonction ζ de Riemann.

On a trouvé, mais sans en avoir encore lu la démonstration, que les nombres premiers annulent la fonction f définie par :

$$f(n) = \sum_{b=2}^{n-1} \sum_{o=1}^{b} cos \frac{2\pi no}{b}$$

Cette nullité de f pour les nombres premiers provient du fait que la somme des diviseurs se calcule par une double somme presque identique à celle ci-dessus si ce n'est que b doit prendre pour la calculer des valeurs de 1 à n (plutôt que de 2 à $n-1$) et que la somme des sommes de cosinus correspondant aux valeurs 1 et n de b a pour valeur $1+n$ qui se trouve être exactement la somme des diviseurs de n lorsque n est un nombre premier.

La fonction zeta est définie par :

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

En particulier, si r est la partie imaginaire d'un nombre complexe annulant zeta, on définit :

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

La fonction f s'annule pour les nombres premiers et la fonction z s'annule pour les parties imaginaires des zéros de ζ et il faudrait établir un passage de f à z.

Par programme, la formule ne converge pas assez vite vers 0 et on trouve sur la toile ici :
http://math.stackexchange.com/questions/490308/show-how-to-calculate-the-riemann-zeta-function-for-the-first-non-trivial-zero
qu'il faut utiliser plutôt la formule

$$\frac{1}{1-2^{1-s}} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^s}$$

pour "voir rapidement l'annulation".

Sommes de 2 carrés (Denise Vella-Chemla, 24.4.2016)

Les nombres premiers de la forme $4n+1$ s'écrivent d'une unique manière comme somme de 2 carrés. Cela permet de les placer dans le plan complexe.

$5 = (2+i)(2-i)$	est	placé	au	point	$(2,1)$.
$13 = (3+2i)(3-2i)$	"	"	"	"	$(3,2)$.
$17 = (4+i)(4-i)$	"	"	"	"	$(4,1)$.
$29 = (5+2i)(5-2i)$	"	"	"	"	$(5,2)$.
$37 = (6+i)(6-i)$	"	"	"	"	$(6,1)$.
$41 = (5+4i)(5-4i)$	"	"	"	"	$(5,4)$.
$53 = (7+2i)(7-2i)$	"	"	"	"	$(7,2)$.
$61 = (6+5i)(6-5i)$	"	"	"	"	$(6,5)$.
$73 = (8+3i)(8-3i)$	"	"	"	"	$(8,3)$.
$89 = (8+5i)(8-5i)$	"	"	"	"	$(8,5)$.
$97 = (9+4i)(9-4i)$	"	"	"	"	$(9,4)$.

13 se trouve à une distance valant $\sqrt{2}$ de 5.

En annexe, on fournit les coordonnées des nombres premiers de la forme $4n+1$ inférieurs à 1000 (sous la forme $a+ib$ avec $a \geqslant b$).

Il y a même possibilité de définir une division en utilisant des réseaux de mailles carrées (la longueur de la maille du réseau valant p, le nombre premier considéré comme module).

La loi de réciprocité quadratique exprime que p est congru à un carré modulo q si et seulement si q est congru à un carré modulo p dès que l'un seulement de p ou q est un nombre premier de la forme $4n+1$. Dans le cas où p et q sont tous les deux de la forme $4n+3$, il y a anti-réciprocité : p est congru à un carré modulo q si et seulement si q *n'est pas* congru à un carré modulo p.

On aimerait utiliser cette loi pour connaître un peu mieux l'ensemble des nombres premiers mais on ne sait pas comment "placer" les nombres premiers de la forme $4n+3$ dans le plan complexe d'une manière plus "équilibrée" que celle présentée dans l'article wikipedia consacré aux "entiers de Gauss". Les $4n+3$ sont tous placés sur l'axe des abscisses et n'ont qu'une coordonnée "valuée". On aimerait leur associer aussi 2 coordonnées, on ne sait encore comment, car cela nous permettrait, en attribuant un booléen de primalité à chacune desdites coordonnées, de revenir à un domaine plus familier.

On a pensé un tout petit temps utiliser le fait qu'un $4n+3$ est un $(4n+1)+2$. On a par exemple que $7 = 5+2 = ((2+i)(2-i)+\sqrt{2}i)((2+i)(2-i)-\sqrt{2}i)$ mais cette idée n'est pas bonne, de très nombreux $4n+1$ ne pouvant pas se mettre sous la forme unique d'une somme de deux carrés (comme par exemple 21 dont on souhaitait se servir pour "fabriquer" 23) et cette idée pose elle-aussi ce souci de la coordonnée "unique".

Les premiers $4n+3$, comme tous les impairs, sont des différences de 2 carrés, ou bien, comme tous les entiers, sont des sommes de 4 carrés, mais on sent bien que ce ne sont pas de bonnes idées non-plus. Il faudrait trouver un truc super-joli pour les $4n+3$, avec des quaternions ;-))

Annexe : Coordonnées des nombres premiers de la forme $4n+1$

$5=(2,1)$	$229=(15,2)$	$509=(22,5)$	$809=(28,5)$	$1109=(25,22)$
$13=(3,2)$	$233=(13,8)$	$521=(20,11)$	$821=(25,14)$	$1117=(26,21)$
$17=(4,1)$	$241=(15,4)$	$541=(21,10)$	$829=(27,10)$	$1129=(27,20)$
$29=(5,2)$	$257=(16,1)$	$557=(19,14)$	$853=(23,18)$	$1153=(33,8)$
$37=(6,1)$	$269=(13,10)$	$569=(20,13)$	$857=(29,4)$	$1181=(34,5)$
$41=(5,4)$	$277=(14,9)$	$577=(24,1)$	$877=(29,6)$	$1193=(32,13)$
$53=(7,2)$	$281=(16,5)$	$593=(23,8)$	$881=(25,16)$	$1201=(25,24)$
$61=(6,5)$	$293=(17,2)$	$601=(24,5)$	$929=(23,20)$	$1213=(27,22)$
$73=(8,3)$	$313=(13,12)$	$613=(18,17)$	$937=(24,19)$	$1217=(31,16)$
$89=(8,5)$	$317=(14,11)$	$617=(19,16)$	$941=(29,10)$	$1229=(35,2)$
$97=(9,4)$	$337=(16,9)$	$641=(25,4)$	$953=(28,13)$	$1237=(34,9)$
$101=(10,1)$	$349=(18,5)$	$653=(22,13)$	$977=(31,4)$	$1249=(32,15)$
$109=(10,3)$	$353=(17,8)$	$661=(25,6)$	$997=(31,6)$	$1277=(34,11)$
$113=(8,7)$	$373=(18,7)$	$673=(23,12)$	$1009=(28,15)$	$1289=(35,8)$
$137=(11,4)$	$389=(17,10)$	$677=(26,1)$	$1013=(23,22)$	$1297=(36,1)$
$149=(10,7)$	$397=(19,6)$	$701=(26,5)$	$1021=(30,11)$	$1301=(26,25)$
$157=(11,6)$	$401=(20,1)$	$709=(22,15)$	$1033=(32,3)$	$1321=(36,5)$
$173=(13,2)$	$409=(20,3)$	$733=(27,2)$	$1049=(32,5)$	$1361=(31,20)$
$181=(10,9)$	$421=(15,14)$	$757=(26,9)$	$1061=(31,10)$	$1373=(37,2)$
$193=(12,7)$	$433=(17,12)$	$761=(20,19)$	$1069=(30,13)$	$1381=(34,15)$
$197=(14,1)$	$449=(20,7)$	$769=(25,12)$	$1093=(33,2)$	$1409=(28,25)$
	$457=(21,4)$	$773=(22,17)$	$1097=(29,16)$	$1429=(30,23)$
	$461=(19,10)$	$797=(26,11)$		$1433=(37,8)$

Rectangles (Denise Vella-Chemla, 26.4.2016)

Il faudrait réfléchir aux petits schémas comme celui ci-dessous :

$$\begin{array}{ccc} x & \xrightarrow{+p} & y \\ \downarrow{\scriptstyle +q} & & \downarrow{\scriptstyle +q} \\ z & \xrightarrow{+p} & t \end{array}$$

Un tel schéma représente que $y = x + p, z = x + q$ et $t = (x + p) + q = (x + q) + p$.

On souhaite combiner ces schémas à des fonctions booléennes qui expriment le fait que x, y, z ou bien t sont divisibles ou pas par tel ou tel module premier p ou q.

On représentera cela directement sur le petit schéma, sans rajouter un niveau de flèche vers les booléens qui rendrait le dessin illisible.

On avait un peu étudié cela dans une note Fractales, symétrie et conjecture de Goldbach (p.6 et 7).

Il faudrait étudier les possibilités combinatoires qui lient deux tels schémas, l'un selon un module p, l'autre selon un module q, avec p et q premiers.

On a le schéma :

$$\begin{array}{ccc} p|x & \xrightarrow{+kp} & p|y \\ \downarrow{\scriptstyle +q} & & \downarrow{\scriptstyle +q} \\ p \not| z & \xrightarrow{+kp} & p \not| t \end{array}$$

si $p \wedge q = 1$.

Par exemple, $(x = 6, y = 18, z = 13, t = 25, p = 3, q = 7)$ est une instance de ce schéma.

Ces schémas sont à rapprocher des règles de congruences $a \equiv b \ (mod\ p)$ et $c \equiv d \ (mod\ p)$ si et seulement si $a + c \equiv b + d \ (mod\ p)$ et $ac \equiv bd \ (mod\ p)$ mais ils permettraient d'étudier également les inégalités, sur lesquelles on peut parfois se prononcer mais pas toujours.

Pgcd, classique ou tropical (Denise Vella-Chemla, 29.4.2016)

On peut programmer la fonction qui renvoie le pgcd de deux nombres selon l'algorithme d'Euclide par :

```
#include <cmath>

int pgcd(int m, int n) {
  while (m != 0) { int r ;
    r = n % m ;
    n = m ;
    m = r ;
  }
  return(n) ;
}
```

Mais on peut également programmer cette fonction ainsi, en remplaçant l'addition habituelle par le max et la multiplication habituelle par la soustraction, comme cela se fait en algèbre tropicale. On remplace n par $n \oplus (n \oslash m)$ et m par $n \oslash (m \oplus (n \oslash m))$

```
#include <cmath>

int pgcd(int m, int n)
{
  if (m >= n) {int r ; r = m ; m = n ; n = r ;}

  while (m != 0) { int r ;
    r = n-max(m, n-m) ;
    n = max(m, n-m) ;
    m = r ;
  }
  return(n) ;
}
```

Cependant le premier petit échange de variables au début de la fonction laisse à désirer.

Cette idée permet-elle de préciser un peu la connaissance qu'on a de l'ensemble des nombres premiers ? On imagine l'ensemble $\mathbb{N}^*$. On applique la fonction *pgcd* à toute paire d'entiers, cette fonction munit l'ensemble des entiers d'une structure d'ordre partiel (1 est plus petit que tous les autres, un diviseur d est plus petit que tous ses multiples kd, k non nul, mais deux nombres premiers entre eux ne sont pas comparables). Les nombres à distance 1 de 1 (dans le graphe de divisibilité) sont les nombres premiers, les nombres composés ont au moins un premier entre eux-mêmes et 1. L'algèbre tropicale apporte peut-être quelque chose en terme de nombre de solutions de certaines équations polynomiales tropicales.

Entrelacs premiers (Denise Vella-Chemla, 4.5.2016)

On étudie la manière dont le théorème de Wilson permet de lier les nombres premiers à certaines permutations.

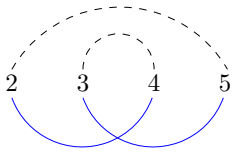
Le théorème de Wilson énonce que p est un nombre premier si et seulement si $(p-1)! \equiv -1 \ (mod\ p)$. Comme $p-1 \equiv -1 \ (mod\ p)$, cela équivaut à $(p-2)! \equiv 1 \ (mod\ p)$. Les nombres de 2 à $p-2$ (au nombre de $p-3$) peuvent être regroupés par 2 lorsque leur produit est congru à l'unité selon le module p (cf en annexe les articles 75 à 78 des Recherches arithmétiques de Gauss).

Illustrons sur quelques dessins la symétrie des *"entrelacs premiers"* découlant de ce théorème.

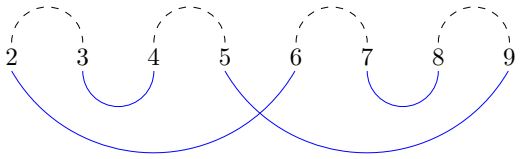
Selon le module 7 premier,

$$2.4 \equiv 8 \equiv 1 \ (mod\ 7)$$
$$3.5 \equiv 15 \equiv 1 \ (mod\ 7)$$

On lie les nombres 2 et 4 d'une part, 3 et 5 d'autre part, par des liens bleus, on complète le schéma par des liens pointillés pour fermer l'entrelacs (les liens bleus représentent ainsi des propositions logiques vraies (i.e. un lien bleu entre x et y représente la proposition $xy \equiv 1 \ (mod\ p)$) et les liens pointillés représentent des propositions logiques fausses). L'entrelacs obtenu est dénommé *entrelacs de Hopf*[1].

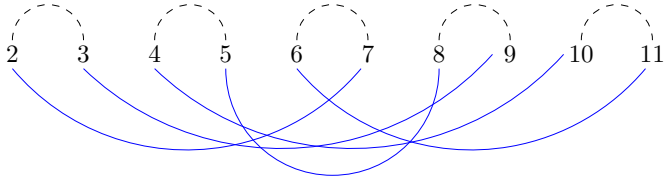


Selon le module 11 premier



[1]Maryam Mirzakhani trace au tableau des dessins similaires, lors d'un cours visionnable sur la toile, à la minute 2 derrière ce lien : *Dynamics of the moduli spaces of curves*. Les lignes ne se croisent pas dans le problème qu'elle présente.

Selon le module 13 premier

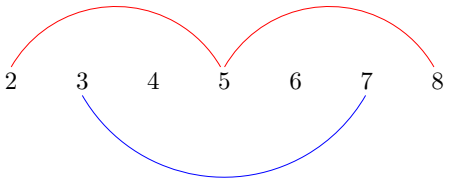


Les symétries autour de l'axe vertical passant par $p/2$ sont dûes au fait que $(p-x)(p-y) \equiv xy \ (mod\ p)$.

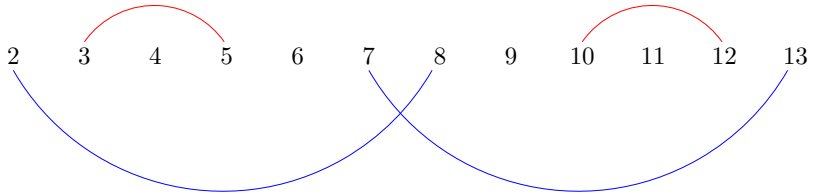
Selon les modules composés, tout nombre n'admet pas forcément un inverse dans $\mathbb{Z}/p\mathbb{Z}$. Dans $\mathbb{Z}/10\mathbb{Z}$ et $\mathbb{Z}/15\mathbb{Z}$, on trouve des paires de nombres dont le produit est congru à l'unité (notées par des liens bleus) mais on ne trouve pas systématiquement une telle paire de nombres (cf le module 8). Pour les modules composés, on note en rouge ci-dessous les paires de nombres dont le produit est congru à 0 selon le module considéré.

Selon le module 8 composé

Selon le module 10,



Selon le module 15,



On peut utiliser ces constatations pour associer à chaque nombre premier une permutation : elle envoie chaque nombre sur son inverse et on "complète les

trous" pour fermer l'entrelacs.

Ainsi la permutation que l'on associe au nombre premier 7 est

$$\begin{pmatrix} 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 2 \end{pmatrix}$$

et celle que l'on associe au nombre premier 11 est

$$\begin{pmatrix} 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 2 & 3 & 4 & 7 & 8 & 9 & 5 \end{pmatrix}.$$

On peut du même coup associer à chaque nombre premier p une matrice de permutation, moyennant un renommage des nombres de 2 à $p-2$ en leur prédécesseur de 1 à $p-3$; c'est une matrice carrée de taille $(p-3)\times(p-3)$. Celle associée au nombre premier 7 est

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

et celle associée au nombre premier 11^2 est

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Il faudrait chercher une opération sur les matrices de permutation que l'on pourrait mettre en correspondance avec la multiplication habituelle.

[2]Le renommage s'effectue ainsi (résultat en bleu) :

1	2	3	4	5	6	7	8
2	3	4	5	6	7	8	9
6	2	3	4	7	8	9	5
5	1	2	3	6	7	8	4

;

Annexe 1 : Articles 75 à 78 des Recherches arithmétiques de Carl-Friedrich Gauss

75. Avant d'abandonner ce sujet, nous présenterons quelques propositions qui ne nous paraissent pas indignes d'attention, à cause de leur simplicité.
Le produit de tous les termes de la période d'un nombre quelconque est $\equiv 1$ *quand leur nombre ou l'exposant auquel appartient le nombre dont il s'agit est impair, et* $\equiv -1$ *quand il est pair.*
Par exemple, pour le module 13, la période de 5 est composée des termes $1, 5, 12, 8$ dont le produit $480 \equiv -1$ (*mod* 13), suivant le même module, la période de 3 est composée des termes $1, 3, 9$, dont le produit $27 \equiv 1$ (*mod* 13).
Soit t l'exposant auquel le nombre appartient ; on peut toujours trouver (n°71) une base pour laquelle l'indice du nombre soit $\frac{p-1}{t}$. Or l'indice du produit de tous les termes sera

$$(1 + 2 + 3 + etc. + t - 1)\frac{p-1}{t} = \frac{(t-1)(p-1)}{2};$$

donc il sera $\equiv 0$ (*mod* $p-1$), quand t est impair et $\equiv \frac{p-1}{2}$ quand t est pair. Dans le premier cas, le produit est $\equiv 1$ (*mod* p) ; dans le second, $\equiv -1$ (*mod* p).

76. Si le produit du théorème précédent est une racine primitive, sa période comprendra tous les nombres $1, 2, 3, 4, \ldots p-1$, dont le produit sera par conséquent toujours $\equiv -1$; car $p-1$ est toujours pair, excepté dans le cas où $p = 2$, et alors on a indifféremment $+1$ ou -1. Ce théorème élégant qu'on énonce ordinairement de cette manière : *Le produit de tous les nombres plus petits qu'un nombre premier étant augmenté de l'unité, est divisible par ce nombre premier,* a été publié par *Waring* qui l'attribue à *Wilson* (*Meditationes Algeb. Ed. 3, p. 380*) ; mais aucun des deux n'a pu le démontrer, et *Waring* avoue que la démonstration lui en semble d'autant plus difficile qu'il n'y a point de *notation* par laquelle on puisse exprimer un nombre premier ; pour nous, nous pensons que la démonstration de cette sorte de vérités doit être puisé dans les principes plutôt que dans la notation. *Lagrange* en a depuis donné une démonstration (*Nouv. Mém. de l'Ac. de Berlin, 1771)*, dans laquelle il s'appuie sur la considération des coefficients que l'on trouve en développant le produit

$$(x+1)(x+2)(x+3)\ldots(x+p-1) :$$

et il fait voir qu'en supposant ce produit

$$= x^{p-1} + Ax^{p-2} + Bx^{p-3} + etc. + Mx + N,$$

les coefficients A, B, etc. M sont divisibles par p ; or

$$N = 1.2.3\ldots p-1$$

Maintenant si $x = 1$, le produit est divisible par p, mais alors il sera $\equiv 1 + N$ (*mod* p) donc $1 + N$ est divisible par p.
Enfin Euler *(Opusc. analyt. T.1, p.329)* en a donné une démonstration qui rentre dans celle que nous venons d'exposer ; ainsi puisque de tels hommes n'ont

pas cru ce sujet indigne de leurs méditations, nous espérons qu'on ne nous désapprouvera pas d'offrir encore ici une autre manière de démontrer ce théorème.

77. Nous dirons que deux nombres sont *associés*, comme l'a fait *Euler*, lorsque leur produit sera congru à l'unité. Cela posé, par la section précédente, tout nombre positif moindre que p, aura toujours un nombre associé moindre que p et il n'en aura qu'un ; or il est facile de prouver que parmi les nombres $1, 2, 3, -1$, il n'y a que 1 et $p-1$ qui soient eux-mêmes leurs associés, car ceux qui jouiront de cette propriété seront donnés par la congruence $x^2 \equiv 1$ qui ne peut avoir que 2 racines 1 et $p-1$. Supprimant donc ces deux nombres, les autres $2, 3, 4 \ldots p-2$, seront associés deux à deux, donc leur produit sera $\equiv 1$; enfin multipliant par $p-1$, le produit de tous $1.2.3.4 \ldots p-1 \equiv p-1 \equiv -1$.
Par exemple, pour $p = 13$, les nombres $2, 3, 4, 5, \ldots 11$ s'associent de la manière suivante : 2 avec 7, 3 avec 9, 4 avec 10, 5 avec 8, 6 avec 11 ; donc $2.3.4 \ldots 11 \equiv 1$, et partant..... $1.2.3 \ldots 12 \equiv 12 \equiv -1$.

78. Le théorème de *Wilson* peut être rendu plus général en l'énonçant comme il suit : *Le produit de tous les nombres premiers avec un nombre donné A et moindres que ce nombre, est congru suivant A, à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A = 4$; et positivement dans tous les autres cas. Le théorème de Wilson est contenu dans le premier cas. *Exemple.* Pour $A = 15$, le produit des nombres $1, 2, 4, 7, 8, 11, 13, 14$ est $\equiv 1$ (*mod* 15). Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de 2 racines, ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le n°75, si l'on y joint ce que nous dirons tout à l'heure des modules composés.

Annexe 2 : Article 41 des Recherches arithmétiques de Carl-Friedrich Gauss

Dans l'article 41 des Recherches arithmétiques de Gauss, on retrouve la notion de permutations et on pense aux travaux de Galois à venir.

41. *Si p est un nombre premier, et qu'on ait p choses parmi lesquelles il peut s'en trouver un certain nombre d'égales entre elles, pourvu que toutes ne le soient pas : le nombre des permutations de ces choses sera divisible par p.*

Par exemple, cinq choses A, A, A, B, B peuvent se disposer de dix manières différentes.

La démonstration de ce théorème se déduit facilement de la théorie connue des permutations. En effet, supposons que parmi ces p choses, il y en ait a égales à A, b égales à B, c égales à C etc., de sorte qu'on ait $a + b + c + etc = p$, les nombres a, b, c,etc. pouvant aussi désigner l'unité. Le nombre de permutations sera $= \dfrac{1.2.3 \ldots p}{1.2 \ldots a.1.2 \ldots b.1.2 \ldots c.etc.}$; or le numérateur est évidemment divisible

par le dénominateur, puisque le nombre des permutations est entier ; mais il est divisible par p, tandis que le dénominateur, qui est composé de facteurs plus petits que p, n'est pas divisible par p (n°15) ; donc le nombre des permutations sera divisible par p.

Nous espérons cependant que la démonstration suivante ne déplaira pas à quelques lecteurs.

Lorsque dans deux permutations l'ordre des choses ne différera qu'en ce que celle qui tient la première place dans l'une, en occupe une différente dans l'autre, mais que du reste toutes les autres choses, à partir de celle-là, suivent le même ordre dans chacune des permutations, de manière que la dernière de l'une se trouve placée immédiatement avant la première, dans l'autre ; nous les appellerons permutations semblables[3]. Ainsi $ABCDE$ et $DEABC$, $ABAAB$ et $ABABA$ seront semblables.

Or comme chaque permutation est composée de p choses, il est clair qu'on pourra en trouver $p-1$ semblables à une quelconque d'entre elles, si l'on met successivement à la seconde, à la troisième place, etc., la chose qui occupait la première ; donc si aucunes de ces permutations semblables ne sont identiques, il est évident que le nombre total des permutations sera égal à p fois le nombre des permutations dissemblables, et conséquemment sera divisible par p. Supposons que deux permutations semblables $PQ\dots TV\dots, V\dots YZPQ\dots T$ puissent être identiques, et que P qui occupe la première place dans la première, occupe la $n+1^{ième}$ dans la seconde : on aura dans la dernière série le $n+1^{ième}$ terme égal au 1^{er}, le $n+2^{ième}$ égal au $2^{ième}$, etc., d'où résulte que le $2n+1^{ième}$ est encore égal au premier et par conséquent le $3n+1^{ième}$, et généralement le $kn+m^{ième}$ égal au $m^{ième}$ (où quand $kn=m>p$, il faut imaginer qu'on reprenne toujours par le commencement, la série $V\dots T$, à moins qu'on ne retranche de $kn+m$, le multiple de p, qui en approche le plus en moins). Cela posé, si on détermine k de manière que $kn \equiv 1 \ (mod\ p)$, ce qui peut toujours se faire, puisque p est premier, il suivra de là que généralement le $m^{ième}$ terme serait égal au $m+1^{ième}$, c'est à dire qu'un terme quelconque serait égal au suivant, ou que tous les termes seraient égaux entre eux, ce qui est contre l'hypothèse.

[3]Si l'on écrivait en cercle les permutations semblables, de manière que la dernière chose touchât la première, il n'y aurait aucune différence entre elles, parce qu'aucune place ne peut s'appeler la première ni la dernière.

Cromagnon child (DV, 5.5.2016)

On fournit ci-dessous un programme d'une simplicité enfantine qui permet de savoir si un nombre est premier ou pas. Le titre provenait de l'écoute d'une conférence de Mikhaïl Gromov à la rencontre Abel in Paris 2015, je le trouvais chouette. Euh, il ne pouvait mieux tomber en fait puisque pour ce texte, j'ai perdu beaucoup de temps à réinventer la poudre, à retrouver que $\varphi(p) = p - 1 \iff p$ *est premier*. Le gamin de Cromagnon, sûr, n'y aurait pas passé la journée.

Ce programme calcule le produit de $\dfrac{1}{4}$ par le cardinal d'ensemble suivant :

$$R(n) = \#\{(x, y) \; tels \; que \; 2 \leqslant x \leqslant n-2 \; et \; 2 \leqslant y \leqslant n-2 \; et \; xy \equiv 1 \; (mod \; n)\}$$

Par exemple, $R(39) = 5.5$ car il y a 22 produits congrus à 1 modulo 39 qui sont $2 \times 20, 4 \times 10, 5 \times 8, 7 \times 28, 8 \times 5, 10 \times 4, 11 \times 32, 14 \times 14, 16 \times 22, 17 \times 23, 19 \times 37, 20 \times 2, 22 \times 16, 23 \times 17, 25 \times 25, 28 \times 7, 29 \times 35, 31 \times 34, 32 \times 11, 34 \times 31, 35 \times 29, 37 \times 19$ et parce que $\dfrac{1}{4} \times 22 = 5.5$. Constatons qu'il est important de distinguer par exemple le produit 7×28 du produit 28×7.

```
#include <iostream>
#include <cmath>

int main (int argc, char* argv[]) {
  int n, x, y ;
  float compteur ;

  for (n = 7 ; n <= 100 ; n=n+2) {
     compteur = 0.0 ;
     std::cout << n << " -> " ;
     for (x = 2 ; x <= n-2 ; ++x)
        for (y = 2 ; y <= n-2 ; ++y)
           if ((x*y) % n == 1)
        compteur = compteur+1 ;
     std::cout << (float) compteur/4.0 << "\n" ;
  }
}
```

Présentons le résultat de ce programme dans un tableau en séparant les nombres impairs de la forme $4k+3$ (colonnes bleues) des nombres impairs de la forme $4k+1$ (colonnes jaunes).

n	$R(n)$	n	$R(n)$	n	$R(n)$	n	$R(n)$
7	1	55	9.5	9	1	57	8.5
11	2	59	14	13	2.5	61	14.5
15	1.5	63	8.5	17	3.5	65	11.5
19	4	67	16	21	2.5	69	10.5
23	5	71	17	25	4.5	73	17.5
27	4	75	9.5	29	6.5	77	14.5
31	7	79	19	33	4.5	81	13
35	5.5	83	20	37	8.5	85	15.5
39	5.5	87	13.5	41	9.5	89	21.5
43	10	91	17.5	45	5.5	93	14.5
47	11	95	17.5	49	10	97	23.5
51	7.5	99	14.5	53	12.5		

Que constate-t-on ?

D'une part, on constate que pour les nombres impairs de la forme $4k+3$, si $R(n)$ est entier et s'il est égal à $\dfrac{n-3}{4}$, n est premier ; il est composé sinon.

D'autre part, pour les nombres impairs de la forme $4k+1$, si $R(n) = \dfrac{n-3}{4}$, n est premier ; il est composé sinon.

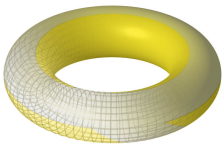
L'étude amène à comprendre que le nombre de produits xy qui sont congrus à l'unité modulo un nombre donné n et tels que x et y sont compris entre 2 et $n-2$, ces produits étant comptés doublement lorsque $x \neq y$ mais simplement lorsque $x = y$, est égal à $\frac{\varphi(n)-2}{4}$. Ce fait permet de distinguer aisément les nombres premiers des nombres composés. Il permet d'établir un lien entre le caractère de primalité de n et le nombre de points appartenant à la courbe d'équation $xy \equiv 1$ dans $\mathbb{Z}/n\mathbb{Z}$.
$(\frac{\varphi(n)-2}{4} = \frac{n-3}{4} \iff \varphi(n) = n-1)$.

Tore ∞-dimensionnel (DV, 8.5.2016)

On voudrait présenter ici un objet, classique pour les mathématiciens, mais qui semble correspondre au modèle de représentation des entiers qu'on a en tête depuis un certain temps et qui consiste à représenter les entiers par leurs restes dans les divisions euclidiennes par les différents nombres premiers.

Il s'agit du tore ∞-dimensionnel.

Le tore est le produit topologique de 2 cercles (il est engendré par la rotation d'un cercle autour d'un autre cercle). Voici le dessin d'un tore de dimension 2 extrait de l'article "théorème de Minkowski" de wikipedia.



Il faut imaginer le tore ∞-dimensionnel comme sous-tendant un réseau engendré par une infinité de cercles tournant les uns autour des autres.

Ce tore est dit ∞-dimensionnel parce qu'il y a une infinité de nombres premiers et que chaque rotation *sur* l'un des cercles correspond au fait de se promener dans $\mathbb{Z}/p\mathbb{Z}$, mais de manière continue (en considérant qu'il y aura lors de cette promenade continue trois "arrêts discrets" aux stations "reste 0 (mod 3)", "reste 1 (mod 3)" et "reste 2 (mod 3)" symbolisés habituellement par les trois sommets $e^0, e^{\frac{2i\pi}{3}}, e^{\frac{4i\pi}{3}}$ d'un triangle équilatéral sur le cercle unité).

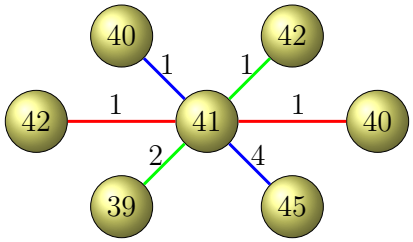
On voudrait se promener sur les "arêtes courbes" de cet objet (des arcs sur les cercles engendrant le tore), selon une promenade similaire à celle de l'algorithme du simplexe de Dantzig le long des arêtes d'un polyèdre convexe à n dimensions, si ce n'est que dans le cas du simplexe, n est fini. On rappelle l'algorithme du simplexe qui est géométriquement très simple : on cherche une solution optimale d'un système d'inéquations linéaires ; chaque itération de l'algorithme consiste à passer d'un sommet (face de dimension 0) du polyèdre convexe déterminé par les équations à un sommet adjacent en suivant une arête (face de dimension 1) particulière de ce polyèdre, de manière à faire décroître une fonction de coût.

D'une façon analogue, on souhaiterait que la promenade le long des arcs de cercles du tore ∞-dimensionnel permette idéalement d'atteindre un nombre premier à partir d'un autre, en ayant préalablement défini une distance qu'on chercherait à optimiser. Dans un premier temps, on pourrait se contenter de passer d'un sommet respectant certaines contraintes à un autre les respectant aussi toutes, ou bien en respectant certaines, ou bien n'en respectant aucune.

Pour illustrer ces idées, on se place en dimension 3 et on présente sur le dessin ci-dessous un *zoom* sur une portion du maillage sur laquelle on voit le nombre 41 et 6 de ses voisins sur le tore ∞-dimensionnel. Chaque direction correspond à un nombre premier p : le réseau de mailles rouges correspond au nombre premier 2, le réseau vert au nombre premier 3 et le réseau bleu au nombre premier 5. Jusque là, un nombre n (ou plutôt sa classe d'appartenance modulo p) avait comme voisins dans chaque direction les classiques $n-1$ et $n+1$ avec $\dot{0} = \dot{p}$ selon chaque direction du tore, dans la mesure où chaque direction correspond à l'un des groupes cycliques $\mathbb{Z}/p\mathbb{Z}$. Sur les arcs du schéma, on a noté la distance habituelle selon le nombre premier maille du réseau qui est la différence des restes. On a vu dans *Distance suprême* qu'une distance classique (racine de la somme des carrés des

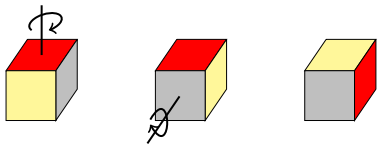
différences des coordonnées dans les différents réseaux) éloigne au maximum les nombres premiers de leurs 2 voisins classiques (prédécesseur et successeur au sens de l'arithmétique de Peano).

On voit qu'on a fait un autre choix de voisinage : un nombre (ici 41) ne se voit pas attribuer ses voisins "classiques" (40 et 42, $n-1$ et $n+1$ comme voisins de n). En effet, peut-être qu'il pourrait être sensé qu'un nombre ait comme voisins selon la direction p les nombres les plus proches de lui (au sens habituel sur les entiers), entre lesquels il se situe et qui sont divisibles par p ; par exemple, 41 est selon la direction (mod 5) compris entre 40 et 45. Il faut avoir à l'esprit que 40 et 45, puisqu'on est sur un tore, correspondent en fait au même point (ils sont tous les deux dans la classe d'équivalence $\dot{0}$ dans $\mathbb{Z}/5\mathbb{Z}$. Il faut noter que 2 points correspondent au nombre 42, ceci pour faciliter la lecture du dessin, mais ces points doivent être imaginés comme n'en étant qu'un seul.

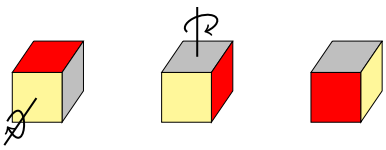


Il faudrait trouver une distance judicieuse. Toutes ces rotations, selon de multiples directions, donnent le tournis. Elles font penser à l'attraction *Danse avec les robots* du futuroscope de Poitiers, si ce n'est que les rotations dans ce cas, forcément, ne sont combinées que selon 3 directions.

On rappelle que la combinaison de 2 rotations est non-commutative. Pour le comprendre aisément, on peut penser à un cube posé sur la table : ses faces supérieure et inférieure sont rouges, ses faces latérales sont alternativement grises et jaunes, une face jaune est dirigée vers l'avant. Faisons subir au cube une rotation d'un quart de tour selon la direction verticale (sa face inférieure restant en contact intégral avec la table, i.e. sans renverser le cube), puis renversons le cube vers la droite (lui faisant ainsi subir une rotation d'axe horizontal traversant les faces avant et arrière en leur centre). La face rouge supérieure "devient" la face latérale droite du cube (on pense cela parce qu'on a comme "gardé la mémoire" d'un cube transparent qui sous-tendrait la coloration initiale du cube mais l'objet cube n'a évidemment pas changé).



Si on effectue les transformations dans l'ordre inverse, la face rouge supérieure est, dès la première rotation, "descendue en face latérale droite", et la deuxième rotation ne peut fatalement pas la laisser là, elle l'envoie vers l'avant du cube. On note systématiquement l'invariance des faces traversées par les axes de rotation.



G comme Gödel (Denise Vella-Chemla, 14.5.2016)

On s'interroge sur la possibilité d'utiliser un codage similaire à celui de Gödel pour transposer un problème additif en problème multiplicatif : on propose d'associer bijectivement à chaque entier impair compris entre 1 et 209 de restes modulaires α_1 (modulo 3), α_2 (modulo 5) et α_3 (modulo 7) l'entier dont la factorisation est $3^{\alpha 1}5^{\alpha 2}7^{\alpha 3}$. Trouver que le complémentaire de 13 (de restes $(1,3,6)$) à 210 (de restes $(0,0,0)$) est 197 (de restes $(2,2,1)$) est analogue au fait de trouver que $44118375 \times 1575 = 69486440625 = 3^3.5^5.7^7$. Mais cette transposition ne semble pas présenter un intérêt. On fournit dans les quatrièmes colonnes du tableau ci-dessous les images des nombres par cette bijection.

Plutôt que de partir dans cette direction qu'on abandonne, il vaut mieux vraisemblablement représenter les nombres par des matrices contenant de multiples rotations (en fait en nombre infini mais on va se limiter ici aux rotations selon les 3 nombres premiers 3, 5 et 7, d'autant plus que les rotations deviennent de plus en plus infimes au fur et à mesure, les nombres premiers grandissant apparaissant au dénominateur des expressions dénotant des angles).

On associe à l'entier 1 la matrice :

$$\begin{pmatrix} e^{\frac{2i\pi}{3}} & 0 & 0 \\ 0 & e^{\frac{2i\pi}{5}} & 0 \\ 0 & 0 & e^{\frac{2i\pi}{7}} \end{pmatrix}$$

qu'on peut aussi écrire :

$$\begin{pmatrix} cos(\frac{2i\pi}{3}) & -sin(\frac{2i\pi}{3}) & 0 & 0 & 0 & 0 \\ sin(\frac{2i\pi}{3}) & cos(\frac{2i\pi}{3}) & 0 & 0 & 0 & 0 \\ 0 & 0 & cos(\frac{2i\pi}{5}) & -sin(\frac{2i\pi}{5}) & 0 & 0 \\ 0 & 0 & sin(\frac{2i\pi}{5}) & cos(\frac{2i\pi}{5}) & 0 & 0 \\ 0 & 0 & 0 & 0 & cos(\frac{2i\pi}{7}) & -sin(\frac{2i\pi}{7}) \\ 0 & 0 & 0 & 0 & sin(\frac{2i\pi}{7}) & cos(\frac{2i\pi}{7}) \end{pmatrix}$$

On associe à 11 (de restes (2,1,4) modulo (3,5,7)) la matrice :

$$\begin{pmatrix} e^{\frac{\mathbf{2}.2i\pi}{3}} & 0 & 0 \\ 0 & e^{\frac{\mathbf{1}.2i\pi}{5}} & 0 \\ 0 & 0 & e^{\frac{\mathbf{4}.2i\pi}{7}} \end{pmatrix}$$

On associe à chaque entier une matrice diagonale de $\mathcal{M}_3(\mathbb{C})$ (idéalement, le nombre de nombres premiers étant infini, il faudrait considérer des matrices diagonales de $\mathcal{M}_\infty(\mathbb{C})$) ; la multiplication est commutative sur cet ensemble.

Il est important de ne pas "mélanger" les restes modulaires obtenus dans les différents corps ((2 mod 3, 4 mod 5) est différent de (2 mod 5, 4 mod 3)) ; un tel "mélange" se serait produit si on avait "agrégé" les multiples rotations en une seule[1]. La représentation permet de ne pas mélanger les restes parce qu'elle s'appuie sur l'ordre strict existant entre les nombres premiers (sur la diagonale apparaît d'abord l'exponentielle correspondant à la classe du nombre représenté dans $\mathbb{Z}/3\mathbb{Z}$, puis celle associée à sa classe dans $\mathbb{Z}/5\mathbb{Z}$, puis celle associée à sa classe dans $\mathbb{Z}/7\mathbb{Z}$, etc.).

Cette obligation de séparer les différents restes est lourde ; Gödel, lui, a trouvé un codage subtil : en utilisant les codages des lettres d'une expression comme les puissances des nombres premiers de factorisations, il obtient non seulement un codage absolument non-ambigu mais également une représentation agrégée en un nombre unique pour chaque programme.

Les nombres premiers ont un seul 1 sur leur diagonale (correspondant au seul reste nul dans la représentation par les restes). On n'a pas avancé d'un pouce.

[1] L'ambiguité aurait pu découler de la commutativité de la somme si on avait choisi de multiplier des exponentielles, ou bien de la commutativité du produit si on avait choisi des élévations à la puissance.

n	3	5	7	$f(n)$	n	3	5	7	$f(n)$	n	3	5	7	$f(n)$
1	1	1	1	105	71	2	1	1	315	141	0	1	1	35
3	0	3	3	42875	73	1	3	3	128625	143	2	3	3	385875
5	2	0	5	151263	75	0	0	5	16807	145	1	0	5	50421
7	1	2	0	75	77	2	2	0	225	147	0	2	0	25
9	0	4	2	30625	79	1	4	2	91875	149	2	4	2	275625
11	2	1	4	108045	81	0	1	4	12005	151	1	1	4	36015
13	1	3	6	44118375	83	2	3	6	132355125	153	0	3	6	14706125
15	0	0	1	7	85	1	0	1	21	155	2	0	1	63
17	2	2	3	77175	87	0	2	3	8575	157	1	2	3	25725
19	1	4	5	31513125	89	2	4	5	94539375	159	0	4	5	10504375
21	0	1	0	5	91	1	1	0	15	161	2	1	0	45
23	2	3	2	55125	93	0	3	2	6125	163	1	3	2	18375
25	1	0	4	7203	95	2	0	4	21609	165	0	0	4	2401
27	0	2	6	2941225	97	1	2	6	8823675	167	2	2	6	26471025
29	2	4	1	39375	99	0	4	1	4375	169	1	4	1	13125
31	1	1	3	5145	101	2	1	3	15435	171	0	1	3	1715
33	0	3	5	2100875	103	1	3	5	6302625	173	2	3	5	18907875
35	2	0	0	9	105	0	0	0	1	175	1	0	0	3
37	1	2	2	3675	107	2	2	2	11025	177	0	2	2	1225
39	0	4	4	1500625	109	1	4	4	4501875	179	2	4	4	13505625
41	2	1	6	5294205	111	0	1	6	588245	181	1	1	6	1764735
43	1	3	1	2625	113	2	3	1	7875	183	0	3	1	875
45	0	0	3	343	115	1	0	3	1029	185	2	0	3	3087
47	2	2	5	3781575	117	0	2	5	420175	187	1	2	5	1260525
49	1	4	0	1875	119	2	4	0	5625	189	0	4	0	625
51	0	1	2	245	121	1	1	2	735	191	2	1	2	2205
53	2	3	4	2701125	123	0	3	4	300125	193	1	3	4	900375
55	1	0	6	352947	125	2	0	6	1058841	195	0	0	6	117649
57	0	2	1	175	127	1	2	1	525	197	2	2	1	1575
59	2	4	3	1929375	129	0	4	3	214375	199	1	4	3	643125
61	1	1	5	252105	131	2	1	5	756315	201	0	1	5	84035
63	0	3	0	125	133	1	3	0	375	203	2	3	0	1125
65	2	0	2	441	135	0	0	2	49	205	1	0	2	147
67	1	2	4	180075	137	2	2	4	540225	207	0	2	4	60025
69	0	4	6	73530625	139	1	4	6	220591875	209	2	4	6	661775625

Programme préféré : les nombres premiers annulent une somme de cosinus (Denise Vella-Chemla, 21.5.2016)

Le programme en C++ ci-dessous, à compléter par un test de nullité (si ce n'est qu'en informatique, la nullité d'un flottant est testée à ε près), distingue les nombres premiers des nombres composés par calcul d'une somme de cosinus.

```
#include <iostream>
#include <cmath>
#include <stdio.h>
#define _USE_MATH_DEFINES

int main (int argc, char* argv[]) {
   float res ;
   int n, o, b ;

   for (n = 1 ; n <= 100 ; ++n) {
      printf("%d -> ", n) ;
      res = 0.0 ;
      for (b = 2 ; b <= n-1 ; ++b) {
         for (o = 1 ; o <= b ; ++o) {
            res=res+cos(2.0*M_PI*(float)n*(float)o/(float)b) ;
         }
      }
      printf("%f\n", res) ;
   }
}
```

Voici son résultat pour les entiers impairs jusqu'à 99. Le calcul renvoie 0 pour les nombres premiers et renvoie la somme des diviseurs propres de x pour x composé.

```
1 -> 0.000000
3 -> 0.000000
5 -> 0.000000
7 -> 0.000000
9 -> 3.000000
11 -> 0.000000
13 -> 0.000000
15 -> 8.000000
17 -> -0.000000
19 -> 0.000000
21 -> 10.000004
23 -> 0.000000
25 -> 5.000001
27 -> 12.000004
29 -> 0.000000
31 -> 0.000000
33 -> 14.000007
35 -> 12.000004
37 -> 0.000000
39 -> 16.000004
41 -> -0.000000
43 -> 0.000000
45 -> 31.999992
47 -> 0.000000
49 -> 7.000001
51 -> 20.000011
53 -> -0.000001
55 -> 16.000008
57 -> 21.999996
59 -> 0.000001
61 -> 0.000001
63 -> 39.999992
65 -> 17.999973
67 -> 0.000001
69 -> 26.000006
71 -> 0.000000
73 -> -0.000002
75 -> 47.999992
77 -> 18.000011
79 -> 0.000002
81 -> 38.999973
83 -> 0.000001
85 -> 21.999985
87 -> 32.000008
89 -> 0.000002
91 -> 19.999964
93 -> 34.000004
95 -> 23.999977
97 -> -0.000002
99 -> 55.999832
```

Coder (Denise Vella-Chemla, 21.5.2016)

On propose le codage des entiers supérieurs à 2 suivant :

$$g(x) = 2^{\alpha_1} 3^{\alpha_2} \dots p_k^{\alpha_k}$$

avec p_k un nombre premier inférieur ou égal à x et $\forall p_k, x \equiv \alpha_k \ (mod\ p_k)$.

x	2	3	5	7	11	13	17	19	$g(x)$
3	1	0							2
4	0	1							3
5	1	2	0						2.3^2
6	0	0	1						5
7	1	1	2	0					$2.3.5^2$
8	0	0	3	1					$5^3.7$
9	1	0	4	2					$2.5^4.7^2$
10	0	1	0	3					3.7^3
11	1	2	1	4					$2.3^2.5.7^4$
12	0	0	2	5	1				$5^2.7^5.11$
13	1	1	3	6	2	0			$2.3.5^3.7^6.11^2$
14	0	2	4	0	3	1			$3^2.5^4.11^3$
15	1	0	0	1	4	2			$2.7.11^4$
16	0	1	1	2	5	3			$3.5.7^2.11^5$
17	1	2	2	3	6	4	0		$2.3^2.5^2.7^3.11^6$
18	0	0	3	4	7	5	1		$5^3.7^4.11^7$
19	1	1	4	5	8	6	2	0	$2.3.5^4.7^5.11^8$
20	0	2	0	6	9	7	3	1	$3^2.7^6.11^9$

Les pairs ont pour images des impairs et inversement.

Un nombre premier a son image divisible par la primorielle du nombre premier qui le précède.

Tout diviseur d'un nombre ne divise pas l'image de ce nombre mais divise l'image de son successeur. Il y a comme une dualité, plus un nombre a de diviseurs, moins son image en a et inversement.

Fun !

Tamis (Denise Vella-Chemla, 12.6.2016)

Dans la suite, on note $x \ mod \ y$ le reste de la division euclidienne de x par y.

$$x \ mod \ y = x - \left\lfloor \frac{x}{y} \right\rfloor y$$

Les relations invariantes qui caractérisent la division euclidienne sur les entiers positifs sont $x = qy + k$ avec $k = x \ mod \ y$ et $qy \leqslant x < (q+1)y$.

Observons la table de restes qui fournit pour les entiers x de 2 à 20 leur reste dans les divisions euclidiennes par les entiers de 2 à x (en dernière colonne est calculée la somme des restes par ligne).

mod	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Σ
2	0																			$\rightarrow 0$
3	1	0																		$\rightarrow 1$
4	0	1	0																	$\rightarrow 1$
5	1	2	1	0																$\rightarrow 4$
6	0	0	2	1	0															$\rightarrow 3$
7	1	1	3	2	1	0														$\rightarrow 8$
8	0	2	0	3	2	1	0													$\rightarrow 8$
9	1	0	1	4	3	2	1	0												$\rightarrow 12$
10	0	1	2	0	4	3	2	1	0											$\rightarrow 13$
11	1	2	3	1	5	4	3	2	1	0										$\rightarrow 22$
12	0	0	0	2	0	5	4	3	2	1	0									$\rightarrow 17$
13	1	1	1	3	1	6	5	4	3	2	1	0								$\rightarrow 28$
14	0	2	2	4	2	0	6	5	4	3	2	1	0							$\rightarrow 31$
15	1	0	3	0	3	1	7	6	5	4	3	2	1	0						$\rightarrow 36$
16	0	1	0	1	4	2	0	7	6	5	4	3	2	1	0					$\rightarrow 36$
17	1	2	1	2	5	3	1	8	7	6	5	4	3	2	1	0				$\rightarrow 51$
18	0	0	2	3	0	4	2	0	8	7	6	5	4	3	2	1	0			$\rightarrow 47$
19	1	1	3	4	1	5	3	1	9	8	7	6	5	4	3	2	1	0		$\rightarrow 64$
20	0	2	0	0	2	6	4	2	0	9	8	7	6	5	4	3	2	1	0	$\rightarrow 61$

Chaque colonne de la table des restes, trivialement, contient une suite cyclique de nombres "retombant" régulièrement à zéro.

On définit pour les entiers supérieurs ou égaux à 2 la fonction $sr(x)$ (sr pour somme des restes) par :

$$sr(x) = \sum_{2 \leqslant y \leqslant x} x \ mod \ y$$

La fonction $sr(x)$ prend les valeurs suivantes (on note en troisième ligne le différentiel $sr(x) - sr(x-1)$) :

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$sr(x)$	0	1	1	4	3	8	8	12	13	22	17	28	31	36	36	51	47	64	61
$sr(x) - sr(x-1)$		1	0	3	−1	5	0	4	1	9	−5	11	3	5	0	15	−4	17	−3

Un nombre premier n'étant divisible par aucun nombre qui lui soit strictement inférieur, à part 1, on comprend aisément que tous les restes d'un nombre premier p sont des incréments stricts des restes du nombre $p-1$. On a donc :

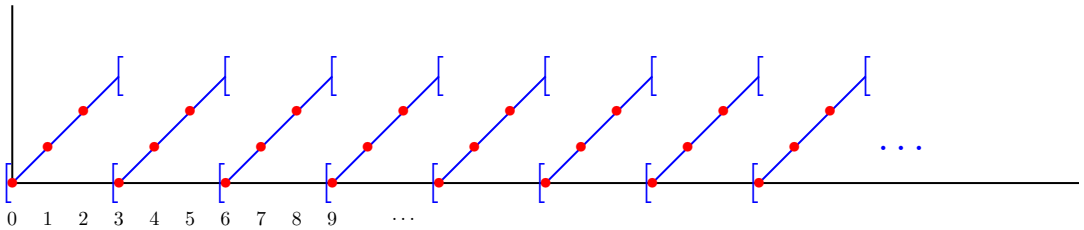
$$p \ premier \iff sr(p) - sr(p-1) = p - 2.$$

En utilisant la somme des diviseurs $\sigma(x)$ dont on fournit les premières valeurs, on obtient une définition par récurrence de la somme des restes :

$$\begin{cases} sr(2) = 0 \\ sr(x+1) = sr(x) - \sigma(x+1) + 2x + 1 \end{cases}$$

x	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$sr(x)$	0	1	1	4	3	8	8	12	13	22	17	28	31	36	36	51	47	64	61
$\sigma(x)$	3	4	7	6	12	8	15	13	18	12	28	14	24	24	31	18	39	20	42

On peut voir les restes comme autant de points discrets de fonctions continues par morceaux en dents de scie, qui sont du fait de l'ouverture/fermeture des intervalles, non dérivables pour les multiples, et qu'il s'agit de sommer. Par exemple, le graphe de la fonction en dents de scie fournissant les restes des divisions par 3 est :



Cette fonction périodique (y désignant le module) est définie par :

$$\begin{cases} f(x,y) & = x \ mod \ y \text{ si } 0 \leqslant \text{x} < \text{y} \\ f(x,y) & = f(x+y,y) \text{ si x} < 0 \\ f(x,y) & = f(x-y,y) \text{ si x} \geqslant \text{y}. \end{cases}$$

Cependant, la fonction *mod* n'étant pas polynomiale, on cherche plutôt une fonction qui, étant donnés deux entiers x et y, fournit le reste de la division euclidienne de x par y (noté $x \ mod \ y = k$), mais sans utiliser la fonction partie entière.

Prenons un exemple : $13 \ mod \ 5 = 3$ car 13 est compris entre $10 = 2 \times 5$ et $15 = 3 \times 5$ et $13 - 10 = 3$. Si on prend deux produits kx et $(k+1)x$ avec $k \geqslant 3$ et qu'on leur ôte 13, ces différences seront de même signe (positif). Si on prend deux produits kx et $(k+1)x$ avec $k < 2$ et qu'on leur ôte 13, les différences seront de même signe (négatif). Le seul cas où les différences kx et $(k+1)x$ sont de signe opposé est le cas où $k = 3 = 13 \ div \ 5$ (div désignant ici la division entière).

On remplace la définition habituelle de la division euclidienne par :

$$\forall x \in \mathbb{N}, \forall y \in \mathbb{N}\backslash\{0\}, x \ mod \ y = k$$

si et seulement si

$$\exists q \in \mathbb{N}, \exists k \in \mathbb{N}\backslash\{0\} \ tels \ que \begin{cases} x - qy = k \ et \\ (x-qy)(x-(q+1)y) \leqslant 0 \end{cases} \iff x^2 - (2q+1)xy + q(q+1)y^2 \leqslant 0$$

On réécrit cette équation d'inconnue q sous la forme habituelle selon les puissances décroissantes de q (x et y sont connues) :

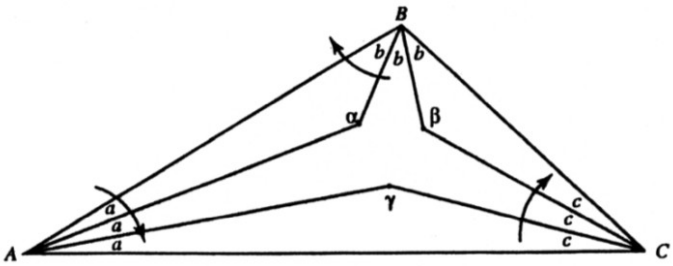
$$y^2q^2 + y(y-2x)q + x(x-y) \leqslant 0$$

Cette équation polynomiale du second degré définit une parabole. y^2 étant positif, la fonction décroît puis croît. Le sommet de la parabole est de coordonnées $\left(\frac{2x-y}{2y}; -\left(\frac{1}{2}y\right)^2\right)$.

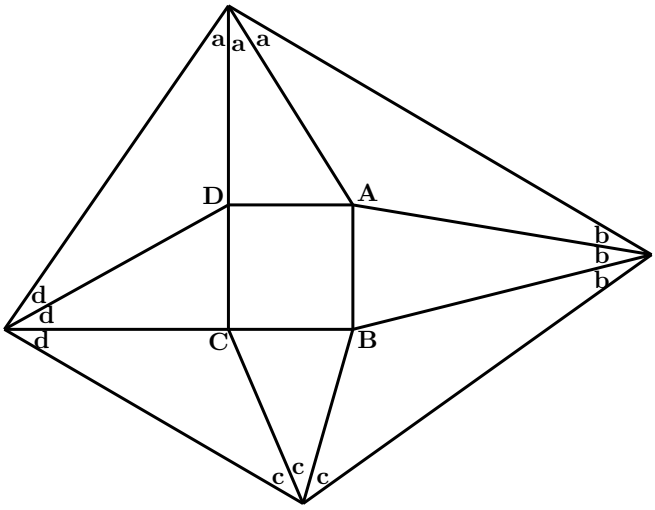
Quadrilatère quelconque, carré *(Denise Vella-Chemla, 23.6.2016)*

On aimerait considérer la droite du plan complexe contenant les points de partie réelle 1/2 comme l'axe vertical de symétrie du carré unité (de sommets $(0,0),(1,0),(0,1),(1,1)$). Le carré est attirant car il peut être considéré comme support du groupe diédral D_4. Le groupe D_4 quant à lui semble intéressant parce qu'il contient des opérations telles que l'échange de coordonnées ou bien le changement d'orientation et que ces opérations nous ont été très utiles dans un autre contexte. D'autre part, un théorème surprenant énonce que tout entier naturel peut être décomposé en somme de 4 carrés. Enfin, on a vu l'utilisation du beau théorème de Morley pour "symétriser" le triangle et on se demande si un théorème similaire ne permettrait pas de symétriser un quadrilatère quelconque.

On emprunte ce dessin au texte de la $181^{ème}$ conférence donnée par Alain Connes le 29 juin 2000 dans le cadre de l'Université de tous les savoirs et intitulée *Géométrie non commutative*. Il illustre le théorème de Morley selon lequel certains points d'intersection des droites qui trisectent les angles d'un triangle quelconque sont les sommets d'un triangle équilatéral.



Imaginons un dessin similaire liant un quadrilatère quelconque et sa symétrisation en un petit carré.



La symétrisation d'un quadrilatère quelconque, dont les longueurs des côtés seraient les 4 carrés α^2, β^2, γ^2 et λ^2 de la décomposition de $n = \alpha^2 + \beta^2 + \gamma^2 + \lambda^2$ en somme de 4 carrés permettrait peut-être de mettre au jour un morphisme qui associerait à chaque entier les 4 rotations utilisées aux 4 coins du quadrilatère quelconque.

On peut rêver.

En fait, deux petites animations gif trouvées sur la toile montre que les trissectrices des angles à l'oeuvre dans le théorème de Morley peuvent être vues comme provenant du dédoublement-éloignement des bissectrices desdits angles. A la recherche de la symétrisation du quadrilatère quelconque en utilisant les bissectrices, on trouve sur le site de Patrice Debart ici

$$http://debart.pagesperso-orange.fr/college/quadrilatere\_college.htmlch8$$

que les intersections des bissectrices intérieures d'un quadrilatère forment un quadrilatère inscriptible. On peut alors par exemple considérer un carré inscrit dans le cercle d'inscription du petit quadrilatère et qui partage un sommet avec lui comme carré symétrisant possible.

Petit pont entre grilles de divisibilité et D_4 (Denise Vella-Chemla, 26.6.2016)

On voudrait présenter ici le lien qu'on peut faire entre certains critères de primalité (dont on a étudié précisément le comportement dans ce qu'on avait appelé des grilles de divisibilité) et le groupe diédral D_4.

On a longuement observé, dans le cadre d'une étude de la conjecture de Goldbach, ce qu'on appelait des grilles de divisibilité des nombres pairs vus comme sommes de deux nombres impairs[1].

Ces grilles semblaient intéressantes car les doubles de nombres premiers ainsi que les doubles de nombres pairs compris entre deux nombres premiers étaient caractérisés par des grilles semblables du point de vue de leur dernière colonne.

Puis on a trouvé des éléments intéressants en écrasant l'information, i.e. en ne considérant plus la divisibilité d'un nombre par tous les nombres premiers inférieurs à sa racine mais en ne le représentant que très succinctement par un booléen qu'on a fixé à 0 si le nombre est premier et à 1 s'il est composé.

On met en oeuvre dans la présente approche ces deux idées : on se focalise sur les première et dernière colonnes des grilles, et on ne garde que des booléens succincts d'information. Cela va nous permettre d'établir un petit pont entre la modélisation choisie et D_4, le groupe diédral à 8 éléments.

On s'intéresse d'une part aux nombres $n-3$ intervenant dans la première colonne des grilles, celle-ci contenant les décompositions de la forme $n = 3 + (n-3)$ car le caractère de primalité de $n-3$ est le seul caractère de primalité supplémentaire (le seul élément d'information ajouté, qu'on note $b_1(n)$), quand on passe de la grille de divisibilité de n à celle de $n+2$. Le décomposant 3 ne voit pas son caractère de primalité changé, on s'en désintéresse ici. On s'intéresse d'autre part pour un nombre pair n aux caractères de primalité (qu'on note $b_2(n)b_3(n)$) des nombres de la décomposition dite médiane de n (cette décomposition médiane (notée $dm(n)$ est égale à $\frac{n}{2} + \frac{n}{2}$ si n est un $4k+2$ ou à $\frac{n-2}{2} + \frac{n+2}{2}$ si n est un $4k$ (les nombres de la dernière colonne des grilles).

Notons dans un tableau les booléens $b_1(n)b_2(n)b_3(n)$ pour les nombres pairs de 6 à 100.

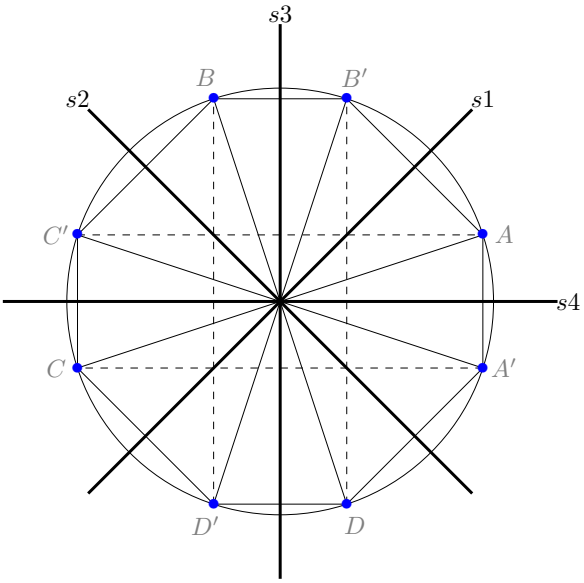
n	$n-3$	$dm(n)$	$b_1(n)b_2(n)b_3(n)$	n	$n-3$	$dm(n)$	$b_1(n)b_2(n)b_3(n)$
6	3	$3+3$	000	54	51	$27+27$	111
8	5	$3+5$	000	56	53	$27+29$	010
10	7	$5+5$	000	58	55	$29+29$	100
12	9	$5+7$	100	60	57	$29+31$	100
14	11	$7+7$	000	62	59	$31+31$	000
16	13	$7+9$	001	64	61	$31+33$	001
18	15	$9+9$	111	66	63	$33+33$	111
20	17	$9+11$	010	68	65	$33+35$	111
22	19	$11+11$	000	70	67	$35+35$	011
24	21	$11+13$	100	72	69	$35+37$	110
26	23	$13+13$	000	74	71	$37+37$	000
28	25	$13+15$	101	76	73	$37+39$	001
30	27	$15+15$	111	78	75	$39+39$	111
32	29	$15+17$	010	80	77	$39+41$	110
34	31	$17+17$	000	82	79	$41+41$	000
36	33	$17+19$	100	84	81	$41+43$	100
38	35	$19+19$	100	86	83	$43+43$	000
40	37	$19+21$	001	88	85	$43+45$	101
42	39	$21+21$	111	90	87	$45+45$	111
44	41	$21+23$	010	92	89	$45+47$	010
46	43	$23+23$	000	94	91	$47+47$	100
48	45	$23+25$	101	96	93	$47+49$	001
50	47	$25+25$	111	98	95	$49+49$	011
52	49	$25+27$	111	100	97	$49+51$	111

On constate bien-sûr des invariances dans ce tableau, dûes au fait que les nombres "avancent" progressivement dans les colonnes des grilles, mais il y a de toute façon une incertitude sur $b_1(n)$ qui empêche d'avancer.

[1] cf http://denise.vella.chemla.free.fr/grilles.pdf.

Les relations invariantes entre les valeurs des 3 booléens sont : $b_1(i) = b_2(2i), b_1(i) = b_3(2i-2), b_3(i) = b_2(i+1)$ et $(b_2(i) = b_2(i+1))$ ou exclusif $(b_3(i) = b_3(i+1))$. Bref, tout ça ne sert à rien : en ne se préoccupant que de la primalité de 3 nombres seulement, on ne bénéficie pas des effets du positionnemeent de l'espace et sa copie tête-bêche.

Le groupe D_4 est bien connu. On le représente graphiquement comme le groupe des transformations qui opèrent sur les points du graphique ci-dessous :



Si on note r_0, r_1, r_2, r_3 les rotations de 0 tour, 1/4 de tour, 1/2 tour, 3/4 de tour, et s_1, s_2 les symétries par rapport aux diagonales, s_3 la symétrie par rapport à l'axe des ordonnées et s_4 la symétrie par rapport à l'axe des abscisses, alors la table de Cayley du groupe D_4 est :

	r_0	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_0	r_0	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	r_0	s_4	s_3	s_1	s_2
r_2	r_2	r_3	r_0	r_1	s_2	s_1	s_4	s_3
r_3	r_3	r_0	r_1	r_2	s_3	s_4	s_2	s_1
s_1	s_1	s_3	s_2	s_4	r_0	r_2	r_1	r_3
s_2	s_2	s_4	s_1	s_3	r_2	r_0	r_3	r_1
s_3	s_3	s_2	s_4	s_1	r_3	r_1	r_0	r_2
s_4	s_4	s_1	s_3	s_2	r_1	r_3	r_2	r_0

On constate que par exemple $r_1 s_2 \neq s_2 r_1$.

La correspondance entre nos triplets de booléens et les points du plan complexe présentés ci-dessus peut par exemple associer aux nombres n tels que $b1(n) = 0$ l'un des points A, B, C ou D selon les valeurs de $b2(n)$ et $b3(n)$ et associer aux nombres n tels que $b1(n) = 1$ l'un des points A', B', C', D' à nouveau selon les valeurs de $b2(n)$ et $b3(n)$.

Matrices de passage entre les différents états (Denise Vella-Chemla, 11.7.2016)

Dans http://denise.vella.chemla.free.fr/petitpont.pdf, on a choisi de représenter chaque nombre pair n par un triplet de booléens $b_1(n)b_2(n)b_3(n)$ selon les caractères de primalité de $n-3$ et des deux nombres "autour de la moitié" de n (i.e. $\frac{n}{2}$ et $\frac{n}{2}$ si n est un $4k+2$ ou bien $\frac{n-2}{2}$ et $\frac{n+2}{2}$ si n est un $4k$).

Chaque triplet de booléens est le codage binaire d'un nombre compris entre 0 et 7 (par exemple, $000 = 0, 100 = 4$ et $111 = 7$).

Notre but est de dénombrer les fréquences d'apparition de certains motifs de passage d'un triplet de booléens à un autre lorsqu'on passe d'un nombre pair au suivant. Par programme, on calcule le contenu de matrices, chaque case contenant le nombre de passages de tel état à tel autre, pour n inférieur à certaines valeurs (de 10^3 à 10^8).

n nombre pair compris entre 6 et 1000

	000	001	010	011	100	101	110	111
000	3	7	0	0	13	24	0	0
001	0	0	0	0	0	0	0	18
010	12	0	0	0	18	0	0	0
011	0	0	0	14	0	0	15	43
100	10	12	0	0	23	27	0	0
101	0	0	0	13	0	0	0	38
110	21	0	0	0	18	0	0	0
111	0	0	30	45	0	0	24	70

n nombre pair compris entre 6 et 10 000

	000	001	010	011	100	101	110	111
000	3	32	0	0	43	156	0	0
001	0	0	0	0	0	0	0	107
010	55	0	0	0	99	0	0	0
011	0	0	0	116	0	0	91	527
100	36	75	0	0	171	279	0	0
101	0	0	0	77	0	0	0	357
110	139	0	0	0	248	0	0	0
111	0	0	154	541	0	0	296	1396

n nombre pair compris entre 6 et 100 000

	000	001	010	011	100	101	110	111
000	3	133	0	0	205	998	0	0
001	0	0	0	0	0	0	0	670
010	213	0	0	0	680	0	0	0
011	0	0	0	876	0	0	599	5215
100	140	537	0	0	1063	2759	0	0
101	0	0	0	528	0	0	0	3228
110	982	0	0	0	2551	0	0	0
111	0	0	893	5286	0	0	2934	19505

n nombre pair compris entre 6 et 1 000 000

	000	001	010	011	100	101	110	111
000	3	747	0	0	970	6989	0	0
001	0	0	0	0	0	0	0	4298
010	1101	0	0	0	4701	0	0	0
011	0	0	0	6319	0	0	4295	49075
100	793	3551	0	0	7365	25685	0	0
101	0	0	0	3529	0	0	0	29145
110	6811	0	0	0	24358	0	0	0
111	0	0	5802	49841	0	0	26874	237746

n nombre pair compris entre 6 et 10 000 000

	000	001	010	011	100	101	110	111
000	3	4456	0	0	5927	51023	0	0
001	0	0	0	0	0	0	0	30737
010	6790	0	0	0	34307	0	0	0
011	0	0	0	47732	0	0	30971	452633
100	4687	26281	0	0	54310	234289	0	0
101	0	0	0	25968	0	0	0	259343
110	49928	0	0	0	225023	0	0	0
111	0	0	41097	457636	0	0	243980	2712877

n nombre pair compris entre 6 et 100 000 000

	000	001	010	011	100	101	110	111
000	3	28841	0	0	37602	392018	0	0
001	0	0	0	0	0	0	0	229551
010	43330	0	0	0	262789	0	0	0
011	0	0	0	368139	0	0	237421	4161761
100	30300	200710	0	0	410298	2140463	0	0
101	0	0	0	199266	0	0	0	2333215
110	384830	0	0	0	2071082	0	0	0
111	0	0	306119	4199916	0	0	2218491	29743853

12.7.2016 : On réussit à identifier sur la matrice jusqu'à 1 000 000 quelques relations de proximité entre certaines différences qu'il faudrait expliquer, une fois identifié à quels passages ces nombres correspondent. On les note succinctement pour rappel au cas où...

- 1er nombre $\simeq$ 10ème nombre : $747 \simeq 793$;
- 4ème nombre $\simeq$ 8ème nombre : $4298 \simeq 4295$;
- 11ème nombre $\simeq$ 14ème nombre : $3551 \simeq 3529$;
- $|n_{16} - n_7| \simeq |n_7 - n_{18}|$: $6811 - 6319 \simeq 6319 - 5802$;
- $|n_{18} - n_{14}| \simeq |n_{15} - n_{20}|$: $5802 - 3529 \simeq 29145 - 26874$.
- $|n_{10} - n_1| + |n_{11} - n_{14}| + |n_5 - n_2| \simeq |n_9 + n_{13} + n_3| - |n_{19} + n_{17} + n_{12}|$:
  $(793 - 747) + (3551 - 3529) + (1101 - 970) \simeq (49841 + 24358 + 7365) - (49075 + 25685 + 6989)$.

13.7.2016 : rectification après de multiples calculs sur lesquels on n'arrive pas à sauter à pieds joints :

- les totaux par colonne et ligne sont égaux, forcément ;
- du coup, la somme des nombres dans la partie haute-droite des matrices est égale à la somme des nombres dans leur partie basse-gauche ;

- la somme des nombres des 4 premières colonnes (ou des 4 premières lignes) fournit le nombre de nombres premiers jusqu'à n, mais calculé selon qu'on entre ou sort d'un nombre premier, les matrices étant des matrices de passage (pour rappel, $\pi(10^3) = 168, \pi(10^4) = 1229, \pi(10^5) = 9592, \pi(10^6) = 78498, \pi(10^7) = 664579, \pi(10^8) = 5761455$) ;

- on a réussi à trouver une relation complètement exacte entre certaines cases :

$$||c38 - c46| - |c86 - c78|| = |c74 - c82|$$

- on a vérifié sur les 6 matrices le fait que les nombres des cases $c15$ et $c21$ d'une part, ou bien des cases $c25$ et $c46$ d'autre part, sont proches.

```
         3       747         0         0       970      6989         0         0
         0         0         0         0         0         0         0      4298
      1101         0         0         0      4701         0         0         0
         0         0         0      6319         0         0      4295     49075
       793      3551         0         0      7365     25685         0         0
         0         0         0      3529         0         0         0     29145
      6811         0         0         0     24358         0         0         0
         0         0      5802     49841         0         0     26874    237746
3  747  970  6989  4298  1101  4701  6319  4295  49075  793  3551  7365  25685
3529  29145  6811  24358  5802  49841  26874  237746  0
0 +- 1 = 744
0 +- 2 = 967
0 +- 3 = 6986
0 +- 4 = 4295
0 +- 5 = 1098
0 +- 6 = 4698
0 +- 7 = 6316
0 +- 8 = 4292
0 +- 9 = 49072
0 +- 10 = 790
0 +- 11 = 3548
0 +- 12 = 7362
0 +- 13 = 25682
0 +- 14 = 3526
0 +- 15 = 29142
0 +- 16 = 6808
0 +- 17 = 24355
0 +- 18 = 5799
0 +- 19 = 49838
0 +- 20 = 26871
0 +- 21 = 237743
1 +- 2 = 223
1 +- 3 = 6242
1 +- 4 = 3551
1 +- 5 = 354
1 +- 6 = 3954
1 +- 7 = 5572
1 +- 8 = 3548
1 +- 9 = 48328
1 +- 10 = 46
1 +- 11 = 2804
1 +- 12 = 6618
1 +- 13 = 24938
1 +- 14 = 2782
1 +- 15 = 28398
1 +- 16 = 6064
1 +- 17 = 23611
1 +- 18 = 5055
1 +- 19 = 49094
1 +- 20 = 26127
1 +- 21 = 236999
2 +- 3 = 6019
2 +- 4 = 3328
2 +- 5 = 131
2 +- 6 = 3731
2 +- 7 = 5349
2 +- 8 = 3325
2 +- 9 = 48105
2 +- 10 = 177
2 +- 11 = 2581
2 +- 12 = 6395
2 +- 13 = 24715
2 +- 14 = 2559
2 +- 15 = 28175
```

2 +- 16 = 5841
2 +- 17 = 23388
2 +- 18 = 4832
2 +- 19 = 48871
2 +- 20 = 25904
2 +- 21 = 236776
3 +- 4 = 2691
3 +- 5 = 5888
3 +- 6 = 2288
3 +- 7 = 670
3 +- 8 = 2694
3 +- 9 = 42086
3 +- 10 = 6196
3 +- 11 = 3438
3 +- 12 = 376
3 +- 13 = 18696
3 +- 14 = 3460
3 +- 15 = 22156
3 +- 16 = 178
3 +- 17 = 17369
3 +- 18 = 1187
3 +- 19 = 42852
3 +- 20 = 19885
3 +- 21 = 230757
4 +- 5 = 3197
4 +- 6 = 403
4 +- 7 = 2021
4 +- 8 = 3
4 +- 9 = 44777
4 +- 10 = 3505
4 +- 11 = 747
4 +- 12 = 3067
4 +- 13 = 21387
4 +- 14 = 769
4 +- 15 = 24847
4 +- 16 = 2513
4 +- 17 = 20060
4 +- 18 = 1504
4 +- 19 = 45543
4 +- 20 = 22576
4 +- 21 = 233448
5 +- 6 = 3600
5 +- 7 = 5218
5 +- 8 = 3194
5 +- 9 = 47974
5 +- 10 = 308
5 +- 11 = 2450
5 +- 12 = 6264
5 +- 13 = 24584
5 +- 14 = 2428
5 +- 15 = 28044
5 +- 16 = 5710
5 +- 17 = 23257
5 +- 18 = 4701
5 +- 19 = 48740
5 +- 20 = 25773
5 +- 21 = 236645
6 +- 7 = 1618
6 +- 8 = 406
6 +- 9 = 44374
6 +- 10 = 3908
6 +- 11 = 1150
6 +- 12 = 2664
6 +- 13 = 20984

6 +- 14 = 1172
6 +- 15 = 24444
6 +- 16 = 2110
6 +- 17 = 19657
6 +- 18 = 1101
6 +- 19 = 45140
6 +- 20 = 22173
6 +- 21 = 233045
7 +- 8 = 2024
7 +- 9 = 42756
7 +- 10 = 5526
7 +- 11 = 2768
7 +- 12 = 1046
7 +- 13 = 19366
7 +- 14 = 2790
7 +- 15 = 22826
7 +- 16 = 492
7 +- 17 = 18039
7 +- 18 = 517
7 +- 19 = 43522
7 +- 20 = 20555
7 +- 21 = 231427
8 +- 9 = 44780
8 +- 10 = 3502
8 +- 11 = 744
8 +- 12 = 3070
8 +- 13 = 21390
8 +- 14 = 766
8 +- 15 = 24850
8 +- 16 = 2516
8 +- 17 = 20063
8 +- 18 = 1507
8 +- 19 = 45546
8 +- 20 = 22579
8 +- 21 = 233451
9 +- 10 = 48282
9 +- 11 = 45524
9 +- 12 = 41710
9 +- 13 = 23390
9 +- 14 = 45546
9 +- 15 = 19930
9 +- 16 = 42264
9 +- 17 = 24717
9 +- 18 = 43273
9 +- 19 = 766
9 +- 20 = 22201
9 +- 21 = 188671
10 +- 11 = 2758
10 +- 12 = 6572
10 +- 13 = 24892
10 +- 14 = 2736
10 +- 15 = 28352
10 +- 16 = 6018
10 +- 17 = 23565
10 +- 18 = 5009
10 +- 19 = 49048
10 +- 20 = 26081
10 +- 21 = 236953
11 +- 12 = 3814
11 +- 13 = 22134
11 +- 14 = 22
11 +- 15 = 25594
11 +- 16 = 3260
11 +- 17 = 20807

11 +- 18 = 2251
11 +- 19 = 46290
11 +- 20 = 23323
11 +- 21 = 234195
12 +- 13 = 18320
12 +- 14 = 3836
12 +- 15 = 21780
12 +- 16 = 554
12 +- 17 = 16993
12 +- 18 = 1563
12 +- 19 = 42476
12 +- 20 = 19509
12 +- 21 = 230381
13 +- 14 = 22156
13 +- 15 = 3460
13 +- 16 = 18874
13 +- 17 = 1327
13 +- 18 = 19883
13 +- 19 = 24156
13 +- 20 = 1189
13 +- 21 = 212061
14 +- 15 = 25616
14 +- 16 = 3282
14 +- 17 = 20829
14 +- 18 = 2273
14 +- 19 = 46312
14 +- 20 = 23345
14 +- 21 = 234217
15 +- 16 = 22334
15 +- 17 = 4787
15 +- 18 = 23343
15 +- 19 = 20696
15 +- 20 = 2271
15 +- 21 = 208601
16 +- 17 = 17547
16 +- 18 = 1009
16 +- 19 = 43030
16 +- 20 = 20063
16 +- 21 = 230935
17 +- 18 = 18556
17 +- 19 = 25483
17 +- 20 = 2516
17 +- 21 = 213388
18 +- 19 = 44039
18 +- 20 = 21072
18 +- 21 = 231944
19 +- 20 = 22967
19 +- 21 = 187905
20 +- 21 = 210872

Polygones et circuits dans des graphes *(Denise Vella-Chemla, 19.6.2016)*

On est très attachée à une représentation des nombres par les restes de divisions euclidiennes. Ci-dessous, les restes dans les divisions euclidiennes par y compris entre 3 et 6 des nombres x compris entre 3 et 6.

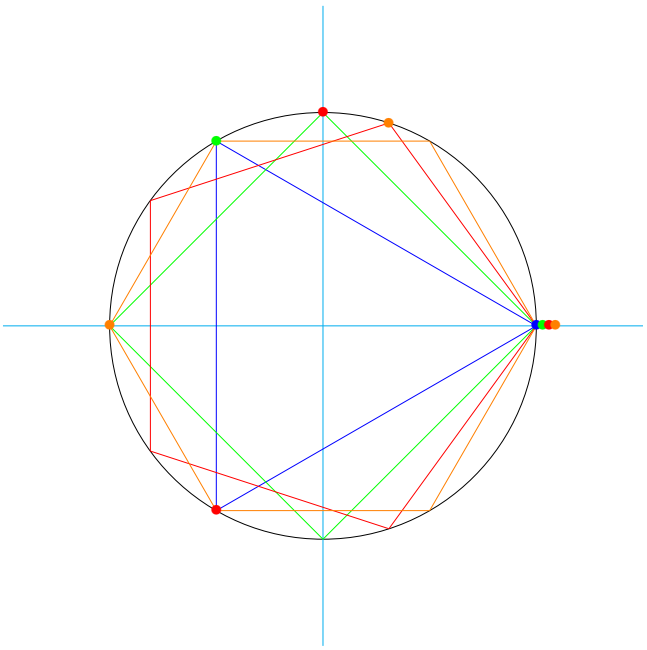
mod	3	4	5	6
3	0			
4	1	0		
5	2	1	0	
6	0	2	1	0

On associe à chaque entier n une séquence $G(n)$ de $n-2$ points du cercle-unité ainsi :

$$G(n) = \{e^{2i\pi x/y} \text{ et } n \geqslant y \geqslant 3 \text{ et } n \equiv x \ (mod\ y)\}$$

Un point peut apparaître plusieurs fois dans la séquence.

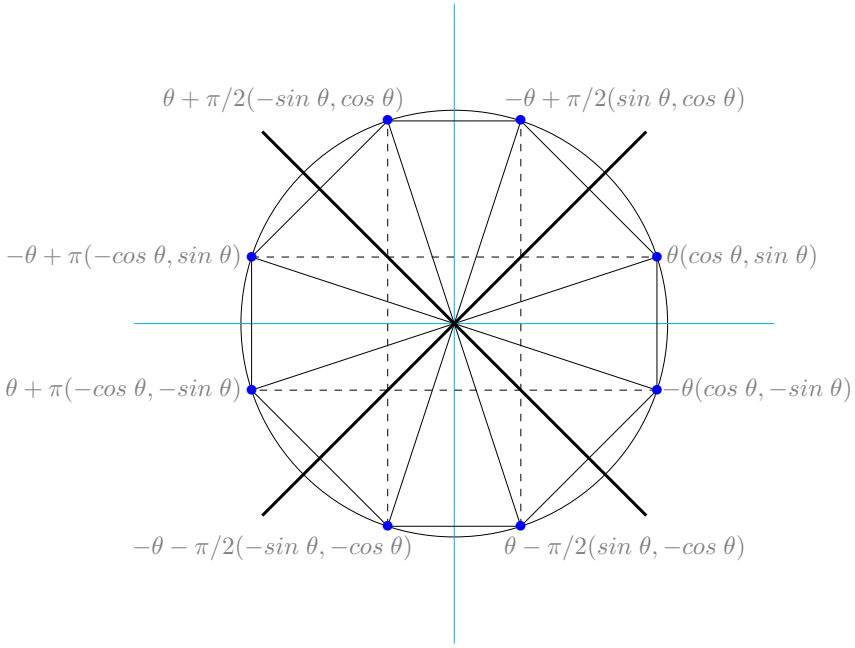
On a noté sur les triangle, carré, pentagone et hexagone ci-dessous, les points associés à 3 (en bleu), 4 (en vert), 5 (en rouge) et 6 (en orange) (on a écarté les points confondus en $(1,0)$ pour qu'ils soient visibles, le point orange en $(1,0)$ est double).



La séquence de points associée à un nombre premier ne contient qu'une occurrence du point $(1,0)$ alors que la séquence associée à un nombre composé en contient plusieurs (appelons ce point le "point-zéro"). On a simplement dit d'une autre manière qu'un nombre premier n'a aucun reste nul dans des divisions de diviseurs compris entre 3 et lui-même. Le fait de ne passer ainsi qu'une et une seule fois par le point-zéro pour les nombres premiers nous fait retrouver, un tout petit peu, Euler, Hamilton et leurs circuits.

Images *(Denise Vella-Chemla, 22.6.2016)*

On s'interroge sur deux transformations, qui semblent en lien avec nos recherches : celle consistant à échanger des coordonnées et celle consistant à inverser[1] l'orientation (qu'on a appelée "mettre tête-bêche"). Voyons ces transformations opérer sur un angle.



On aimerait bien comprendre comment se combinent ces 2 transformations parce qu'on s'est un peu familiarisée avec la somme des diviseurs, en programmant la récurrence d'Euler ; or la somme des diviseurs caractérise parfaitement les nombres premiers (p nombre premier a sa somme de diviseurs qui vaut $p+1$). Une autre récurrence existe pour la somme des diviseurs, plus simple à programmer mais d'origine moins claire, dont il semblerait qu'elle provienne d'une équation de Chazy, qui fait peut-être partie des équations de Painlevé VI ; tout ça est inaccessible, mais on a cependant lu que de telles équations sont liées au groupe diédral D_4 qui contient 8 éléments. Et comme le mot diédral fait penser à inversion et que la modélisation qu'on propose utilise 2 booléens, 4 lettres, 16 règles de réécriture, des échanges de coordonnées et/ou des orientations à opposer, peut-être y aurait-il moyen de relier tout ça, même si pour l'instant, c'est tout flou.

La composition des deux opérations qui consistent à échanger les coordonnées et à "opposer" l'abscisse, par exemple, est non-commutative :

Si on applique d'abord l'échange de coordonnées, puis le fait de prendre l'opposé de l'abscisse au point $\begin{pmatrix} cos\ \theta \\ sin\ \theta \end{pmatrix}$, on obtient d'abord $\begin{pmatrix} sin\ \theta \\ cos\ \theta \end{pmatrix}$ puis $\begin{pmatrix} -sin\ \theta \\ cos\ \theta \end{pmatrix}$ alors que si on effectue ces transformations dans l'ordre inverse, on obtient d'abord $\begin{pmatrix} -cos\ \theta \\ sin\ \theta \end{pmatrix}$ puis $\begin{pmatrix} sin\ \theta \\ -cos\ \theta \end{pmatrix}$.

Si on note $r_0, r_{1,2}, r_3$ les rotations de 0 tour, 1/4 de tour, 1/2 tour, 3/4 de tour, et s_1, s_2 les symétries par rapport aux diagonales, s_3 la symétrie par rapport à l'axe des ordonnées et s_4 la symétrie par rapport à l'axe des abscisses, alors la table de Cayley du groupe D_4 est :

[1] Le verbe opposer conviendrait mieux que le verbe inverser, au sens de prendre la direction opposée.

	r_0	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_0	r_0	r_1	r_2	r_3	s_1	s_2	s_3	s_4
r_1	r_1	r_2	r_3	r_0	s_4	s_3	s_1	s_2
r_2	r_2	r_3	r_0	r_1	s_2	s_1	s_4	s_3
r_3	r_3	r_0	r_1	r_2	s_3	s_4	s_2	s_1
s_1	s_1	s_3	s_2	s_4	r_0	r_2	r_1	r_3
s_2	s_2	s_4	s_1	s_3	r_2	r_0	r_3	r_1
s_3	s_3	s_2	s_4	s_1	r_3	r_1	r_0	r_2
s_4	s_4	s_1	s_3	s_2	r_1	r_3	r_2	r_0

On constate que par exemple $r_1 s_2 \neq s_2 r_1$.

```
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

for n in range(14,102,2):
  pix=0 ; pi2x = 0
  for compteprem in range(2,n+1,1):
    if (prime(compteprem)):
      if (compteprem <= n//2): pix=pix+1
      pi2x=pi2x+1
  xa=0 ; xb=0 ; xc=0 ; xd=0
  ya=0 ; yc=0
  za=0 ; zc=0
  zaprec = za ; zcprec = zc ; yaprec=ya ; ycprec=yc
  for x in range(3,n//2+1,2):
    if (prime(x)):
      if (prime(n-x)): xa=xa+1
      else: xc=xc+1
    else:
      if (prime(n-x)): xb=xb+1
      else: xd=xd+1
  for x in range(6,((n+4)//2)+1,2):
    if (prime(x-3)): za=za+1
    else: zc=zc+1
  if ((n//2) % 2 == 0): debuthaut=((n+4)//2)+2
  else: debuthaut = ((n+4)//2)+1
  for x in range(debuthaut, n+1, 2):
     if (prime(x-3)): ya=ya+1
     else: yc=yc+1
  pix=0 ; pi2x = 0
  for compteprem in range(2, n+1, 1):
     if (prime(compteprem)):
        if (compteprem <= n//2): pix=pix+1
        pi2x=pi2x+1
  print("\n",n,"  :  ")
  print("Xa ",xa, "Xb ",xb, "Xc ",xc, "Xd ",xd)
  print("Ya ",ya, "Yc ",yc)
  print("Za ",za, "Zc ",zc)
  print("(n-4)/4 ",(n-4)//4,"(n-2)/4", (n-2)//4)
  if ((n%4) == 0): print("bool_4k+2 0 ")
  else:
    print("bool_4k+2 1 ")
    if (prime(n//2)) :
       print("bool_2p 1 ")
       print("bool_2c-imp 0")
    else:
       print("bool_2p 0 ")
       print("bool_2c-imp 1")
  print("n/4 ",n//4," pi(n) ",pi2x," pi(n/2) ",pix)
  if (prime(n-1)): print("n-1 premier ")
```

```
  else: print("n-1 composé ")
  if (prime(n+1)): print("n+1 premier ")
  else: print("n+1 composé ")
  if (prime(n//2)): print("n/2 premier ")
  else: print("n/2 composé ")
  if (prime((n+2)//2)): print("(n+2)/2 premier")
  else: print("(n+2)/2 composé")
  print("d_za ",za-pix, "d_zc ",zc-n//4+pix)
  print("d_ya ",ya-pi2x+pix,"d_yc ",yc-n//4+pi2x-pix)
  print("d_zc-za ",zc-za-n//4+2*pix,"d_za-ya ",za-ya-2*pix+pi2x,"d_yc-zc ",yc-
zc-2*pix+pi2x)
  print("d_zc-ya ",zc-ya-n//4+pi2x,"d_yc-za ",yc-za-n//4+pi2x,"d_xd-xa ",xd-xa-
n//4+pi2x)
################################################################################
# valeurs des variables
################################################################################
#
# xa est le nombre de décompositions de n comme somme de 2 impairs premiers
# p1 et p2
# n=p1+p2 avec 3 <= p1 <= n/2 et n/2 <= p2 <= n-3 (ces bornes des intervalles
# d'appartenance de p1 et p2 sont identiques dans les définitions de xb, xc
# et xd ci-dessous)
# xb est le nombre de décompositions de n comme somme d'un impair premier
# p1 et d'un impair composé p2
# xc est le nombre de décompositions de n comme somme d' un impair composé
# p1 et d'un impair premier p2
# xd est le nombre de décompositions de n comme somme de 2 impairs composés
# p1 et p2
# ya est le nombre de décompositions de n de la forme 3+p avec p premier >= n/2
# yc est le nombre de décompositions de n de la forme 3+c avec c composé >= n/2
# za est le nombre de décompositions de n de la forme 3+p avec p premier < n/2
# zc est le nombre de décompositions de n de la forme 3+c avec p premier < n/2
# bool_4k+2 vaut 1 si n est de la forme 4k+2 et 0 sinon.
# bool_2p vaut 1 si n est le double d'un nombre premier et 0 sinon.
# bool_2c_imp vaut 1 si n est le double d'un nombre impair composé et 0 sinon.
#
################################################################################
# invariants
################################################################################
#
# ya=xa+xb
# yc=xc+xd
# ya+yc=xa+xb+xc+xd=(n-2)//4
# za+zc=(n-4)//4
# xa+xc=za+delta_za+bool_2p
# xb+xd=zc+bool_2c_imp
# zc-ya=xd-xa-bool_2c_imp
# zc-ya=yc-za-bool_4k+2
# za = pi(n/2)+delta_za avec delta_za=-2 si n est le double d'un nombre
# premier et -1 sinon.
# zc=n/4-pi(n/2)+delta_zc avec delta_zc=1 si n est le double d'un nombre
# premier et 0 sinon
# ya=pi(n)-pi(/2)+delta_ya avec delta_ya=-1, 0 ou 1 suivant les caractères
# de primalité de n-1 et n/2
# (se reporter à https://hal.archives-ouvertes.fr/hal-01109052)
# yc=n/4-pi(n)+pi(n/2)+delta_yc avec delta_yc=-1, 0 ou 1
# (se reporter au document référencé ci-dessus)
# (n < 240) ou (ya < za < zc < yc) est toujours vraie
# (n < 244) ou (yc+zc < xd) est toujours vraie
#
################################################################################
```

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

int main (int argc, char* argv[]) {
  int cible, i, n, n1, i1, i2, i3, pastrouve ;
  int t[200] ;
  float fk ;

  for (i = 1 ; i <= 100 ; i++)
    {
      t[i] = i*(i+1) /2 ;
      std::cout << i << " --> " << t[i] << "\n" ;
    }

  for (cible = 3 ; cible <= 100 ; cible = cible+1) {
    fk = (float) cible ;
    n = floor ((sqrt (8.0 * fk + 1.0) - 1.0) / 2.0) ;
    n1 = n * (n + 1.0) / 2.0 ;

    pastrouve = true ;
    i1 = n1 ;
    while ((i1 >= 1) && pastrouve)
      {
      i2 = i1 ;
      while ((i2 >= 1) && pastrouve)
        {
          if (t[i1] == cible) {
            std::cout << "\n" << cible << "=" ;
            std::cout << t[i1] ;
            pastrouve = false ;
          }
          else if (t[i2] + t[i1] == cible) {
            std::cout << "\n" << cible << "=" ;
            std::cout << t[i1] << "+" << t[i2] ;
            pastrouve = false ;
          }
          else if (t[i2] + t[i1] < cible)
            {
            i3 = i2 ;
            while ((i3 >= 1) && pastrouve) {
              if (t[i1] + t[i2] + t[i3] == cible) {
                std::cout << "\n" << cible << "=" ;
                std::cout << t[i1] << "+" << t[i2] << "+" << t[i3] << "\n" ;
                std::cout << i1 << "+" << i2 << "+" << i3 << "\n" ;
                pastrouve = false ;
              }
              i3=i3-1 ;
            }
            }
          i2=i2-1 ;
        }
      i1=i1-1 ;
      }
  }
}
```

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

int main (int argc, char* argv[]) {
  int cible, i, n, n1, i1, i2, i3, i4, pastrouve ;
  int t[200] ;
  float fk ;

  for (i = 1 ; i <= 100 ; i++)
    {
      t[i] = i*i ;
      std::cout << i << " --> " << t[i] << "\n" ;
    }

  for (cible = 3 ; cible <= 100 ; cible = cible+1) {
    pastrouve = true ;
    i1 = cible ;
    while ((i1 >= 1) && pastrouve)
      {
      i2 = i1 ;
      while ((i2 >= 1) && pastrouve)
        {
          i3 = i2 ;
          while ((i3 >= 1) && pastrouve)
            {
            if (t[i1] == cible) {
              std::cout << "\n" << cible << "=" ;
              std::cout << t[i1] ;
              pastrouve = false ;
            }
            else if (t[i2] + t[i1] == cible) {
              std::cout << "\n" << cible << "=" ;
              std::cout << t[i1] << "+" << t[i2] ;
              pastrouve = false ;
            }
            else if (t[i3] + t[i2] + t[i1] == cible) {
              std::cout << "\n" << cible << "=" ;
              std::cout << t[i1] << "+" << t[i2] << "+" << t[i3] ;
              pastrouve = false ;
            }
            else if (t[i3] + t[i2] + t[i1] < cible) {
              i4 = i3 ;
              while ((i4 >= 1) && pastrouve) {
                if (t[i1] + t[i2] + t[i3] + t[i4] == cible) {
                  std::cout << "\n" << cible << "=" ;
                  std::cout << t[i1] << "+" << t[i2] << "+" ;
                  std::cout << t[i3] << "+" << t[i4] ;
                  pastrouve = false ;
                }
                i4=i4-1 ;
              }
            }
            i3=i3-1 ;
            }
          i2=i2-1 ;
        }
      i1=i1-1 ;
      }
  }
}
```

```
from math import *
import numpy as np

t = np.zeros(100, dtype='i')
for i in range(1,100):
    t[i]=i*(i-1)//2
    print(i," --> ",t[i])

for cible in range(3,101):
    n = floor ((sqrt (8.0 * cible + 1.0) - 1.0) / 2.0)
    n1 = n * (n + 1.0) / 2.0

    pastrouve = True
    i1 = n1
    while (i1 >= 1) and pastrouve:
        i2 = i1
        while (i2 >= 1) and pastrouve:
            if t[i1] == cible:
                print(cible,"=",t[i1])
                pastrouve = False
            elif t[i2] + t[i1] == cible:
                print(cible,"=",t[i1],"+",t[i2])
                pastrouve = False
            elif t[i2]+t[i1] < cible:
                i3 = i2
                while ((i3 >= 1) and pastrouve):
                    if t[i1] + t[i2] + t[i3] == cible:
                        print(cible,"=",t[i1],"+",t[i2],"+",t[i3])
                        pastrouve = False
                    i3=i3-1
            i2=i2-1
        i1=i1-1
```

```
from math import *
import numpy as np

t = np.zeros(150, dtype='i')
for i in range(1,150):
    t[i]=i*i
    print(i," --> ",t[i])

for cible in range(3,101):
    pastrouve = True
    i1 = cible
    while (i1 >= 1) and pastrouve:
        i2 = i1
        while (i2 >= 1) and pastrouve:
            i3 = i2
            while ((i3 >= 1) and pastrouve):
                if t[i1] == cible:
                    print(cible,"=",t[i1])
                    pastrouve = False
                elif t[i2] + t[i1] == cible:
                    print(cible,"=",t[i1],"+",t[i2])
                    pastrouve = False
                elif t[i1] + t[i2] + t[i3] == cible:
                    print(cible,"=",t[i1],"+",t[i2],"+",t[i3])
                    pastrouve = False
                elif t[i3]+t[i2]+t[i1] < cible:
                    i4 = i3
                    while (i4 >= 1) and pastrouve:
                        if t[i1] + t[i2] + t[i3] + t[i4] == cible:
                            print(cible,"=",t[i1],"+",t[i2],"+",t[i3],"+",t[i4])
                            pastrouve = False
                        i4=i4-1
                i3=i3-1
            i2=i2-1
        i1=i1-1
```

[18] Euréka ! nombre $= \Delta + \Delta + \Delta$. *10-7-1796, Göttingen.*

Tout nombre est somme de trois nombres triangulaires, c. a. d. de la forme $\frac{x(x+1)}{2}$.

Si :

$$M = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2}, \quad 8M + 3 = (2x+1)^2 + (2y+1)^2 + (2z+1)^2,$$

et réciproquement ; mais tout nombre de la forme $8M + 3$ est décomposable en somme de trois carrés nécessairement impairs (voir note 17).

Cauchy a démontré plus généralement une conjecture de Fermat que tout nombre est la somme de n nombres n-gonaux.

[19] Détermination eulérienne des formes dans lesquelles sont contenus des nombres composés de plus d'un facteur.

Juillet 1796, Göttingen.

Se rapporte aux méthodes d'Euler pour reconnaître si un nombre donné de la forme $4n + 1$ est premier. Les calculs correspondants se trouvent en maints endroits dans *Leiste*.

[20] Principes de la composition des échelles dans les séries récurrentes. *16-7-1796, Göttingen.*

Voir note 10.

[21] Étendu à toutes les courbes la méthode d'Euler pour démontrer la relation entre les segments découpés par deux droites sécantes dans les sections coniques. *31-7-1796, Göttingen.*

Soient OAB, $OA'B'$ deux sécantes menées par O à une conique ; quand O varie, les sécantes se déplaçant parallèlement à elles-mêmes, le rapport $\frac{OA \times OB}{OA' \times OB'}$ est constant. Ce théorème d'Appolonius est démontré à nouveau par Euler, auquel n'échappent pas d'ailleurs les généralisations à des courbes d'ordre supérieur.

Cf. EULER, *Introductio in analysin infinitorum*, Lausanne, 1748, II, pp. 92-93 et 247.

[22] $a^{2^n-1\,(p)} \equiv 1$, toujours résoudre en puissance. *3-8-1796, Göttingen.*

Si p premier est de la forme $2^n \pm 1$, Gauss affirme sans doute qu'il sait décomposer $x^p - 1$ en ses facteurs premiers modulo un nombre premier.

Cf. *Analysis Residuorum*, *Gauss*, II, p. 229, pp. 199-211.

Le cas $p = 31 = 2^5 - 1$ modulo 331 est traité p. 209.

[23] J'ai cherché comment il convenait d'obtenir une raison plus profonde du théorème d'or, et à cet effet je m'apprête à essayer de dépasser les équations quadratiques. Découverte de formules qui peuvent toujours être scindées en considérant les nombres premiers congrus à $\sqrt[\pi]{1}$. *13-8-1796, Göttingen.*

$x^\pi - 1$ pour lesquelles $p^n \equiv 1 \pmod{\pi}$. Le sens de la deuxième phrase se dégage dans : « Disquisitiones generales de congruentis », *Gauss*, II, p. 230.

3=1+1+1
4=4
5=4+1
6=4+1+1
7=4+1+1+1
8=4+4
9=9
10=9+1
11=9+1+1
12=9+1+1+1
13=9+4
14=9+4+1
15=9+4+1+1
16=16
17=16+1
18=16+1+1
19=16+1+1+1
20=16+4
21=16+4+1
22=16+4+1+1
23=9+9+4+1
24=16+4+4
25=25
26=25+1
27=25+1+1
28=25+1+1+1
29=25+4
30=25+4+1
31=25+4+1+1
32=16+16
33=25+4+4
34=25+9
35=25+9+1
36=36
37=36+1
38=36+1+1
39=36+1+1+1
40=36+4
41=36+4+1
42=36+4+1+1
43=25+16+1+1
44=36+4+4
45=36+9
46=36+9+1
47=36+9+1+1
48=36+4+4+4
49=49
50=49+1
51=49+1+1
52=49+1+1+1
53=49+4
54=49+4+1
55=49+4+1+1
56=36+16+4
57=49+4+4
58=49+9
59=49+9+1
60=49+9+1+1
61=49+4+4+4
62=49+9+4
63=49+9+4+1
64=64
65=64+1
66=64+1+1

67=64+1+1+1
68=64+4
69=64+4+1
70=64+4+1+1
71=49+9+9+4
72=64+4+4
73=64+9
74=64+9+1
75=64+9+1+1
76=64+4+4+4
77=64+9+4
78=64+9+4+1
79=49+25+4+1
80=64+16
81=81
82=81+1
83=81+1+1
84=81+1+1+1
85=81+4
86=81+4+1
87=81+4+1+1
88=64+16+4+4
89=81+4+4
90=81+9
91=81+9+1
92=81+9+1+1
93=81+4+4+4
94=81+9+4
95=81+9+4+1
96=64+16+16
97=81+16
98=81+16+1
99=81+16+1+1
100=100

Espace (Denise Vella-Chemla, 17.7.2016)

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 la somme des coefficients diagonaux de la portion finie haute-gauche de la matrice $PlusUn$.

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 $664577 + 8.73825i$.

Etudier des nombres d'écarts (Denise Vella-Chemla, 31.7.2016)

Ici, on fournit simplement des nombres d'écarts entre nombres premiers et certaines constatations les concernant.

Dans le tableau ci-dessous, sont fournis pour n une puissance de 10 :

- en seconde colonne, $\pi(n)$, le nombre de nombres premiers inférieurs ou égaux à n ;
- dans les colonnes $e = k$ le nombre de couples de nombres premiers dont le plus petit des deux est inférieur ou égal à n et dont la différence est k (d'écart k).

n	$\pi(n)$	$e=2$	$e=4$	$e=6$	$e=8$	$e=10$	$e=12$
10^2	25	8	9	16	9	11	15
10^3	168	35	41	74	38	51	70
10^4	1 229	205	203	411	208	270	404
10^5	9 592	1 224	1 216	2 447	1 260	1 624	2 421
10^6	78 498	8 169	8 144	16 386	8 242	10 934	16 378
10^7	664 579	58 980	58 622	117 207	58 595	78 211	117 486
10^8	5 761 455	440 312	440 258	879 908	439 908	586 811	880 196

n	$e=14$	$e=16$	$e=18$	$e=20$	$e=22$	$e=24$	$e=26$	$e=28$	$e=30$
10^2	10	9	14	10	7	15	9	8	18
10^3	48	39	74	48	41	79	42	41	99
10^4	245	200	417	269	226	404	240	248	536
10^5	1 488	1 233	2 477	1 645	1 351	2 475	1 348	1 468	3 329
10^6	9 878	8 210	16 451	10 972	9 171	16 343	8 928	9 784	21 990
10^7	70 463	58 606	117 463	78 218	65 320	117 342	64 203	70 440	156 517
10^8	528 095	441 055	880 444	586 267	489 085	880 927	480 567	528 313	1 173 934

On constate que les écarts multiples de 6, et parmi eux l'écart 30, sont bien plus fréquents que les autres (à cause de la nécessité pour les nombres premiers d'appartenir à telle ou telle classe de congruence selon les modules 2 et 3).

Pour les couples de nombres premiers dont le plus petit est inférieur à 100, on s'est intéressé aux nombres d'occurrence de tel ou tel écart de valeur paire comprise entre 2 et 96.

Mais il y a redondance dans les comptages : si deux écarts de longueur 4 se suivent, on comptera également un écart de longueur 8. On peut représenter les divisibilités entre les écarts, divisibilités qui entraînent des comptages redondant, par des chaînes (ces chaînes sont autant de branches d'un arbre de racine 2, 2 divisant tout nombre pair). On préfère une telle structure d'arbre plutôt que de graphe pour la relation de divisibilité, en "accrochant" un nombre à un père unique qui est son plus grand diviseur strict.

Voici les chaînes de divisibilité :

2 | 4 | 8 | 16 | 32 | 64	2 | 54
2 | 6 | 12 | 24 | 48 | 96	2 | 58
2 | 6 | 18 | 36 | 72	2 | 62
2 | 6 | 42 | 84	2 | 66
2 | 10 | 20 | 40 | 80	2 | 70
2 | 10 | 30 | 60	2 | 74
2 | 10 | 50	2 | 78
2 | 14 | 28 | 56	2 | 82
2 | 22 | 44 | 88	2 | 86
2 | 26 | 52	2 | 94
2 | 34 | 68	
2 | 38 | 76	
2 | 46 | 92	

En s'intéressant à la chaîne de divisibilité 2 | 4 | 8 | 16 | 32 | 64, on a l'idée de comparer la somme des écarts de longueurs 2, 8 et 32 et la somme des écarts de longueur 4, 16 et 64. On constate que les colonnes

$e = 2$, $e = 4$, $e = 8$, $e = 16$, $e = 32$ et $e = 64$ sont sensiblement les mêmes. Ces proximités ont pour conséquence que les sommes de colonnes sont sensiblement égales aussi (les nombres à comparer sont en bleu).

n	$e=2$	$e=8$	$e=32$	$\sum$	n	$e=4$	$e=16$	$e=64$	$\sum$
10^2	9	9	6	24	10^2	9	9	7	25
10^3	36	38	37	111	10^2	41	39	36	116
10^4	206	208	196	610	10^2	203	200	201	604
10^5	1 225	1 260	1 204	3 689	10^2	1 216	1 233	1 255	3 704
10^6	8 170	8 242	8 196	24 608	10^2	8 144	8 210	8 261	24 615
10^7	58 981	58 595	58 565	176 141	10^2	58 622	58 606	58 664	175 892
10^8	440 313	439 908	439 524	1 319 745	10^2	440 258	441 055	440 328	1 321 641

De même, en étudiant la chaîne 2 | 6 | 12 | 24 | 48 | 96, la somme des écarts de longueurs 6 et 24 est proche de la somme des écarts de longueur 12 et 48.

n	$e=6$	$e=24$	$\sum$	n	$e=12$	$e=48$	$\sum$
10^2	16	15	31	10^2	15	13	28
10^3	74	79	153	10^2	70	72	142
10^4	411	404	815	10^2	404	409	813
10^5	2 447	2 475	4 922	10^2	2 421	2 483	4 904
10^6	16 386	16 343	32 729	10^2	16 378	16 501	32 879
10^7	117 207	117 342	234 549	10^2	117 486	117 313	234 799
10^8	879 908	880 927	1 760 835	10^2	880 196	880 138	1 760 334

On constate (un peu paradoxalement) que les colonnes $e = 3k$ sont sensiblement les doubles des colonnes $e = k$ (par exemple, pour $e = 4$ ou bien $e = 8$ ou encore $e = 10$, à mettre en relation avec $e = 12$, $e = 24$ ou encore $e = 30$) mais que cela n'est pas le cas pour les colonnes $e = 6$ et $e = 3 \times 6 = 18$ qui sont sensiblement les mêmes.

Enfin, deux dernières constatations très troublantes :

- observons les colonnes $e = 2$ et $e = 10$ d'une part, $e = 4$ et $e = 20$ d'autre part, et enfin $e = 6$ et $e = 30$. On multiplie l'écart dont on comptabilise les occurrences par 5 dans les 3 cas. Les nombres dans les colonnes quant à eux semblent être multipliés par 4/3, ce rapport semblant s'améliorer au fur et à mesure ;
- de ce fait, on observe alors les colonnes $e = 2$ et $e = 14$ d'une part, et $e = 4$ et $e = 28$ d'autre part, dans le cas où les écarts sont multipliés par 7 et là, surprise, les contenus des colonnes semblent multipliés par 6/5.

Les données concernant les puissances de 2 plutôt que les puissances de 10 semblent confirmer cela : ci-dessous les nombres d'occurences des écarts jusqu'à $2^{20} = 1\,048\,576$.

$\Delta = 2$: 8535	$\Delta = 26$: 9305	$\Delta = 50$: 11463	$\Delta = 74$: 8783	$\Delta = 98$: 10221
$\Delta = 4$: 8500	$\Delta = 28$: 10192	$\Delta = 52$: 9281	$\Delta = 76$: 9043	$\Delta = 100$: 11376
$\Delta = 6$: 17064	$\Delta = 30$: 22887	$\Delta = 54$: 17097	$\Delta = 78$: 18593	
$\Delta = 8$: 8588	$\Delta = 32$: 8543	$\Delta = 56$: 10232	$\Delta = 80$: 11362	
$\Delta = 10$: 11382	$\Delta = 34$: 9111	$\Delta = 58$: 8884	$\Delta = 82$: 8777	
$\Delta = 12$: 17056	$\Delta = 36$: 17115	$\Delta = 60$: 22752	$\Delta = 84$: 20498	
$\Delta = 14$: 10266	$\Delta = 38$: 9074	$\Delta = 62$: 8913	$\Delta = 86$: 8739	
$\Delta = 16$: 8545	$\Delta = 40$: 11416	$\Delta = 64$: 8594	$\Delta = 88$: 9494	
$\Delta = 18$: 17119	$\Delta = 42$: 20642	$\Delta = 66$: 19034	$\Delta = 90$: 22788	
$\Delta = 20$: 11443	$\Delta = 44$: 9575	$\Delta = 68$: 9194	$\Delta = 92$: 9074	
$\Delta = 22$: 9523	$\Delta = 46$: 8945	$\Delta = 70$: 13701	$\Delta = 94$: 8806	
$\Delta = 24$: 17004	$\Delta = 48$: 17170	$\Delta = 72$: 17118	$\Delta = 96$: 17161	

Il semblerait que les écarts apparaissant le moins souvent entre deux nombres premiers soient les puissances de 2, puis les écarts de la forme $2^k.p$ avec p premier, puis les écarts de la forme $2^k.5^{k'}$, puis les écarts de la forme $6k$, les écarts ayant beaucoup de diviseurs semblant bien plus nombreux que les autres.

On a alors l'idée de calculer par programme des nombres d'écarts entre nombres premiers tous les deux inférieurs à n ainsi que les sommes alternées de ces écarts (alors que les nombres fournis dans les tableaux ci-dessus comptent des écarts pour lesquels seul le plus petit des deux nombres premiers est inférieur à n).

On les fournit pour $n = 100$. On constate que les sommes alternées des nombres d'occurrence sont proches (on fait la somme des nombres d'occurrences pour les écarts doubles de pairs d'une part (apparaissant dans les colonnes impaires du tableau) et la somme des nombres d'occurrences pour les écarts doubles d'impairs d'autre part (dans les colonnes paires du tableau)).

écart	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38
nb occur.	8	8	15	9	10	13	9	8	12	8	6	12	8	6	13	5	5	11	6

écart	40	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70	72	74	76
nb occur.	6	9	5	4	7	6	4	7	6	3	7	3	3	6	4	3	3	2	3

écart	78	80	82	84	86	88	90	92	94	96
nb occur.	3	2	1	2	2	0	1	1	1	0

Ci-dessous sont fournies les sommes alternées des nombres d'occurrences pour n une puissance de 10.

n	*écarts* $4k$	*écarts* $4k+2$
10^2	143	133
10^3	6 901	6 960
10^4	376 407	376 971
10^5	22 992 181	22 996 664

Les différences sont trop grandes pour être approfondies.

Enfin, comme on a constaté dans les tableaux précédents que certaines colonnes vérifient "presque" certaines relations de proportionnalité (par exemple, la colonne $e = 6$ est "presque" la somme des colonnes $e = 2$ et $e = 4$[1], on essaie d'obtenir des puissances de matrices 2×2 dont les valeurs approcheraient les valeurs des colonnes mais on n'y parvient pas.

On fournit ci-après les puissances successives de la matrice $D = \begin{pmatrix} 2 & 1 \\ 1 & 1/2 \end{pmatrix}$.

$D^2 = \begin{pmatrix} 5 & 2.5 \\ 2.5 & 1.25 \end{pmatrix}$	$D^9 = \begin{pmatrix} 3051.76 & 1525.88 \\ 1525.88 & 762.939 \end{pmatrix}$
$D^3 = \begin{pmatrix} 12.5 & 6.25 \\ 6.25 & 3.125 \end{pmatrix}$	$D^{10} = \begin{pmatrix} 7629.39 & 3814.7 \\ 3814.7 & 1907.35 \end{pmatrix}$
$D^4 = \begin{pmatrix} 31.25 & 15.625 \\ 15.625 & 7.8125 \end{pmatrix}$	$D^{11} = \begin{pmatrix} 19073.5 & 9536.74 \\ 9536.74 & 4768.37 \end{pmatrix}$
$D^5 = \begin{pmatrix} 78.125 & 39.0625 \\ 39.0625 & 19.5312 \end{pmatrix}$	$D^{12} = \begin{pmatrix} 47683.7 & 23841.9 \\ 23841.9 & 11920.9 \end{pmatrix}$
$D^6 = \begin{pmatrix} 195.312 & 97.6562 \\ 97.6562 & 48.8281 \end{pmatrix}$	$D^{13} = \begin{pmatrix} 119209 & 59604.6 \\ 59604.6 & 29802.3 \end{pmatrix}$
$D^7 = \begin{pmatrix} 488.281 & 244.141 \\ 244.141 & 122.07 \end{pmatrix}$	$D^{14} = \begin{pmatrix} 298023 & 149012 \\ 149012 & 74505.8 \end{pmatrix}$
$D^8 = \begin{pmatrix} 1220.7 & 610.352 \\ 610.352 & 305.176 \end{pmatrix}$	$D^{15} = \begin{pmatrix} 745058 & 372529 \\ 372529 & 186265 \end{pmatrix}$

Le 1220 de D^8 est "presque" $\pi(10^4)$.

[1] Ceci se disant de la façon suivante avec le langage mnémotechnique associé aux nombres premiers "On compte environ autant de premiers jumeaux et cousins mis ensemble que de premiers sexy !".

Voici les puissances successives de la matrices $T = \begin{pmatrix} 3 & 1 \\ 1 & 1/3 \end{pmatrix}$.

$T^2 = \begin{pmatrix} 10 & 3.33333 \\ 3.33333 & 1.11111 \end{pmatrix}$	$T^7 = \begin{pmatrix} 4115.23 & 1371.74 \\ 1371.74 & 457.247 \end{pmatrix}$
$T^3 = \begin{pmatrix} 33.3333 & 11.1111 \\ 11.1111 & 3.7037 \end{pmatrix}$	$T^8 = \begin{pmatrix} 13717.4 & 4572.47 \\ 4572.47 & 1524.16 \end{pmatrix}$
$T^4 = \begin{pmatrix} 111.111 & 37.037 \\ 37.037 & 12.3457 \end{pmatrix}$	$T^9 = \begin{pmatrix} 45724.7 & 15241.6 \\ 15241.6 & 5080.53 \end{pmatrix}$
$T^5 = \begin{pmatrix} 370.37 & 123.457 \\ 123.457 & 41.1523 \end{pmatrix}$	$T^{10} = \begin{pmatrix} 152416 & 50805.3 \\ 50805.3 & 16935.1 \end{pmatrix}$
$T^6 = \begin{pmatrix} 1234.57 & 411.523 \\ 411.523 & 137.174 \end{pmatrix}$	$T^{11} = \begin{pmatrix} 508053 & 169351 \\ 169351 & 56450.3 \end{pmatrix}$

Voici enfin les puissances successives de la matrices $S = \begin{pmatrix} 6 & 1 \\ 1 & 1/6 \end{pmatrix}$.

$S^2 = \begin{pmatrix} 37 & 6.166676.16667 & 1.02778 \end{pmatrix}$	$S^8 = \begin{pmatrix} 2034719.6 & 339119.9 \\ 339119.9 & 56520.0 \end{pmatrix}$
$S^3 = \begin{pmatrix} 228.2 & 38.0 \\ 38.0 & 6.3 \end{pmatrix}$	$S^9 = \begin{pmatrix} 12547437.5 & 2091239.6 \\ 2091239.6 & 348539.9 \end{pmatrix}$
$S^4 = \begin{pmatrix} 1407.0 & 234.5 \\ 234.5 & 39.1 \end{pmatrix}$	$S^{10} = \begin{pmatrix} 77375864.4 & 12895977.4 \\ 12895977.4 & 2149329.6 \end{pmatrix}$
$S^5 = \begin{pmatrix} 8676.7 & 1446.1 \\ 1446.1 & 241.0 \end{pmatrix}$	$S^{11} = \begin{pmatrix} 477151163.6 & 79525193.9 \\ 79525193.9 & 13254199.0 \end{pmatrix}$
$S^6 = \begin{pmatrix} 53506.1 & 8917.7 \\ 8917.7 & 1486.3 \end{pmatrix}$	$S^{12} = \begin{pmatrix} 2942432175.3 & 490405362.5 \\ 490405362.5 & 81734227.1 \end{pmatrix}$
$S^7 = \begin{pmatrix} 329954.5 & 54992.4 \\ 54992.4 & 9165.4 \end{pmatrix}$	$S^{13} = \begin{pmatrix} 18144998414.3 & 3024166402.4 \\ 3024166402.4 & 504027733.7 \end{pmatrix}$

Formule récurrente d'Euler pour le calcul de la somme des diviseurs

Denise Vella-Chemla

4.8.16

1 Etudier la formule de récurrence

Dans l'article *"Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs"*, Euler fournit une formule par récurrence qui calcule la somme des diviseurs d'un nombre.

Dans la mesure où la somme des diviseurs permet totalement de distinguer les nombres premiers des nombres composés puisqu'elle vaut $n+1$ pour un nombre n premier alors qu'elle vaut bien davantage pour un nombre composé, on essaie de trouver une nouvelle façon d'envisager cette fonction. On s'interroge notamment sur la manière dont les transformations du carré pourraient intervenir.

Voici la table de la somme des diviseurs des entiers de 1 à 100, présentée en section 4 de la note d'Euler.

$\sigma(1) = 1$	$\sigma(21) = 32$	$\sigma(41) = 42$	$\sigma(61) = 62$	$\sigma(81) = 121$
$\sigma(2) = 3$	$\sigma(22) = 36$	$\sigma(42) = 96$	$\sigma(62) = 96$	$\sigma(82) = 126$
$\sigma(3) = 4$	$\sigma(23) = 24$	$\sigma(43) = 44$	$\sigma(63) = 104$	$\sigma(83) = 84$
$\sigma(4) = 7$	$\sigma(24) = 60$	$\sigma(44) = 84$	$\sigma(64) = 127$	$\sigma(84) = 224$
$\sigma(5) = 6$	$\sigma(25) = 31$	$\sigma(45) = 78$	$\sigma(65) = 84$	$\sigma(85) = 108$
$\sigma(6) = 12$	$\sigma(26) = 42$	$\sigma(46) = 72$	$\sigma(66) = 144$	$\sigma(86) = 132$
$\sigma(7) = 8$	$\sigma(27) = 40$	$\sigma(47) = 48$	$\sigma(67) = 68$	$\sigma(87) = 120$
$\sigma(8) = 15$	$\sigma(28) = 56$	$\sigma(48) = 124$	$\sigma(68) = 126$	$\sigma(88) = 180$
$\sigma(9) = 13$	$\sigma(29) = 30$	$\sigma(49) = 57$	$\sigma(69) = 96$	$\sigma(89) = 90$
$\sigma(10) = 18$	$\sigma(30) = 72$	$\sigma(50) = 93$	$\sigma(70) = 144$	$\sigma(90) = 234$
$\sigma(11) = 12$	$\sigma(31) = 32$	$\sigma(51) = 72$	$\sigma(71) = 72$	$\sigma(91) = 112$
$\sigma(12) = 28$	$\sigma(32) = 63$	$\sigma(52) = 98$	$\sigma(72) = 195$	$\sigma(92) = 168$
$\sigma(13) = 14$	$\sigma(33) = 48$	$\sigma(53) = 54$	$\sigma(73) = 74$	$\sigma(93) = 128$
$\sigma(14) = 24$	$\sigma(34) = 54$	$\sigma(54) = 120$	$\sigma(74) = 114$	$\sigma(94) = 144$
$\sigma(15) = 24$	$\sigma(35) = 48$	$\sigma(55) = 72$	$\sigma(75) = 124$	$\sigma(95) = 120$
$\sigma(16) = 31$	$\sigma(36) = 91$	$\sigma(56) = 120$	$\sigma(76) = 140$	$\sigma(96) = 252$
$\sigma(17) = 18$	$\sigma(37) = 38$	$\sigma(57) = 80$	$\sigma(77) = 96$	$\sigma(97) = 98$
$\sigma(18) = 39$	$\sigma(38) = 60$	$\sigma(58) = 90$	$\sigma(78) = 168$	$\sigma(98) = 171$
$\sigma(19) = 20$	$\sigma(39) = 56$	$\sigma(59) = 60$	$\sigma(79) = 80$	$\sigma(99) = 156$
$\sigma(20) = 42$	$\sigma(40) = 90$	$\sigma(60) = 168$	$\sigma(80) = 186$	$\sigma(100) = 217$

Et voilà la formule de récurrence qu'Euler a trouvée.

$$\begin{cases} \sigma(n) = \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) + \sigma(n-12) + \sigma(n-15) \\ \qquad -\sigma(n-22) - \sigma(n-26) + \sigma(n-35) + \sigma(n-40 - \sigma(n-51) - \sigma(n-57) \\ \qquad +\sigma(n-70) + \sigma(n-77) - \sigma(n-92) - \sigma(n-100) + etc. \\ \sigma(0) = \sigma(1) = 1 \\ \sigma(n) = 0 \text{ si n} < 0. \end{cases}$$

Plusieurs éléments entrent en ligne de compte :

- les nombres pentagonaux n_k qui sont à soustraire à n pour savoir quels $\sigma(n-n_k)$ utiliser pour appliquer la formule de récurrence.

  Euler fournit l'aide suivante :

  la progression des nombres 1, 2, 5, 7, 12, 15, etc. qu'il faut successivement retrancher du nombre proposé n, deviendra évidente, en prenant leurs différences :

  $$\begin{array}{lccccccccccccccccc} N. & 1, & 2, & 5, & 7, & 12, & 15, & 22, & 26, & 35, & 40, & 51, & 57, & 70, & 77, & 92, & 100, & etc. \\ Diff. & 1, & 3, & 2, & 5, & 3, & 7, & 4, & 9, & 5, & 11, & 6, & 13, & 7, & 15, & 8, & etc. \end{array}$$

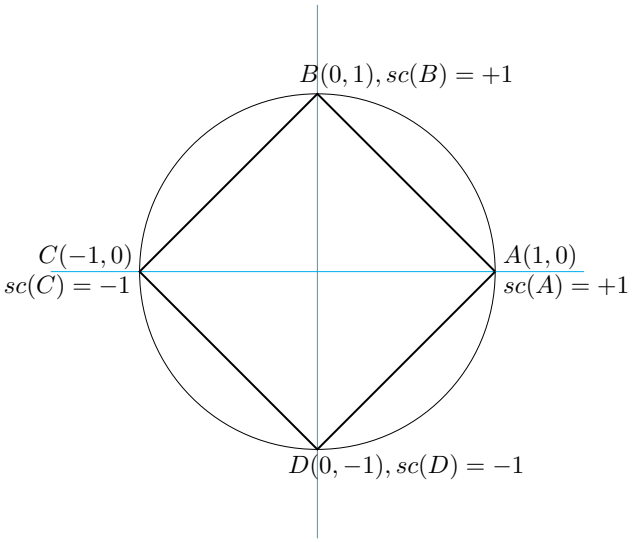
  Car alternativement, on aura tous les nombres naturels 1, 2, 3, 4, 5, 6, etc. *et les nombres impairs* 3, 5, 7, 9, 11, etc., *d'où l'on pourra continuer la suite de ces nombres aussi loin qu'on voudra.*

- le fait d'alterner deux signes "+" et deux signes "−" pour agréger les différents $\sigma(n-n_k)$;
- le fait qu'il faille remplacer $\sigma(0)$ par n et $\sigma(n-n_k)$ par 0 dans le cas où $n-n_k$ est négatif.

Pour le calcul des nombres pentagonaux, on utilise la série définie par :

$$\left\{\begin{array}{lll} s_1 & = 1, & \\ s_n & = s_{n-1} + n/2 & \forall n > 1 \text{ pair} \\ & = s_{n-1} + n & \forall n > 1 \text{ impair} \end{array}\right.$$

Pour alterner deux signes "+" suivis de deux signes "−" cycliquement, on va utiliser une rotation de $\pi/2$ (antihoraire) sur le dessin suivant :



et utiliser la somme des coordonnées qui vaudra alternativement $+1, +1, -1, -1, +1, +1, -1, \ldots$ On nécessite la série de nombres complexes z_n définie par :

$$\left\{\begin{array}{ll} z_1 & = 1, \\ z_n & = iz_{n-1} \end{array}\right.$$

(z_1 correspond au point A et les points sont parcourus cycliquement selon l'ordre $A, B, C, D, A, B, C, D, etc.$).

On a aussi besoin de la fonction somme des coordonnées sc définie sur les complexes par $sc(a+ib) = a+b$.

La récurrence pour la somme des diviseurs s'écrit alors :

$$\left\{\begin{array}{lll} \sigma(n) & = 0 & \forall n < 0 \\ \sigma(0) & = n & \forall n \ (hum\ !), \\ \sigma(1) & = 1, & \\ \sigma(n) & = \sum_{k=1}^{n} sc(z_k)\sigma(n-s_k) & \forall n > 1 \end{array}\right.$$

2 Programmer

Est fourni page suivante le programme proposé.

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

#define M_PI 3.14159265358979323846

typedef std::complex<double> dcomplex ;
const dcomplex di = dcomplex(0.0,1.0) ;

int main (int argc, char* argv[])
{
  int n, tempo, sommedivtempo, k, nmax ;
  int s[350] ;
  int sigma[350] ;
  int sc[350] ;
  dcomplex z[350] ;

  nmax = 320 ;
  s[1] = 1 ;
  for (n = 2 ; n <= nmax ; ++n) {
    if ((n % 2) == 0) s[n] = s[n-1]+n/2 ;
    else s[n] = s[n-1]+n ;
  }
  z[1] = dcomplex(1.0,0.0) ;
  for (n = 2 ; n <= nmax ; ++n) z[n] = di * z[n-1] ;
  for (n = 1 ; n <= nmax ; ++n) sc[n] = real(z[n]) + imag(z[n]) ;
  sigma[1] = 1 ;
  for (n = 2 ; n <= nmax ; ++n) {
    tempo = n ;
    sommedivtempo = 0 ;
    k = 1 ;
    while (tempo-s[k] >= 0) {
      if (tempo-s[k] == 0) sommedivtempo = sommedivtempo + sc[k] * n ;
      else sommedivtempo = sommedivtempo + sc[k] * sigma[tempo - s[k]] ;
      k=k+1 ;
    }
    sigma[n] = sommedivtempo ;
    std::cout << n << " --> " << sigma[n] << "\n" ;
  }
}
```

On a l'intuition de la manière dont peuvent intervenir ces signes qui alternent en se plaçant sur un corps seulement, modulo 5 par exemple. $13\ mod\ 5 = 3$ car 13 est compris entre $10 = 2 \times 5$ et $15 = 3 \times 5$ et $13 - 10 = 3$. Si on prend deux produits kx et $(k+1)x$ avec $k \geqslant 3$ et qu'on leur ôte 13, ces différences seront de même signe (positif). Si on prend deux produits kx et $(k+1)x$ avec $k < 2$ et qu'on leur ôte 13, les différences seront de même signe (négatif). Le seul cas où les différences kx et $(k+1)x$ sont de signe opposé est le cas où $k = 3 = 13\ div\ 5$ (div désignant ici la division entière). Quand on fait le produit de l'infinité des corps premiers $\mathbb{Z}/p\mathbb{Z}$, ces changements de signes interfèrent les uns avec les autres et la récurrence de la somme des diviseurs d'Euler agrège tous ces changements par un simple parcours cyclique de $\mathbb{Z}/4\mathbb{Z}$ et changement de signe une fois sur 2 seulement.

Pour rappel même si cela n'a pas été utilisé ici, $\sigma(n)$ est une fonction multiplicative.

Pour rappel également, l'élévation à la puissance (suite géométrique) ou bien le fait d'additionner toujours une même raison (suite arithmétique) font "cycler" les restes dans un corps premier (la même suite de tous les restes permutés dans un certain ordre revient cycliquement indéfiniment).

On rappelle enfin que $x^{a+ib} = x^a cos(b\ ln\ x) + ix^a sin(b\ ln\ x)$.

Alors la motivation est grande de transformer cette formule de calcul de la somme des diviseurs pour obtenir une formule qui fournirait directement par de simples opérations booléennes le caractère de primalité d'un entier

donné (on imagine que les caractères de primalité à utiliser pourraient être les mêmes que ceux utilisés ici pour calculer la somme des diviseurs).

Il faut revenir sur le nombre de termes qui intervient dans chaque étape de la récursion : on n'est pas satisfait du critère d'arrêt (noté d'un "hum !" ci-dessus) qui fait s'arrêter la formule récurrente quand la fonction σ a comme argument 0 ou bien un nombre entier négatif.

On étudie plus avant le nombre de termes et on obtient que la somme des termes intervenant dans le calcul de $\sigma(n)$ contient :

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

Cela peut être résumé par :

- il y a $\dfrac{p+1}{2}$ nombres entiers successifs dont la somme récurrente contient p termes lorsque p est impair ;
- il y a $p+1$ nombres entiers successifs dont la somme récurrente contient p termes lorsque p est pair.

On voit bien à nouveau les deux termes du produit faire alterner les pairs et les impairs successifs s'agissant du premier, ou bien parcourir la suite simple des entiers successifs en ce qui concerne le deuxième.

Il est étonnant que le nombre de termes de la somme récurrente $\sigma(n)$ à calculer soit fixé étant donné n. Il se calcule ainsi :

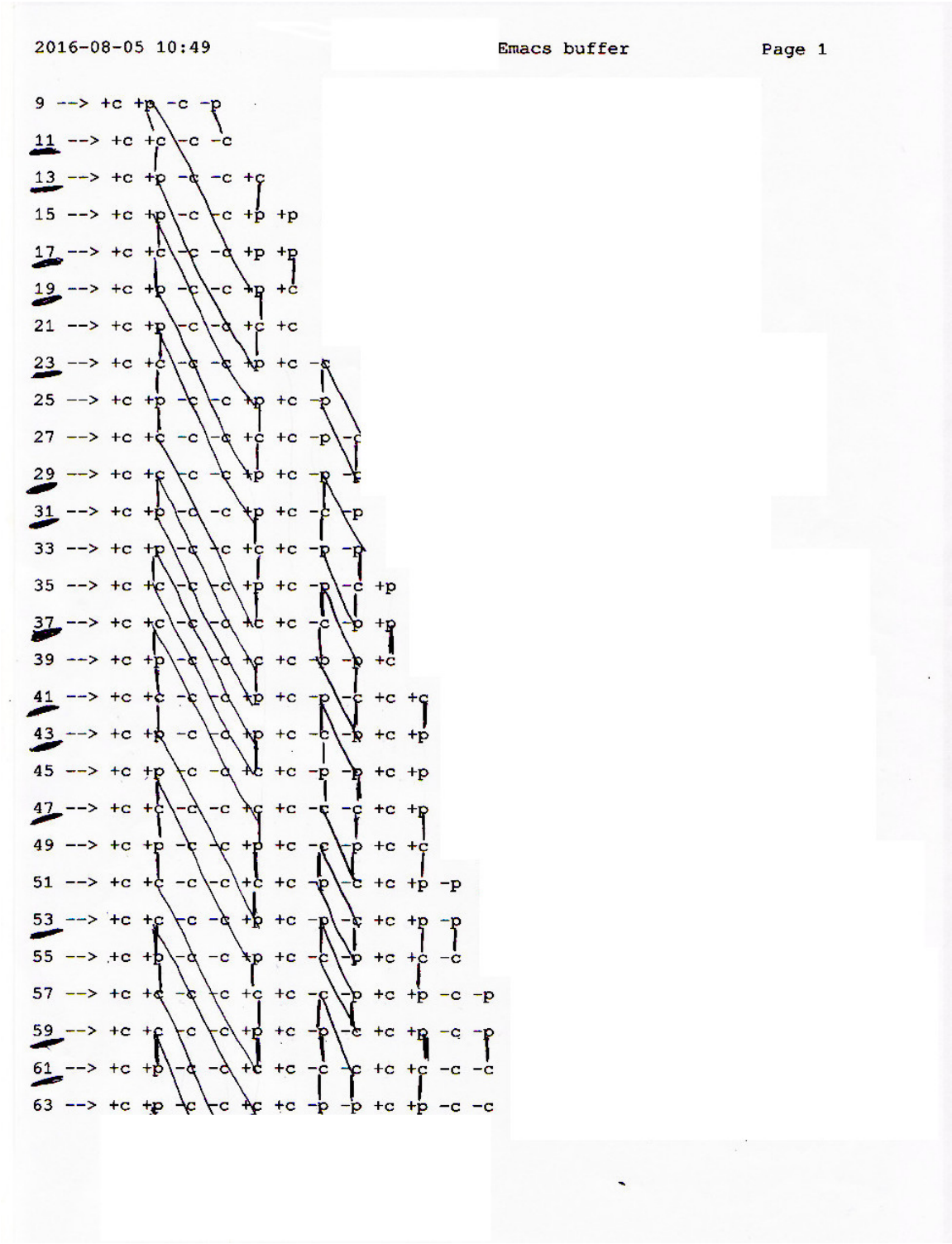
- trouver le plus grand entier inf_1 inférieur à n de la forme $f(x) = \dfrac{3x^2 - x}{2}$ ainsi que le plus petit entier sup_1 de cette forme qui lui soit supérieur ;
- trouver le plus grand entier inf_2 inférieur à n de la forme $g(x) = \dfrac{3x^2 + x}{2}$ ainsi que le plus petit entier sup_2 de cette forme qui lui soit supérieur ;
- si $f(inf_1) \leq n < f(inf_2)$ alors il y aura $2inf_1 - 1$ termes intervenant dans la formule ;
- si $g(inf_2) \leq n < (sup_1)$ alors il y aura $2inf_1$ termes intervenant dans la formule.

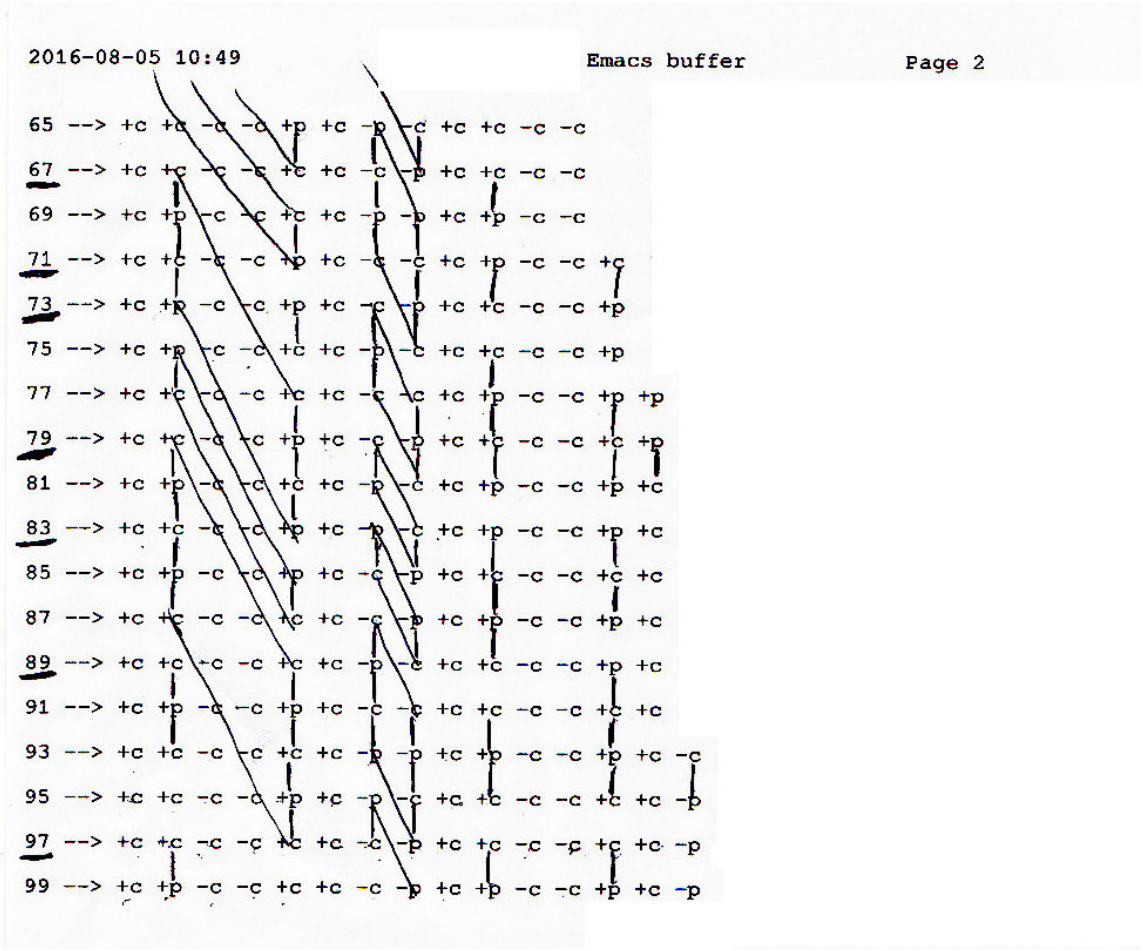
Ainsi, pour 30, compris entre 22 et 35 selon la fonction f et entre 26 et 40 selon la fonction g, étant supérieur à 26, il y aura 8 termes intervenant dans la formule récurrente de calcul de $\sigma(30)$.

3 Détourner le programme à la recherche de relations invariantes

On modifie le programme de manière à ce qu'il écrive p ou c selon que les $\sigma(n-n_i)$ intervenant dans la récurrence sont premiers ou composés. On conserve les signes alternés une fois sur 2 "+,+,-,-,+,+,..." et on effectue des comptages : combien obtient-on de $+c$, de $+p$, de $-c$ et de $-p$? On compte, ce faisant, et comme on l'a déjà fait à une autre occasion, des nombres d'assertions logiques.

On scanne le fichier résultant.



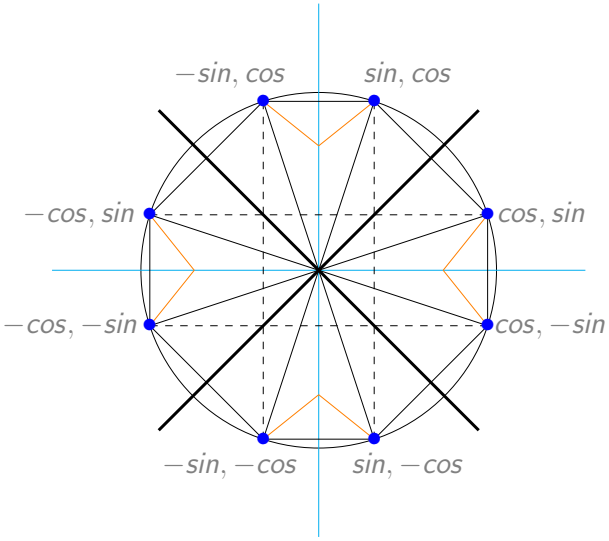


On repère des parallélogrammes contenant les mêmes lettres, dûs au fait que lorsque un $n - n_i$ intervenant dans l'un des calculs est égal au $n' - n'_i$ intervenant dans un autre, le caractère de primalité est le même puisqu'il code l'information concernant un même nombre dans les deux cas. On ne trouve pas de critère général qui permettrait de distinguer les nombres premiers des nombres composés, pourtant les informations fournies ici devraient suffire puisque la somme des diviseurs, calculée selon une récurrence similaire, contient le caractère de primalité d'un nombre quant à elle. Peut-être qu'en ne gardant que le caractère de primalité plutôt que la somme des diviseurs de chaque nombre, on a perdu de l'information.

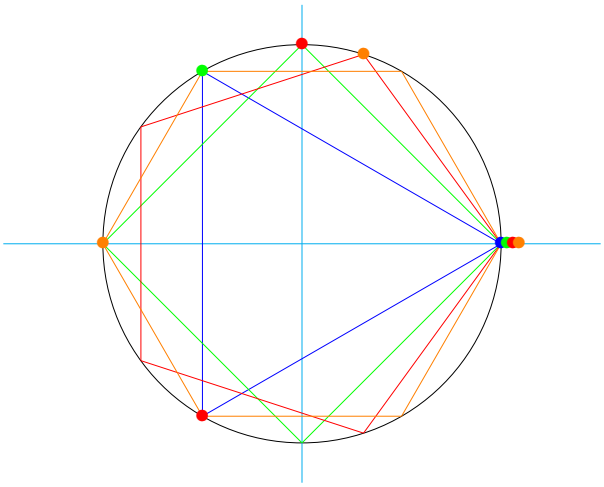
L'opérateur Snur∞

$$PlusUn = \begin{pmatrix} exp\left(\frac{2i\pi}{2}\right) & 0 & 0 & 0 & 0 & \dots \\ 0 & exp\left(\frac{2i\pi}{3}\right) & 0 & 0 & 0 & \dots \\ 0 & 0 & exp\left(\frac{2i\pi}{5}\right) & 0 & 0 & \dots \\ 0 & 0 & 0 & exp\left(\frac{2i\pi}{7}\right) & 0 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix}$$

Malte

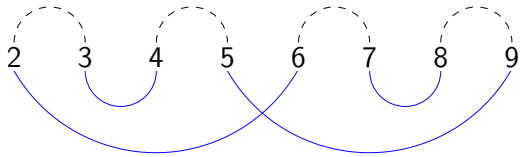


Polygones sur lesquels cyclent les restes modulaires

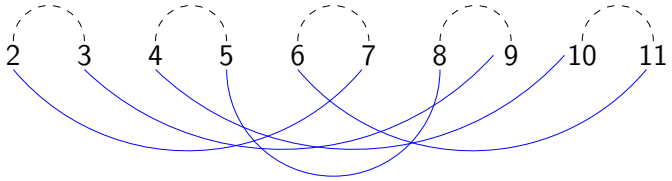


Entrelacs sur les inversibles

Selon le module 11 premier



Selon le module 13 premier



Nombre de résidus quadratiques d'un nombre entier inférieurs à sa moitié

Denise Vella-Chemla

8.8.16

On souhaiterait démontrer qu'on peut établir le caractère de primalité d'un entier n impair en comptant le nombre (qu'on note *prq*) de ses résidus quadratiques (non nuls, on le spécifie une fois pour toutes) qui sont inférieurs ou égaux à $n/2$.

Plus précisément, on induit de comptages effectués pour les nombres impairs jusqu'à 100 l'hypothèse suivante :

(H) Si le nombre prq des résidus quadratiques d'un entier n inférieurs à n/2 est supérieur à n/4, n est premier ; sinon, n est composé.

Cette hypothèse s'écrit :

$$(H)\quad \forall p,\ p \text{ impair et } p \leq 3,$$
$$\rho(p) = \#\left\{ y \text{ tels que } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kp - y = 0 \text{ avec } 0 < y \leq \frac{p-1}{2} \right\} > \frac{n}{4}$$
$$\iff$$
$$p \text{ premier}$$

On teste notre hypothèse en la programmant : on ne peut la tester très loin car l'élévation au carré dépasse vite les limites des entiers (la limite des "unsigned long int" en C++ ne permet de tester l'hypothèse que pour des entiers inférieurs à 300 000 car on utilise un programme simple). On réalise en programmant que les nombres premiers p de la forme $4k+1$ ont leur nombre de "petits résidus quadratiques" qui est égal à $p/4$ tandis que les nombres premiers p de la forme $4k+3$ ont le nombre en question strictement supérieur à $p/4$.

Fournissons quelques éléments qui pourraient être utiles dans une démonstration.

Concernant les produits de nombres de la forme $4k+1$ ou de la forme $4k+3$, le produit de deux $4k+1$ ou le produit de deux $4k+3$ sont des $4k+1$ tandis que le produit d'un $4k+1$ et d'un $4k+3$ est un $4k+3$.

En effet,

$$\begin{array}{lll}
a)\ (4k+1)(4k'+1) & = 16kk' + 4k + 4k' + 1 & = 4(4kk' + k + k') + 1 & = 4k'' + 1 \\
b)\ (4k+3)(4k'+3) & = 16kk' + 12k + 12k' + 9 & = 4(4kk' + 3k + 3k' + 2) + 1 & = 4k'' + 1 \\
c)\ (4k+1)(4k'+3) & = 16kk' + 12k + 4k' + 3 & = 4(4kk' + 3k + k') + 3 & = 4k'' + 3
\end{array}$$

Du fait de ces propriétés de la multiplication des $4k+1$ et $4k+3$, Gauss avait pour habitude de noter les $4k+3$ du signe $-$ et les $4k+1$ du signe $+$.

Pour essayer de démontrer l'hypothèse (H) émise plus haut, on peut avoir à utiliser la loi de réciprocité quadratique qui énonce :

Soient deux nombres x et y.

- *si l'un au moins de ces 2 nombres est un 4k+1, alors x est un résidu quadratique de y si et seulement si y est un résidu quadratique de x ;*
- *si les 2 nombres sont des 4k+3, alors x est un résidu quadratique de y si et seulement si y n'est pas un résidu quadratique de x.*

On va utiliser la notation $x\ R\ m$ pour exprimer que x est un résidu quadratique de m et la notation $x\ \neg R\ m$ pour exprimer que x n'est pas un résidu quadratique de m.

On rappelle la définition de *x est un résidu quadratique de m* (notée $x\ R\ m$) :

$$x\ R\ m \iff \exists y \text{ tel que } x^2 \equiv y\ (mod\ m).$$

Quelques petites règles qui illustrent des utilisations potentielles de la relation *x est un résidu quadratique de m* :

- $x\ R\ m \implies x\ R\ m^n$
- $\forall x,\ x\ R\ 2$
- $\forall k,\ (4k+1)\ R\ 4$
- $\forall k,\ (4k+3)\ \neg\ R\ 4$
- $\forall k,\ (8k+1)\ R\ 2^k$
- $\forall k,\ (8k+3)\ \neg\ R\ 2^k$
- $\forall k,\ (8k+5)\ \neg\ R\ 2^k$
- $\forall k,\ (8k+7)\ \neg\ R\ 2^k$
- $\forall x, y, m,\ x\ R\ m$ *et* $y\ R\ m \implies xy\ R\ m$
- $\forall x, y, m,\ x\ \neg\ R\ m$ *et* $y\ \neg\ R\ m \implies xy\ R\ m$
- $\forall x, y, m,\ x\ R\ m$ *et* $y\ \neg\ R\ m \implies xy\ \neg\ R\ m$

En annexes, sont fournis les résidus quadratiques des nombres entiers impairs de 3 à 51 inférieurs à leur moitié (dits petits résidus quadratiques) ainsi que leur nombre.

Le nombre total de résidus quadratiques de 2 et de ses puissances, ou bien d'un premier p (noté $\rho(p)$) et de ses puissances sont donnés par les formules ci-dessous :

$$\begin{aligned}
\rho(2) &= 2 \\
\rho(2^n) &= \frac{3}{2} + \frac{2^n}{6} + \frac{(-1)^{n+1}}{6} \\
\rho(p) &= \frac{p+1}{2} \\
\rho(p^n) &= \frac{3}{4} + \frac{(p-1)(-1)^{n+1}}{4(p+1)} + \frac{p^{n+1}}{2(p+1)}
\end{aligned}$$

Quelle est notre localisation actuelle ?

On sait que les points de l'espace à 3 dimensions recherchés sont les points à coordonnées entières de surfaces quadriques dégénérées d'équations de la forme $x^2 - pz - y = 0$. On représente ces points par des triplets de la forme (x, z, y). Les seuls points admissibles sont ceux dont la troisième coordonnée y vérifie les inéquations $0 < y \leq p/2$.

On ne croit pas qu'il soit possible de faire un raisonnement par récurrence parce qu'un point solution pour m n'est pas obligatoirement solution pour $m+2$: il est difficile de connaître les points qui restent petits résidus, ou bien ceux qui le deviennent alors qu'ils ne l'étaient pas, ou enfin ceux qui cessent de l'être alors qu'ils l'étaient, lors du passage de m à $m+2$.

Illustrons cela sur un exemple : le triplet $(14, 6, 10)$ est solution pour le module 31 (i.e. 14 est un petit résidu quadratique de 31) car $14^2 - 6.31 - 10 = 0$ et $14 < 31/2$. On sait que si $x^2 - y - pz = 0$ alors $x^2 - (y-2z) - (p+2)z = 0$ et le triplet $(14, 10, 6)$ pour le module 31 pourrait être transformé en le triplet $(14, -14, 10)$ (que l'on réécrit $(14, 19, 10)$ de manière à ne traiter que d'entiers strictement positifs) pour le module 33 mais alors l'inéquations $19 \leq 33/2$ n'est pas vérifiée.

On n'arrive même pas à passer d'un petit résidu quadratique en p et d'un petit résidu quadratique en q à un petit résidu quadratique en pq : de $x^2 - y - pz = 0$ et $x'^2 - y' - qz' = 0$, on tire

$$(xx')^2 - pq(-zz') - (x^2y' + x^2qz' + x'^2y - yy' - qyz' + x'^2pz - y'pz) = 0$$

dont on ne voit pas du tout à quelle condition cela permettrait d'obtenir un petit résidu quadratique de pq.

Ces idées ne semblant pas de bonnes voies, il faudrait peut-être plutôt utiliser les chaînes de causalité entraînées par la loi de réciprocité quadratique. Voyons ces chaînes de causalité à l'oeuvre dans un exemple emprunté à Cyril Banderier : on cherche à savoir si 713 est résidu quadratique (simple, pas "petit") de 1009 (il se trouve que 713 est le carré de 210 modulo 1009) ; on effectue les calculs suivants, qui utilisent le symbole de Legendre $\frac{x}{y}$, qui vaut 1 si x est un résidu quadratique de y (i.e. si $x\ R\ y$) et -1 sinon.

$$\begin{aligned}
\left(\frac{713}{1009}\right) &= \left(\frac{1009}{713}\right)(-1)^{\frac{1008\times 712}{4}} \\
&= \left(\frac{296}{713}\right)(+1) \\
&= \left(\frac{8\times 37}{713}\right) \\
&= \left(\frac{8}{713}\right)\left(\frac{37}{713}\right) \\
&= \left(\frac{2}{713}\right)\left(\frac{37}{713}\right) \\
&= (+1)\left(\frac{37}{713}\right) \\
&= \left(\frac{713-740}{37}\right) \\
&= \left(\frac{-27}{37}\right) \\
&= \left(\frac{10}{37}\right) \\
&= \left(\frac{2}{37}\right)\left(\frac{5}{37}\right) \\
&= (-1)\left(\frac{2}{5}\right)(-1)^{\frac{4\times 36}{4}} \\
&= (-1)(-1)(+1) \\
&= 1
\end{aligned}$$

Les opérations autorisées pour passer d'une relation $\left(\frac{a}{b}\right)$ à la relation $\left(\frac{a'}{b'}\right)$ suivante sont :

- appliquer la loi de réciprocité quadratique : intervertir a et b et multiplier le nouveau caractère de résiduosité par $(-1)^{\frac{(a-1)(b-1)}{4}}$;
- traiter comme il se doit le nombre particulier 2 ;
- remplacer un $a = p^m$ (resp. un $b = p^m$) par $a = p$ (resp. $b = p$) ;
- remplacer a ou b par leurs facteurs indépendants et réappliquer la procédure récursivement sur chaque facteur ;
- remplacer a ou b par $a - b$, $a + b$ ou $a \,\%\, b$ (i.e. $a \mod b$).

Annexe 1 : petits résidus quadratiques des nombres impairs de 3 à 51

Entre parenthèses est fournie la plus petite racine carrée d'un résidu quadratique du module considéré.

$3 \to 1$.

$5 \to 1$.

$7 \to 1$, 2 (3).

$9 \to 1$, 4 (2).

$11 \to 1$, 3 (5), 4 (2), 5 (4).

$13 \to 1$, 3 (4), 4 (2).

$15 \to 1$, 4 (2), 6 (6).

$17 \to 1$, 2 (6), 4 (2), 8 (5).

$19 \to 1$, 4 (2), 5 (9), 6 (5), 7 (8), 9 (3).

$21 \to 1$, 4 (2), 7 (7), 9 (3).

$23 \to 1$, 2 (5), 3 (7), 4 (2), 6 (11), 8 (10), 9 (3).

$25 \to 1$, 4 (2), 6 (9), 9 (3).

$27 \to 1$, 4 (2), 7 (13), 9 (3), 10 (8), 13 (11).

$29 \to 1$, 4 (2), 5 (11), 6 (8), 7 (6), 9 (3), 13 (10).

$31 \to 1$, 2 (8), 4 (2), 5 (6), 7 (10), 8 (15), 9 (3), 10 (14), 14 (13).

$33 \to 1$, 3 (6), 4 (13), 9 (3), 12 (12), 15 (9), 16 (4).

$35 \to 1$, 4 (2), 9 (3), 11 (9), 14 (7), 15 (15), 16 (4).

$37 \to 1$, 3 (15), 4 (2), 7 (9), 9 (3), 10 (11), 11 (14), 12 (7), 16 (4).

$39 \to 1$, 3 (9), 4 (2), 9 (3), 10 (7), 12 (18), 13 (13), 16 (4).

$41 \to 1$, 2 (17), 4 (2), 5 (13), 8 (7), 9 (3), 10 (16), 16 (4), 18 (10), 20 (15).

$43 \to 1$, 4 (2), 6 (7), 9 (3), 10 (15), 11 (21), 13 (20), 14 (10), 15 (12), 16 (4), 17 (19), 21 (8).

$45 \to 1$, 4 (2), 9 (3), 10 (10), 16 (4), 19 (8).

$47 \to 1$, 2 (7), 3 (12), 4 (2), 6 (10), 7 (17), 8 (14), 9 (3), 12 (23), 14 (22), 16 (4), 17 (8), 18 (21), 21 (16).

$49 \to 1$, 2 (10), 4 (2), 8 (20), 9 (3), 11 (16), 15 (8), 16 (4), 18 (19), 22 (13), 23 (11).

$51 \to 1$, 4 (2), 9 (3), 13 (8), 15 (24), 16 (4), 18 (18), 19 (11), 21 (15), 25 (5).

Annexe 2 : Nombre de résidus quadratiques des nombres impairs de 3 à 51 inférieurs à leur moitié

$3 \to 1$

$5 \to 1$

$7 \to 2$

$9 \to 2$

$11 \to 4$

$13 \to 3$

$15 \to 3$

$17 \to 4$

$19 \to 6$

$21 \to 4$

$23 \to 7$

$25 \to 5$

$27 \to 6$

$29 \to 7$

$31 \to 9$

$33 \to 7$

$35 \to 7$

$37 \to 9$

$39 \to 8$

$41 \to 10$

$43 \to 12$

$45 \to 6$

$47 \to 14$

$49 \to 9$

$51 \to 9$

Plus de la moitié ?

Denise Vella-Chemla

16.8.16

On souhaiterait ici montrer une manière enfantine de présenter le lemme de Gauss associé à la loi de réciprocité quadratique. Ce travail peut présenter un intérêt dans la mesure où le comptage des "petits" résidus quadratiques d'un nombre permet de savoir s'il est premier ou composé.

L'énoncé du lemme de Gauss est :

Soit p un nombre premier et a un entier non divisible par p. On considère les entiers

$$a, 2a, 3a, \ldots, \frac{p-1}{2}a$$

et leur plus petit résidu positif modulo p. Parmi ces $(p-1)/2$ entiers distincts compris entre 1 et $p-1$, soit n le nombre de ceux qui sont plus grands que $p/2$. Alors,

$$\left(\frac{a}{p}\right) = (-1)^n$$

où $\left(\frac{a}{p}\right)$ est le symbole de Legendre.

Pour visualiser ce lemme, utilisons des tables de multiplication modulaire et comptons les éléments "supérieurs à la moitié" (à la manière de Gauss, on utilise la lettre R pour noter $x\ R\ y$ le fait que x est un résidu quadratique de y et la lettre N pour noter $x\ N\ y$ le fait que x n'est pas un résidu quadratique de y).

Modulo 7 : (comptage en couleur cyan des nombres supérieurs à $(7-1)/2\ =\ 3$)

	1	2	3	
1	1	2	3	0 est pair $\rightarrow$ 1 R 7
2	2	4	6	2 est pair $\rightarrow$ 2 R 7
3	3	6	2	1 est impair $\rightarrow$ 3 N 7

Modulo 11 : (comptage en couleur cyan des nombres supérieurs à $(11-1)/2\ =\ 5$)

	1	2	3	4	5	
1	1	2	3	4	5	0 est pair $\rightarrow$ 1 R 11
2	2	4	6	8	10	3 est impair $\rightarrow$ 2 N 11
3	3	6	9	1	4	2 est pair $\rightarrow$ 3 R 11
4	4	8	1	5	9	2 est pair $\rightarrow$ 4 R 11
5	5	10	4	9	3	2 est pair $\rightarrow$ 5 R 11

Modulo 19 : (comptage en couleur cyan des nombres supérieurs à $(19-1)/2 = 9$)

	1	2	3	4	5	6	7	8	9	
1	1	2	3	4	5	6	7	8	9	0 est pair → 1 R 19
2	2	4	6	8	10	12	14	16	18	5 est impair → 2 N 19
3	3	6	9	12	15	18	2	5	8	3 est impair → 3 N 19
4	4	8	12	16	1	5	9	13	17	4 est pair → 4 R 19
5	5	10	15	1	6	11	16	2	7	4 est pair → 5 R 19
6	6	12	18	5	11	17	4	10	16	6 est pair → 6 R 19
7	7	14	2	9	16	4	11	18	6	4 est pair → 7 R 19
8	8	16	5	13	2	10	18	7	15	5 est impair → 8 N 19
9	9	18	8	17	7	16	6	15	5	4 est pair → 9 R 19

Modulo 23 : (comptage en couleur cyan des nombres supérieurs à $(23-1)/2 = 11$)

	1	2	3	4	5	6	7	8	9	10	11	
1	1	2	3	4	5	6	7	8	9	10	11	0 est pair → 1 R 23
2	2	4	6	8	10	12	14	16	18	20	22	6 est pair → 2 R 23
3	3	6	9	12	15	18	21	1	4	7	10	4 est pair → 3 R 23
4	4	8	12	16	20	1	5	9	13	17	21	6 est pair → 4 R 23
5	5	10	15	20	2	7	12	17	22	4	9	5 est impair → 5 N 23
6	6	12	18	1	7	13	19	2	8	14	20	6 est pair → 6 R 23
7	7	14	21	5	12	19	3	10	17	1	8	5 est impair → 7 N 23
8	8	16	1	9	17	2	10	18	3	11	19	4 est pair → 8 R 23
9	9	18	4	13	22	8	17	3	13	21	7	6 est pair → 9 R 23
10	10	20	7	17	4	14	1	11	21	8	18	5 est impair → 10 N 23
11	11	22	10	21	9	20	8	19	7	18	6	5 est impair → 11 N 23

La parité du nombre d'éléments "supérieurs à la moitié" par ligne exprime le caractère de résiduosité quadratique du nombre indice de la ligne au module considéré. On a indiqué ce caractère en regard des lignes, à droite. On appellera *lignes paires* les lignes dont le nombre d'éléments supérieurs à la moitié du module considéré est pair et *lignes impaires* les autres.

Voyons sur le module 15 que le comptage ne permet pas de déduire le caractère de résiduosité quadratique à un module composé :

Modulo 15 : (comptage en couleur cyan des nombres supérieurs à $(15-1)/2 = 7$)

	1	2	3	4	5	6	7	
1	1	2	3	4	5	6	7	0 est pair → 1 R 15
2	2	4	6	8	10	12	14	4 est pair or 2 N 15
3	3	6	9	12	0	3	6	2 est pair or 3 N 15
4	4	8	12	1	5	9	13	4 est pair → 4 R 15
5	5	10	0	5	10	0	5	2 est pair or 5 N 15
6	6	12	3	9	0	6	12	3 est impair or 6 R 15
7	7	14	6	13	5	12	4	3 est impair → 7 N 15

Outre le fait que 3 et 15, par comptage, seraient considérés comme résidus quadratiques de 15 alors qu'ils le divisent, on voit que 2 a un nombre pair d'éléments supérieurs à 7 dans sa ligne alors qu'il n'est pas résidu quadratique de 15 ou bien on voit que 6 a un nombre impair d'éléments supérieurs à 7 dans sa ligne alors qu'il est quant à lui effectivement résidu quadratique de 15 (il est son propre carré modulo 15 car $6 \times 6 = 36 \equiv 6 \ (mod\ 15)$).

Ce qu'il faudrait comprendre et démontrer, c'est pourquoi le nombre de lignes "paires" (correspondant au nombre de résidus quadratiques *inférieurs ou égaux*[1] à $n/2$) est toujours supérieur à $n/4$ pour les nombres premiers de la forme $4k+3$.

Il faudrait également démontrer une hypothèse qu'on a émise et vérifiée jusqu'à 3.10^5. Le nombre de résidus quadratiques de n inférieurs ou égaux à $n/2$ est toujours inférieur à $n/4$ pour les nombres composés. Cette hypothèse peut présenter un intérêt par sa simplicité : elle correspond au fait de compter le nombre de points à coordonnées entières et dont la seconde coordonnée est inférieure ou égale à une certaine valeur $(n/2)$, ces points appartenant à une surface définie par une équation quadratique de la forme $x^2-y-nz=0$.

1. Attention à l'inversion ici, il s'agit effectivement de compter les *petits* résidus quadratiques, i.e. ceux qui sont *inférieurs ou égaux* à la moitié du module.

De visu (Denise Vella-Chemla, 17.8.16)

On cherche une règle de récurrence, qui régirait les nombres de petits résidus quadratiques, dans la mesure où ces nombres permettent de distinguer les nombres premiers des nombres composés.

Pour cela, on observe la manière dont évolue la coloration de certaines cases des tables de multiplication modulaire des nombres de 7 à 23.

Les zones colorées s'étendent comme des sortes de vagues, de formes de plus en plus logarithmiques (?) au fur et à mesure qu'elles grossissent.

Modulo 7 : (comptage en couleur cyan des nombres supérieurs à $7/2 = 3$)

	1	2	3	
1	1	2	3	0
2	2	4	6	2
3	3	6	2	1

Modulo 8 : (comptage en couleur cyan des nombres supérieurs à $8/2 = 4$)

	1	2	3	4	
1	1	2	3	4	0
2	2	4	6	0	1
3	3	6	1	4	1
4	4	0	4	0	0

Modulo 9 : (comptage en couleur cyan des nombres supérieurs à $9/2 = 4$)

	1	2	3	4	
1	1	2	3	4	0
2	2	4	6	8	2
3	3	6	0	3	1
4	4	8	3	7	2

Modulo 10 : (comptage en couleur cyan des nombres supérieurs à $10/2 = 5$)

	1	2	3	4	5	
1	1	2	3	4	5	0
2	2	4	6	8	0	2
3	3	6	9	2	5	2
4	4	8	2	6	0	2
5	5	0	5	0	5	0

Modulo 11 : (comptage en couleur cyan des nombres supérieurs à $11/2 = 5$)

	1	2	3	4	5	
1	1	2	3	4	5	0
2	2	4	6	8	10	3
3	3	6	9	1	4	2
4	4	8	1	5	9	2
5	5	10	4	9	3	2

Modulo 12 : (comptage en couleur cyan des nombres supérieurs à $12/2 = 6$)

	1	2	3	4	5	6	
1	1	2	3	4	5	6	0
2	2	4	6	8	10	0	2
3	3	6	9	0	3	6	1
4	4	8	0	4	8	0	2
5	5	10	3	8	1	6	2
6	6	0	6	0	6	0	0

Modulo 13 : (comptage en couleur cyan des nombres supérieurs à 13/2 = 6)

	1	2	3	4	5	6	
1	1	2	3	4	5	6	0
2	2	4	6	8	10	12	3
3	3	6	9	12	2	5	2
4	4	8	12	3	7	11	4
5	5	10	2	7	12	4	3
6	6	12	5	11	4	11	3

Modulo 14 : (comptage en couleur cyan des nombres supérieurs à 14/2 = 7)

	1	2	3	4	5	6	7	
1	1	2	3	4	5	6	7	0
2	2	4	6	8	10	12	0	3
3	3	6	9	12	1	4	0	2
4	4	8	12	2	6	10	0	3
5	5	10	1	6	11	2	7	2
6	6	12	4	10	2	8	0	3
7	7	0	7	0	7	0	7	0

Modulo 15 : (comptage en couleur cyan des nombres supérieurs à 15/2 = 7)

	1	2	3	4	5	6	7	
1	1	2	3	4	5	6	7	0
2	2	4	6	8	10	12	14	4
3	3	6	9	12	0	3	6	2
4	4	8	12	1	5	9	13	4
5	5	10	0	5	10	0	5	2
6	6	12	3	9	0	6	12	3
7	7	14	6	13	5	12	4	3

Modulo 16 : (comptage en couleur cyan des nombres supérieurs à 16/2 = 8)

	1	2	3	4	5	6	7	8	
1	1	2	3	4	5	6	7	8	0
2	2	4	6	8	10	12	14	0	3
3	3	6	9	12	15	2	5	8	2
4	4	8	12	0	4	8	12	0	2
5	5	10	15	4	9	14	3	8	2
6	6	12	2	8	14	4	10	0	3
7	7	14	5	12	3	10	1	8	3
8	8	0	8	0	8	0	8	0	0

Modulo 17 : (comptage en couleur cyan des nombres supérieurs à 17/2 = 8)

	1	2	3	4	5	6	7	8	
1	1	2	3	4	5	6	7	8	0
2	2	4	6	8	10	12	14	16	4
3	3	6	9	12	15	1	4	7	2
4	4	8	12	16	3	7	11	15	4
5	5	10	15	3	8	13	1	6	3
6	6	12	1	7	13	2	8	14	3
7	7	14	4	1	1	8	15	5	3
8	8	16	7	15	6	14	5	13	4

Modulo 18 : (comptage en couleur cyan des nombres supérieurs à $18/2 = 9$)

	1	2	3	4	5	6	7	8	9	
1	1	2	3	4	5	6	7	8	9	0
2	2	4	6	8	10	12	14	16	0	4
3	3	6	9	12	15	0	3	6	9	2
4	4	8	12	16	2	6	10	14	0	4
5	5	10	15	2	7	12	17	4	9	4
6	6	12	0	6	12	0	6	12	0	3
7	7	14	3	10	17	6	13	2	9	4
8	8	16	6	14	4	12	2	10	0	4
9	9	0	9	0	9	0	9	0	9	0

Modulo 19 : (comptage en couleur cyan des nombres supérieurs à $19/2 = 9$)

	1	2	3	4	5	6	7	8	9	
1	1	2	3	4	5	6	7	8	9	0
2	2	4	6	8	10	12	14	16	18	5
3	3	6	9	12	15	18	2	5	8	3
4	4	8	12	16	1	5	9	13	17	4
5	5	10	15	1	6	11	16	2	7	4
6	6	12	18	5	11	17	4	10	16	5
7	7	14	2	9	16	4	11	18	6	4
8	8	16	5	13	2	10	18	7	15	5
9	9	18	8	17	7	16	6	15	5	4

Modulo 20 : (comptage en couleur cyan des nombres supérieurs à $20/2 = 10$)

	1	2	3	4	5	6	7	8	9	10	
1	1	2	3	4	5	6	7	8	9	10	0
2	2	4	6	8	10	12	14	16	18	0	4
3	3	6	9	12	15	18	1	4	7	10	3
4	4	8	12	16	0	4	8	12	16	0	4
5	5	10	15	0	5	10	15	0	5	10	2
6	6	12	18	4	10	16	2	8	14	0	4
7	7	14	1	8	15	2	9	16	3	10	3
8	8	16	4	12	0	8	16	4	12	0	4
9	9	18	7	16	5	14	3	12	1	10	4
10	10	0	10	0	10	0	10	0	10	0	0

Modulo 21 : (comptage en couleur cyan des nombres supérieurs à $21/2 = 10$)

	1	2	3	4	5	6	7	8	9	10	
1	1	2	3	4	5	6	7	8	9	10	0
2	2	4	6	8	10	12	14	16	18	18	5
3	3	6	9	12	15	18	0	3	6	9	3
4	4	8	12	16	20	3	7	11	15	19	6
5	5	10	15	20	4	9	14	19	3	8	4
6	6	12	18	3	9	15	0	6	12	18	5
7	7	14	0	7	14	0	7	14	0	7	3
8	8	16	3	11	19	6	14	1	9	17	5
9	9	18	6	15	3	12	0	9	18	6	4
10	10	20	9	19	8	18	7	17	6	16	5

Modulo 22 : (comptage en couleur cyan des nombres supérieurs à $22/2 = 11$)

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

Modulo 23 : (comptage en couleur cyan des nombres supérieurs à $23/2 = 11$)

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

Pour les nombres impairs, les séquences de nombres de petits résidus quadratiques sont successivement :

7 :	0	2	1							
9 :	0	2	1	2						
11 :	0	3	2	2	2					
13 :	0	3	2	4	3	3				
15 :	0	4	2	4	2	3	3			
17 :	0	4	2	4	3	3	3	4		
19 :	0	5	3	4	4	5	4	5	4	
21 :	0	5	3	6	4	5	3	5	4	5
23 :	0	6	4	6	5	6	5	4	6	5	5

Pour les pairs, ont été obtenues les séquences suivantes :

8 :	0	1	1	0						
10 :	0	2	2	2	0					
12 :	0	2	1	2	2	0				
14 :	0	3	2	3	2	3	0			
16 :	0	3	2	2	2	3	3	0		
18 :	0	4	2	4	4	3	4	4	0	
20 :	0	4	3	4	2	4	3	4	4	0
22 :	0	5	4	5	4	5	5	4	4	5	0

Peut-être faut-il étudier toutes les séquences à la fois, même si aucun pair sauf 2 n'est premier.

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

Tables de résidus quadratiques des modules 3 à 51 (Denise Vella-Chemla, 16.8.16)

Voici les tables qui permettent d'induire, de visu, mais cela ne reste qu'une hypothèse :

- que les nombres premiers de la forme $4k+3$ ont strictement plus de $n/4$ résidus quadratiques inférieurs ou égaux à leur moitié ;
- que les nombres premiers de la forme $4k+1$ ont $(n-1)/4$ résidus quadratiques inférieurs ou égaux à leur moitié ;
- que les nombres composés ont moins de $n/4$ résidus quadratiques inférieurs ou égaux à leur moitié.

On commence par calculer les carrés modulo le nombre n considéré et les noter dans la troisième ligne, sous la barre. Puis on colorie leur occurrence dans les deux premières lignes. Enfin, on compte les petits résidus quadratiques (notés *prq*, i.e. ceux qui sont inférieurs à $n/2$, et qui apparaissent dans la seconde ligne).

Module $n = 3$ (1 prq $> 3/4$)

2
1
1

Module $n = 5$ (1 prq)

4	3
1	2
1	4

Module $n = 7$ (2 prq $> 7/4$)

6	5	4
1	2	3
1	4	2

Module $n = 9$ (2 prq $< 9/4$)

8	7	6	5
1	2	3	4
1	4	0	7

Module $n = 11$ (4 prq $> 11/4$)

10	9	8	7	6
1	2	3	4	5
1	4	9	5	3

Module $n = 13$ (3 prq $= 13/4$)

12	11	10	9	8	7
1	2	3	4	5	6
1	4	9	3	12	10

Module $n = 15$ (3 prq $< 15/4$)

14	13	12	11	10	9	8
1	2	3	4	5	6	7
14	9	1	10	6	4	

Module $n = 17$ (4 prq = 17/4)

16	15	14	13	12	11	10	9
1	2	3	4	5	6	7	8
1	4	9	16	8	2	15	13

Module $n = 19$ (6 prq > 19/4)

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

Module $n = 21$ (4 prq < 21/4)

20	19	18	17	16	15	14	13	12	11
1	2	3	4	5	6	7	8	9	10
1	4	9	16	4	15	7	1	18	16

Module $n = 23$ (7 prq > 23/4)

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

Module $n = 25$ (5 prq < 25/4)

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

Module $n = 27$ (6 prq < 27/4)

26	25	24	23	22	21	20	19	18	17	16	15	14
1	2	3	4	5	6	7	8	9	10	11	12	13
1	4	9	16	25	9	22	10	0	19	13	9	7

Module $n = 29$ (7 prq > 29/4)

28	27	26	25	24	23	22	21	20	19	18	17	16	15
1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	4	9	16	25	7	20	6	23	13	5	28	24	22

Module $n = 31$ (9 prq > 31/4)

30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	4	9	16	25	5	18	2	19	7	28	20	14	10	8

Module $n = 33$ (7 prq < 33/4)

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	4	9	16	25	3	16	31	15	1	22	12	4	31	27	25

Module $n = 35$ (7 prq < 35/4)

34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9

Module $n = 37$ (9 prq $> 37/4$)

36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	4	9	16	25	36	12	27	7	26	10	33	21	11	3	34	30	28

Module $n = 39$ (8 prq $< 39/4$)

38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
1	4	9	16	25	36	10	25	3	22	4	27	13	1	30	22	16	12	10

Module $n = 41$ (10 prq $> 41/4$)

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	4	9	16	25	36	8	23	40	18	39	21	5	32	20	10	2	37	33	31

Module $n = 43$ (12 prq $> 43/4$)

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

Module $n = 45$ (6 prq $< 45/4$)

44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	4	9	16	25	36	4	19	36	10	31	9	34	16	0	31	19	9	1	40	36	34

Module $n = 47$ (14 prq $> 47/4$)

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

Module $n = 49$ (11 prq $< 49/4$)

48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	4	9	16	25	36	0	15	32	2	23	46	22	0	29	11	44	30	18	8	0	43	39	37

Module $n = 51$ (10 prq $< 51/4$)

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

On remarque enfin un élément qu'il est peut-être intéressant de souligner : selon le module $p = 23$ par exemple, les carrés s'obtenant par additions d'impairs successifs à partir de 0, on a la succession de restes modulaires suivante :

$$0 \xrightarrow{+1} 1 \xrightarrow{+3} 4 \xrightarrow{+5} 9 \xrightarrow{+7} 16 \xrightarrow{+9} 2$$

$$\xrightarrow{+11} 13 \xrightarrow{+13} 3 \xrightarrow{+15} 18 \xrightarrow{+17} 12 \xrightarrow{+19} 8 \xrightarrow{+21} 6$$

dans laquelle on compte 7 restes quadratiques inférieurs ou égaux à $11 = \dfrac{23-1}{2}$.

On obtient le même nombre de restes inférieurs ou égaux à $\frac{p-1}{2}$ dans la suite précédente que dans la suite obtenue en ajoutant des *pairs* successifs plutôt que des *impairs*, dans une suite commençant à $6 = \frac{p+1}{4}$.

$$6 \xrightarrow{+\,2} 8 \xrightarrow{+\,4} 12 \xrightarrow{+\,6} 18 \xrightarrow{+\,8} 3 \xrightarrow{+\,10} 13$$

$$\xrightarrow{+\,12} 2 \xrightarrow{+\,14} 16 \xrightarrow{+\,16} 9 \xrightarrow{+\,18} 4 \xrightarrow{+\,20} 1 \xrightarrow{+\,22} 0$$

Nombre de résidus quadratiques d'un nombre entier inférieurs à sa moitié

Denise Vella-Chemla

26.8.2016

On souhaiterait démontrer qu'on peut établir le caractère de primalité d'un entier n impair en comptant le nombre (qu'on note $R_b(n)$) de ses résidus quadratiques (non nuls, on le spécifie une fois pour toutes) qui sont inférieurs ou égaux à $n/2$.

Plus précisément, on induit de comptages effectués pour les nombres impairs jusqu'à 100 l'hypothèse suivante :

(H) Si le nombre $R_b(n)$ des résidus quadratiques d'un entier n inférieurs à $n/2$ est supérieur à $n/4$, n est premier ; sinon, n est composé.

Cette hypothèse s'écrit :

$$(H)\quad \forall n,\ n \text{ impair et } n \geq 3,$$
$$R_b(n) = \#\left\{ y \text{ tels que } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kn - y = 0 \text{ avec } 0 < y \leq \frac{n-1}{2} \right\} > \frac{n}{4}$$
$$\iff$$
$$n \text{ premier}$$

On teste notre hypothèse en la programmant : on ne peut la tester très loin car l'élévation au carré dépasse vite les limites des entiers (la limite des "unsigned long int" en C++ ne permet de tester l'hypothèse que pour des entiers inférieurs à 300 000 car on utilise un programme simple). On réalise en programmant que les nombres premiers p de la forme $4k+1$ ont leur nombre de "petits résidus quadratiques" qui est égal à $\lfloor p/4 \rfloor$ tandis que les nombres premiers p de la forme $4k+3$ ont le nombre en question strictement supérieur à $\lfloor p/4 \rfloor$.

On va utiliser la notation $x\ R\ m$ pour exprimer que x est un résidu quadratique de m et la notation $x\ N\ m$ pour exprimer que x n'est pas un résidu quadratique de m.

On rappelle la définition de *x est un résidu quadratique de m* (notée $x\ R\ m$) :

$$x\ R\ m \iff \exists y \text{ tel que } x^2 \equiv y\ (mod\ m).$$

On a :

- $\forall x, y, m,\ x\ R\ m \text{ et } y\ R\ m \implies xy\ R\ m$
- $\forall x, y, m,\ x\ N\ m \text{ et } y\ N\ m \implies xy\ R\ m$
- $\forall x, y, m,\ x\ R\ m \text{ et } y\ N\ m \implies xy\ N\ m$

En annexe, sont fournis les résidus quadratiques des nombres entiers impairs de 3 à 51 inférieurs à leur moitié ainsi que leur nombre.

On rappelle qu'on peut déduire le caractère de résiduosité quadratique d'un nombre a premier à p un nombre premier impair par un simple calcul de puissance (cf. paragraphe 106 des Recherches arithmétiques de Gauss) :

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}\ (mod\ p)$$

On rappelle que -1 est résidu quadratique de tout nombre premier de la forme $4k+1$ et n'est pas résidu quadratique de tout nombre premier de la forme $4k+3$ (cf. paragraphe 109 des Recherches arithmétiques de Gauss).

Ces particularités du caractère de résiduosité quadratique de -1 aux nombres premiers impairs ont pour conséquence que si p est un nombre premier impair de la forme $4k+1$ alors $r\ R\ p \iff -r\ R\ p$ tandis que si p est un nombre premier impair de la forme $4k+3$ alors $r\ R\ p \iff -r\ N\ p$.

Pour démontrer notre hypothèse, il faudrait démontrer :

1) qu'elle est vraie pour les nombres premiers de la forme $4k+1$;

2) qu'elle est vraie pour les nombres premiers de la forme $4k+3$;

3) qu'elle est vraie par élévation d'un nombre premier p à la puissance k ;

4) qu'elle est vraie par multiplication de deux nombres premiers simples ;

5) qu'elle est vraie par multiplication de deux puissances de nombres premiers (incluant peut-être (4)).

1) Pour les nombres premiers p de la forme $4k+1$, le nombre de résidus quadratiques de p inférieurs ou égaux à $p/2$ est trivialement égal à $\dfrac{p-1}{4}$ car r et $-r$ sont systématiquement soit tous deux résidus quadratiques de p soit tous deux non-résidus quadratiques de p et parce que seul l'un des deux dans chaque couple est inférieur ou égal à $p/2$.

2) Pour les nombres premiers p de la forme $4k+3$, Dirichlet a démontré qu'il y a davantage de petits résidus quadratiques de p que de petits non-résidus quadratiques de p en utilisant l'analyse infinitésimale[1] :

$$\sum_{n=1}^{n=\frac{p-1}{2}} \left(\frac{n}{p}\right) > 0.$$

Dans la suite, l'adjectif *petit* signifie *inférieur ou égal à* $p/2$ et *grand* signifie *supérieur strictement à* $p/2$.

Dans [1], on trouve les relations invariantes suivantes ; notons :

- $\sum R$ la somme des résidus quadratiques de p un nombre premier impair,
- $\sum N$ la somme de ses non-résidus quadratiques,
- $\sum R_b$ la somme de ses "petits" résidus quadratiques,
- $\sum N_b$ la somme de ses "petits" non-résidus quadratiques,
- $\sum R_h$ la somme de ses "grands" résidus quadratiques,
- $\sum N_h$ la somme de ses "grands" non-résidus quadratiques,
- R_b le nombre de ses petits résidus quadratiques ;
- N_b le nombre de ses petits non-résidus quadratiques.

On a, si $p \equiv 7\ (mod\ 8)$:

$$\begin{cases} \sum R_b = \sum N_b. \\ \dfrac{\sum N - \sum R}{p} = R_b - N_b. \end{cases}$$

On a, si $p \equiv 3\ (mod\ 8)$:

$$\begin{cases} \sum R - \sum N = \sum R_b - \sum N_b. \\ \dfrac{3(\sum N - \sum R)}{p} = R_b - N_b. \end{cases}$$

[1] Je ne parviens pas à trouver ce résultat de Dirichlet dont les références possibles sont *Applications de l'analyse infinitésimale à la théorie des nombres*, Journal de Crelle, 1839, vol. 19, p.324-369 ou vol. 21, p.1-12 ou p.134-155.

Concernant les nombres premiers de la forme $p = 8k + 7$, on réalise par le calcul, même si on ne sait pas le démontrer, que la somme des petits résidus quadratiques, qui est égale selon l'un des résultats de Victor-Amédée Lebesgue à la somme des petits non-résidus quadratiques, est égale à :

$$\sum R_b = \frac{(p-1)(p+1)}{16}.$$

Il y a sûrement de très nombreuses fonctions f qui sont telles que $f(7) = 3, f(23) = 33, f(31) = 60, f(47) = 138, f(71) = 315, f(79) = 390, f(103) = 663$ et $f(9967) = 6208818$ mais $f(p) = \frac{(p-1)(p+1)}{16}$ semble pertinente dans ce contexte.

On a ainsi deux ensembles, l'ensemble des petits résidus quadratiques et l'ensemble des petits non-résidus quadratiques, dont les sommes des éléments sont égales à $\frac{(p-1)(p+1)}{16}$, et dont on sait qu'ils sont de cardinaux différents. On sait également que 4 est toujours élément de l'ensemble des petits résidus quadratiques. Ces différents éléments ont peut-être pour conséquence qu'il y a forcément plus de petits résidus quadratiques que de petits non-résidus quadratiques.

Pour illustrer l'idée de la supériorité en nombre des petits résidus quadratiques, on peut présenter la multiplication modulaire modulo 7 sur 2 tables, l'une dans laquelle les nombres sont comme habituellement dans l'ordre croissant, l'autre dans laquelle les résidus quadratiques sont énumérés avant les non-résidus quadratiques.

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

	1	2	4	3	5	6
1	1	2	4	3	5	6
2	2	4	1	6	3	5
4	4	1	2	5	6	3
3	3	6	5	2	1	4
5	5	3	6	1	4	2
6	6	5	3	4	2	1

Sur la table de multiplication modulaire modulo 23, la supériorité en nombre des petits résidus quadratiques sur les petits non-résidus quadratiques apparaît clairement dans le quart haut-gauche de la table. Ce sont peut-être les permutations qui perturbent l'ordre habituel sur les entiers lorsqu'on les considère comme étant des carrés modulaires qui a pour conséquence la loi qui nous semble être toujours vérifiée (ou du moins jusqu'à 300 000).

	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

On peut noter les symétries-miroir horizontale et verticale.

Intéressons-nous au cas qu'on avait numéroté (3) ci-dessus dans le cas où on parviendrait à démontrer formellement notre hypothèse, c'est à dire le fait que pour les nombres n qui sont des puissances de nombres premiers ($n = p^m$ avec p premier), il y a moins de $n/4$ petits résidus quadratiques qui sont inférieurs à $n/2$.

Pour le calcul du nombre de petits résidus quadratiques de p^k une puissance d'un nombre premier p (i.e. les résidus inférieurs ou égaux à $p/2$), on induit des formules en analysant les premières valeurs calculées par ordinateur pour 3 d'abord, car il semble se comporter différemment des autres, puis pour les puissances des nombres premiers de la forme $4k+1$ et enfin, pour les puissances des nombres premiers de la forme $4k+3$.

Des valeurs

$$\begin{aligned} R_b(9) &= 2, \\ R_b(27) &= 6, \\ R_b(81) &= 16, \\ R_b(243) &= 47, \\ R_b(729) &= 138, \\ R_b(2187) &= 412, \\ R_b(6561) &= 1232, \\ R_b(19683) &= 3693, \end{aligned}$$

on induit la formule suivante pour le nombre de petits résidus quadratiques des puissances de 3.

$$R_b(3^k) = \left\lceil \frac{3^{k-1}}{2} \right\rceil + R_b(3^{k-2}).$$

Des valeurs

$$\begin{aligned} R_b(25) &= 5, \\ R_b(125) &= 26, \\ R_b(625) &= 130, \\ R_b(3125) &= 651, \\ R_b(15625) &= 3255, \end{aligned}$$

pour les puissances de 5, puis

$$\begin{aligned} R_b(169) &= 39, \\ R_b(2197) &= 510, \\ R_b(28561) &= 6630, \end{aligned}$$

pour les puissances de 13, on trouve la formule suivante pour le nombre de petits résidus quadratiques des puissances de p pour p de la forme $4k+1$.

$$R_b(p^k) = kp^{k-1} + R_b(p^{k-2}).$$

Ce qu'il est amusant de constater, c'est que cette formule pour les $4k+1$ s'applique également au nombre premier 3 si ce n'est qu'il faut considérer celui-ci non pas comme un $4k+3$, ce qu'on a coutume de faire habituellement, mais plutôt comme un $4k+1$ avec k qui vaudrait $\frac{1}{2}$.

Des valeurs

$$\begin{aligned} R_b(7) &= 2, \\ R_b(49) &= 11, \\ R_b(343) &= 76, \\ R_b(2401) &= 526, \\ R_b(16807) &= 3678, \end{aligned}$$

pour les puissances de 7, puis

$$\begin{aligned} R_b(11) &= 4, \\ R_b(121) &= 29, \\ R_b(1331) &= 308, \\ R_b(14641) &= 3358, \end{aligned}$$

pour les puissances de 11, on induit que le nombre de petits résidus quadratiques des puissances de p pour p de la forme $4k+3$ (sauf 3) est d'un ordre proche de p fois le nombre de petits résidus quadratiques de la puissance de p juste inférieure :

$$R_b(p^k) \approx pR_b(p^{k-1}).$$

Il semble plus judicieux, par un principe de symétrie, de s'intéresser au nombre de grands non-résidus (i.e. supérieurs strictement à $\frac{n-1}{2}$), qu'on note $N_h(n)$. En effet, les valeurs des $N_h(7^k)$ ou des $N_h(11^k)$ sont :

$$\begin{aligned} N_h(7) &= 2, \\ N_h(49 = 7^2) &= 14, \\ N_h(343 = 7^3) &= 97, \\ N_h(2401 = 7^4) &= 676, \end{aligned}$$

$$\begin{aligned} N_h(11) &= 4, \\ N_h(121 = 11^2) &= 34, \\ N_h(1331 = 11^3) &= 363. \end{aligned}$$

L'approximation $N_h(p^k) \approx pN_h(p^{k-1})$ semble de meilleure qualité que l'approximation précédente.

Concernant les produits de puissances (point (5) évoqué plus haut), des valeurs suivantes de $N_h(n)$,

$$\begin{aligned} N_h(3.7) &= 7, \\ N_h(3^2.7) &= 25, \\ N_h(3.7^2) &= 52, \\ N_h(3^2.7^2) &= 178, \end{aligned}$$

$$\begin{aligned} N_h(5.7) &= 13, \\ N_h(5^2.7) &= 68, \\ N_h(5.7^2) &= 91, \\ N_h(5^2.7^2) &= 494, \end{aligned}$$

$$\begin{aligned} N_h(13.17) &= 79, \\ N_h(13^2.17) &= 1081, \\ N_h(13.17^2) &= 1399. \end{aligned}$$

on induit un ordre d'approximation pour $N_h(n)$ $(p < q)$:

$$N_h(p^m.q^n) \approx p.N_h(p^{m-1}.q^n)$$

Concernant les nombres de petits résidus quadratiques dont les valeurs suivent,

$$\begin{array}{ll} R_b(3.7) & = 4, \\ R_b(3^2.7) & = 9, \\ R_b(3.7^2) & = 22, \\ R_b(3^2.7^2) & = 45, \end{array}$$

$$\begin{array}{ll} R_b(5.7) & = 7, \\ R_b(5^2.7) & = 24, \\ R_b(5.7^2) & = 34, \\ R_b(5^2.7^2) & = 123, \end{array}$$

$$\begin{array}{ll} R_b(13.17) & = 31, \\ R_b(13^2.17) & = 355, \\ R_b(13.17^2) & = 479. \end{array}$$

même si on ne peut trouver de règles quant à leur progression, on constate que les valeurs étudiées vérifient toujours :

$$R_b(p^m.q^n) < p.R_b(p^{m-1}.q^n).$$

Le nombre de petits résidus quadratiques pour les puissances de nombres premiers de la forme $p = 4k + 3$ (sauf dans le cas où $p = 3$) est toujours strictement inférieur à $\dfrac{p^k - 1}{4}$ car tous les multiples de p ne peuvent être résidus quadratiques des puissances successives de p, ce qui réduit d'autant le nombre de petits résidus quadratiques.

On peut maintenant démonter le mécanisme à l'oeuvre pour les produits, ce mécanisme ayant pour conséquence une très grande redondance des carrés obtenus, qui réduit d'autant leur nombre, le rendant toujours inférieur au quart du nombre n considéré.

Montrons ce mécanisme sur un exemple simple (en annexe, on fournira comme autre exemple la redondance des carrés dans le cas du nombre $n = 175 = 5^2.7$).

La combinatoire à l'oeuvre, même si elle montre clairement la réduction du nombre de petits résidus quadratiques pour les nombres composés, est trop compliquée pour nous permettre de trouver une formule qui donnerait directement ce nombre de petits résidus quadratiques en fonction de n.

Module $n = 35$ ($R_b(35) = 7$ et $7 < 35/4$)

34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9

Les redondances de carrés pour le module 35 sont :

$$\begin{array}{rlll} 6^2 \equiv 1^2 \ (mod\ 35) & \text{car } (6-1).(6+1) = & 5.7 & \text{et } 35 \mid 35. \\ 11^2 \equiv 4^2 \ (mod\ 35) & \text{car } (11-4).(11+4) = & 7.15 = 105 & \text{et } 35 \mid 105. \\ 12^2 \equiv 2^2 \ (mod\ 35) & \text{car } (12-2).(12+2) = & 10.14 = 105 & \text{et } 35 \mid 140. \\ 13^2 \equiv 8^2 \ (mod\ 35) & \text{car } (13-8).(13+8) = & 5.21 = 105 & \text{et } 35 \mid 105. \\ 16^2 \equiv 9^2 \ (mod\ 35) & \text{car } (16-9).(16+9) = & 7.25 = 175 & \text{et } 35 \mid 175. \\ 17^2 \equiv 3^2 \ (mod\ 35) & \text{car } (17-3).(17+3) = & 14.20 = 280 & \text{et } 35 \mid 280. \end{array}$$

Il reste à étudier le cas des produits de nombres premiers simples, de la forme $p.q$ avec p et q premiers (le point (4) évoqué plus haut). L'étude suggère que le nombre de petits résidus quadratiques $R_b(pq)$ est proche de $\dfrac{R_b(p^2) + R_b(q^2)}{4}$, toujours inférieur à $\dfrac{pq}{4}$. Le mécanisme d'élimination des carrés redondants du fait de l'identité remarquable s'applique à nouveau, faisant diminuer d'autant le nombre de petits résidus quadratiques.

Enfin, si l'objectif est de démontrer formellement notre assertion en utilisant plutôt la théorie des groupes, peut-être que le fait suivant est à considérer pour le comptage des petits résidus quadratiques de produits de puissances de nombres premiers différents : il y a comme un "triangle" de produits qui se répondent ;

le produit d'un $8k+3$ et d'un $8k'+7$ est un $8k''+5$, celui d'un $8k+3$ et d'un $8k'+5$ est un $8k''+7$ et enfin, le produit d'un $8k+5$ et d'un $8k'+7$ est un $8k''+3$.

Conclusion

On réalise, une fois les mécanismes de redondance des carrés analysés et compris, qu'un critère bien plus simple permettant de distinguer les nombres impairs premiers des nombres impairs composés est que les nombres impairs premiers ont leur nombre de résidus quadratiques égal à $\frac{p-1}{2}$ tandis que les nombres impairs composés ont leur nombre de résidus quadratiques strictement inférieur à $\frac{p-1}{2}$.

Bibliographie

[1] Victor-Amédée Lebesgue, *Démonstrations de quelques théorèmes relatifs aux résidus et aux non-résidus quadratiques*, Journal de Mathématiques pures et appliquées (Journal de Liouville), 1842, vol.7, p.137-159.

Annexe 1 : Redondance des carrés pour le module $175 = 5^2.7$

Pour le module 175, on écrit, sous forme de couples, les nombres qui ont même carré, on ne précise pas l'identité remarquable $a^2-b^2=(a-b)(a+b)$ qui est telle que les factorisations des nombres $a-b$ et $a+b$ "contiennent" tous les facteurs de $175 = 5^2.7$:

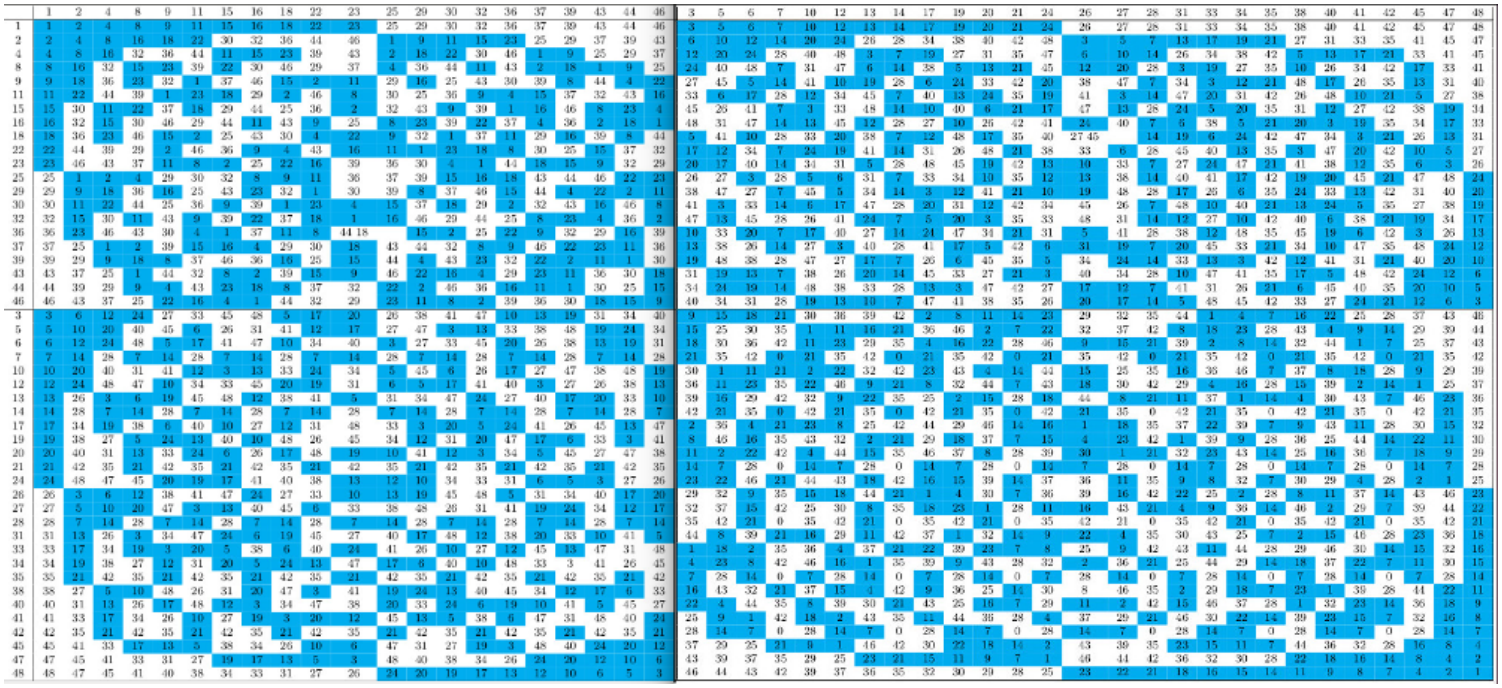
$(16,9),(20,15),(23,2),(25,10),(30,5),(32,18),(37,12),(39,11),(40,5),(41,34),(44,19),$
$(45,10),(46,4),(48,27),(50,15),(51,26),(53,3),(55,15),(57,43),(58,33),(60,10),(62,13),$
$(64,36),(65,5),(66,59),(67,17),(69,6),(71,29),(72,47),(73,52),(74,24),(75,5),(76,1),$
$(78,22),(79,54),(80,10),(81,31),(82,68),(83,8),(85,15),(86,61),(87,38).$

De plus, 35 et 70 ont leur carré nul et on a pris comme convention de ne pas les compter comme petits résidus quadratiques.

Annexe 2 : petits résidus quadratiques des nombres impairs de 3 à 51 et leur nombre

Entre parenthèses est fournie la plus petite racine carrée d'un résidu quadratique du module considéré.

3 → 1.	→ 1
5 → 1.	→ 1
7 → 1, 2 (3).	→ 2
9 → 1, 4 (2).	→ 2
11 → 1, 3 (5), 4 (2), 5 (4).	→ 4
13 → 1, 3 (4), 4 (2).	→ 3
15 → 1, 4 (2), 6 (6).	→ 3
17 → 1, 2 (6), 4 (2), 8 (5).	→ 4
19 → 1, 4 (2), 5 (9), 6 (5), 7 (8), 9 (3).	→ 6
21 → 1, 4 (2), 7 (7), 9 (3).	→ 4
23 → 1, 2 (5), 3 (7), 4 (2), 6 (11), 8 (10), 9 (3).	→ 7
25 → 1, 4 (2), 6 (9), 9 (3), 11 (6).	→ 5
27 → 1, 4 (2), 7 (13), 9 (3), 10 (8), 13 (11).	→ 6
29 → 1, 4 (2), 5 (11), 6 (8), 7 (6), 9 (3), 13 (10).	→ 7
31 → 1, 2 (8), 4 (2), 5 (6), 7 (10), 8 (15), 9 (3), 10 (14), 14 (13).	→ 9
33 → 1, 3 (6), 4 (13), 9 (3), 12 (12), 15 (9), 16 (4).	→ 7
35 → 1, 4 (2), 9 (3), 11 (9), 14 (7), 15 (15), 16 (4).	→ 7
37 → 1, 3 (15), 4 (2), 7 (9), 9 (3), 10 (11), 11 (14), 12 (7), 16 (4).	→ 9
39 → 1, 3 (9), 4 (2), 9 (3), 10 (7), 12 (18), 13 (13), 16 (4).	→ 8
41 → 1, 2 (17), 4 (2), 5 (13), 8 (7), 9 (3), 10 (16), 16 (4), 18 (10), 20 (15).	→ 10
43 → 1, 4 (2), 6 (7), 9 (3), 10 (15), 11 (21), 13 (20), 14 (10), 15 (12), 16 (4), 17 (19), 21 (8).	→ 12
45 → 1, 4 (2), 9 (3), 10 (10), 16 (4), 19 (8).	→ 6
47 → 1, 2 (7), 3 (12), 4 (2), 6 (10), 7 (17), 8 (14), 9 (3), 12 (23), 14 (22), 16 (4), 17 (8), 18 (21), 21 (16).	→ 14
49 → 1, 2 (10), 4 (2), 8 (20), 9 (3), 11 (16), 15 (8), 16 (4), 18 (19), 22 (13), 23 (11).	→ 11
51 → 1, 4 (2), 9 (3), 13 (8), 15 (24), 16 (4), 18 (18), 19 (11), 21 (15), 25 (5).	→ 10



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

	3	5	6	7	10	12	13	14	17	19	20	21	24	26	27	28	31	33	34	35	38	40	41	42	45	47	48
1	3	5	6	7	10	12	13	14	17	19	20	21	24	26	27	28	31	33	34	35	38	40	41	42	45	47	48
2	6	10	12	14	20	24	26	28	34	38	40	42	48	3	5	7	13	17	19	21	27	31	33	35	41	45	47
4	12	20	24	28	40	48	3	7	19	27	31	35	47	6	10	14	26	34	38	42	5	13	17	21	33	41	45
8	24	40	48	7	31	47	6	14	38	5	13	21	45	12	20	28	3	19	27	35	10	26	34	42	17	33	41
9	27	45	5	14	41	10	19	28	6	24	33	42	20	38	47	7	34	3	12	21	48	17	26	35	13	31	40
11	33	6	17	28	12	34	45	7	40	13	24	35	19	41	3	14	47	20	31	42	26	48	10	21	5	27	38
15	45	26	41	7	3	33	48	14	10	40	6	21	17	47	13	28	24	5	20	35	31	12	27	42	38	19	34
16	48	31	47	14	13	45	12	28	27	10	26	42	41	24	40	7	6	38	5	21	20	3	19	35	34	17	33
18	5	41	10	28	33	20	38	7	12	48	17	35	40	27 45		14	19	6	24	42	47	34	3	21	26	13	31
22	17	12	34	7	24	19	41	14	31	26	48	21	38	33	6	28	45	40	13	35	3	47	20	42	10	5	27
23	20	17	40	14	34	31	5	28	48	45	19	42	13	10	33	7	27	24	47	21	41	38	12	35	6	3	26
25	26	27	3	28	5	6	31	7	33	34	10	35	12	13	38	14	40	41	17	42	19	20	45	21	47	48	24
29	38	47	27	7	45	5	34	14	3	12	41	21	10	19	48	28	17	26	6	35	24	33	13	42	31	40	20
30	41	3	33	14	6	17	47	28	20	31	12	42	34	45	26	7	48	10	40	21	13	24	5	35	27	38	19
32	47	13	45	28	26	41	24	7	5	20	3	35	33	48	31	14	12	27	10	42	40	6	38	21	19	34	17
36	10	33	20	7	17	40	27	14	24	47	34	21	31	5	41	28	38	12	48	35	45	19	6	42	3	26	13
37	13	38	26	14	27	3	40	28	41	17	5	42	6	31	19	7	20	45	33	21	34	10	47	35	48	24	12
39	19	48	38	28	47	27	17	7	26	6	45	35	5	34	24	14	33	13	3	42	12	41	31	21	40	20	10
43	31	19	13	7	38	26	20	14	45	33	27	21	3	40	34	28	10	47	41	35	17	5	48	42	24	12	6
44	34	24	19	14	48	38	33	28	13	3	47	42	27	17	12	7	41	31	26	21	6	45	40	35	20	10	5
46	40	34	31	28	19	13	10	7	47	41	38	35	26	20	17	14	5	48	45	42	33	27	24	21	12	6	3
3	9	15	18	21	30	36	39	42	2	8	11	14	23	29	32	35	44	1	4	7	16	22	25	28	37	43	46
5	15	25	30	35	1	11	16	21	36	46	2	7	22	32	37	42	8	18	23	28	43	4	9	14	29	39	44
6	18	30	36	42	11	23	29	35	4	16	22	28	46	9	15	21	39	2	8	14	32	44	1	7	25	37	43
7	21	35	42	0	21	35	42	0	21	35	42	0	21	35	42	0	21	35	42	0	21	35	42	0	21	35	42
10	30	1	11	21	2	22	32	42	23	43	4	14	44	15	25	35	16	36	46	7	37	8	18	28	9	29	39
12	36	11	23	35	22	46	9	21	8	32	44	7	43	18	30	42	29	4	16	28	15	39	2	14	1	25	37
13	39	16	29	42	32	9	22	35	25	2	15	28	18	44	8	21	11	37	1	14	4	30	43	7	46	23	36
14	42	21	35	0	42	21	35	0	42	21	35	0	42	21	35	0	42	21	35	0	42	21	35	0	42	21	35
17	2	36	4	21	23	8	25	42	44	29	46	14	16	1	18	35	37	22	39	7	9	43	11	28	30	15	32
19	8	46	16	35	43	32	2	21	29	18	37	7	15	4	23	42	1	39	9	28	36	25	44	14	22	11	30
20	11	2	22	42	4	44	15	35	46	37	8	28	39	30	1	21	32	23	43	14	25	16	36	7	18	9	29
21	14	7	28	0	14	7	28	0	14	7	28	0	14	7	28	0	14	7	28	0	14	7	28	0	14	7	28
24	23	22	46	21	44	43	18	42	16	15	39	14	37	36	11	35	9	8	32	7	30	29	4	28	2	1	25
26	29	32	9	35	15	18	44	21	1	4	30	7	36	39	16	42	22	25	2	28	8	11	37	14	43	46	23
27	32	37	15	42	25	30	8	35	18	23	1	28	11	16	43	21	4	9	36	14	46	2	29	7	39	44	22
28	35	42	21	0	35	42	21	0	35	42	21	0	35	42	21	0	35	42	21	0	35	42	21	0	35	42	21
31	44	8	39	21	16	29	11	42	37	1	32	14	9	22	4	35	30	43	25	7	2	15	46	28	23	36	18
33	1	18	2	35	36	4	37	21	22	39	23	7	8	25	9	42	43	11	44	28	29	46	30	14	15	32	16
34	4	23	8	42	46	16	1	35	39	9	43	28	32	2	36	21	25	44	29	14	18	37	22	7	11	30	15
35	7	28	14	0	7	28	14	0	7	28	14	0	7	28	14	0	7	28	14	0	7	28	14	0	7	28	14
38	16	43	32	21	37	15	4	42	9	36	25	14	30	8	46	35	2	29	18	7	23	1	39	28	44	22	11
40	22	4	44	35	8	39	30	21	43	25	16	7	29	11	2	42	15	46	37	28	1	32	23	14	36	18	9
41	25	9	1	42	18	2	43	35	11	44	36	28	4	37	29	21	46	30	22	14	39	23	15	7	32	16	8
42	28	14	7	0	28	14	7	0	28	14	7	0	28	14	7	0	28	14	7	0	28	14	7	0	28	14	7
45	37	29	25	21	9	1	46	42	30	22	18	14	2	43	39	35	23	15	11	7	44	36	32	28	16	8	4
47	43	39	37	35	29	25	23	21	15	11	9	7	1	46	44	42	36	32	30	28	22	18	16	14	8	4	2
48	46	44	43	42	39	37	36	35	32	30	29	28	25	23	22	21	18	16	15	14	11	9	8	7	4	2	1

Nombres de résidus quadratiques des nombres premiers ou composés

Denise Vella-Chemla

28.8.2016

On souhaite préciser ici le fait qu'on peut établir le caractère de primalité d'un entier n en comptant le nombre (qu'on note $R(n)$) de ses résidus quadratiques non nuls[1].

Plus précisément, on induit de comptages effectués pour les nombres jusqu'à 100 l'hypothèse (H) suivante :

- *Si n est un nombre impair :*
  - *si $R(n)$ est égal à $(n-1)/2$ alors n est premier.*
  - *si $R(n)$ est inférieur à $(n-1)/2$ alors n est composé ;*
- *Si n est un nombre pair :*
  - *si $R(n)$ est égal à $n/2$ alors n est le double d'un nombre premier ;*
  - *si $R(n)$ est inférieur à $n/2$ alors n est le double d'un nombre composé.*

Cette hypothèse peut s'écrire :

$(H1)$ $\forall n,\ n \geq 3,$

$$R(n) = \#\left\{y \text{ tels que } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kn - y = 0 \text{ avec } 0 < y\right\} < \frac{n}{2}$$

$\iff$

n est le double d'un nombre composé s'il est pair et n est composé s'il est impair

$(H2)$ $\forall n,\ n \geq 3,$

$$R(n) = \#\left\{y \text{ tels que } \exists x \in \mathbb{N}^{\times},\ \exists k \in \mathbb{N},\ x^2 - kn - y = 0 \text{ avec } 0 < y\right\} = \frac{n}{2}$$

$\iff$

n est le double d'un nombre premier s'il est pair et n est premier s'il est impair.

Pour démontrer notre hypothèse, il faudrait prouver :

1) qu'elle est vraie par élévation d'un nombre premier p à la puissance k ;

2) qu'elle est vraie par multiplication de deux puissances de nombres premiers.

On rappelle que le nombre de résidus quadratiques d'un nombre premier p est égal à $\frac{p-1}{2}$.

Essayons de comprendre l'hypothèse heuristiquement.

Le nombre de résidus quadratiques des puissances p^k d'un nombre premier p est toujours strictement inférieur à $\frac{p^k-1}{2}$ car tous les multiples de p ne peuvent être résidus quadratiques des puissances de p.

L'identité remarquable modulaire $a^2 - b^2 \equiv (a-b)(a+b)\ (mod\ n)$ a pour conséquence une grande redondance des carrés obtenables selon le module n et cela réduit le nombre des résidus quadratiques des produits, rendant ce nombre toujours inférieur à la moitié du produit considéré.

[1] On spécifie la non-nullité des résidus considérés une fois pour toutes.

Montrons ce mécanisme sur un exemple simple (en annexe, on fournira comme autre exemple la redondance des carrés dans le cas du nombre $n = 175 = 5^2.7$).

Module $n = 35$ ($R(35) = 11$ et $11 < (35-1)/2$)

34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9

Les redondances de carrés pour le module 35 sont :

$$\begin{array}{lll}
6^2 \equiv 1^2\ (mod\ 35) & \text{car } (6-1).(6+1) = & 5.7 \quad \text{et } 35 \mid 35. \\
11^2 \equiv 4^2\ (mod\ 35) & \text{car } (11-4).(11+4) = & 7.15 = 105 \quad \text{et } 35 \mid 105. \\
12^2 \equiv 2^2\ (mod\ 35) & \text{car } (12-2).(12+2) = & 10.14 = 140 \quad \text{et } 35 \mid 140. \\
13^2 \equiv 8^2\ (mod\ 35) & \text{car } (13-8).(13+8) = & 5.21 = 105 \quad \text{et } 35 \mid 105. \\
16^2 \equiv 9^2\ (mod\ 35) & \text{car } (16-9).(16+9) = & 7.25 = 175 \quad \text{et } 35 \mid 175. \\
17^2 \equiv 3^2\ (mod\ 35) & \text{car } (17-3).(17+3) = & 14.20 = 280 \quad \text{et } 35 \mid 280.
\end{array}$$

Le nombre de résidus quadratiques de 2 et de ses puissances, ou bien d'un premier et de ses puissances sont donnés par les formules ci-dessous :

$$\begin{array}{lll}
R(2) & = 1, & \\
R(4) & = 1, & \\
R(p) & = \dfrac{p-1}{2} & \forall\ p\ premier\ > 2 \\
R(2p) & = p & \forall\ p\ premier\ > 2 \\
R(4p) & = p & \forall\ p\ premier\ > 2 \\
R(2^k) & = \left(\dfrac{3}{2} + \dfrac{2^k}{6} + \dfrac{(-1)^{k+1}}{6}\right) - 1, & \forall\ k > 2 \\
R(p^k) & = \left(\dfrac{3}{4} + \dfrac{(p-1)(-1)^{k+1}}{4(p+1)} + \dfrac{p^{k+1}}{2(p+1)}\right) - 1 & \forall\ p\ premier\ > 2, \forall\ k \geq 2 \\
R\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) & = -1 + \prod_{i=1}^{k} \left(R\left(p_i^{\alpha_i}\right) + 1\right) &
\end{array}$$

Il est à noter que dans le cas des puissances, on soustrait 1 après avoir effectué le calcul entre parenthèses pour obtenir un nombre entier.

Bibliographie

[1] Victor-Amédée Lebesgue, *Démonstrations de quelques théorèmes relatifs aux résidus et aux non-résidus quadratiques*, Journal de Mathématiques pures et appliquées (Journal de Liouville), 1842, vol.7, p.137-159.

[2] Augustin Cauchy, Théorèmes divers sur les résidus et les non-résidus quadratiques, Comptes-rendus de l'Académie des Sciences, T10, 06, 16 mars 1840.

Annexe 1 : Redondance des carrés pour le module $175 = 5^2.7$

Pour le module 175, on écrit, sous forme de couples, les nombres qui ont même carré, on ne précise pas l'identité remarquable $a^2 - b^2 = (a - b)(a + b)$ qui est telle que les factorisations des nombres $a - b$ et $a + b$ "contiennent" tous les facteurs de $175 = 5^2.7$:

$(16, 9), (20, 15), (23, 2), (25, 10), (30, 5), (32, 18), (37, 12), (39, 11), (40, 5), (41, 34), (44, 19),$
$(45, 10), (46, 4), (48, 27), (50, 15), (51, 26), (53, 3), (55, 15), (57, 43), (58, 33), (60, 10), (62, 13),$
$(64, 36), (65, 5), (66, 59), (67, 17), (69, 6), (71, 29), (72, 47), (73, 52), (74, 24), (75, 5), (76, 1),$
$(78, 22), (79, 54), (80, 10), (81, 31), (82, 68), (83, 8), (85, 15), (86, 61), (87, 38).$

De plus, 35 et 70 ont leur carré nul et on a pris comme convention de ne pas les compter comme résidus quadratiques.

$R(175) = 43$ et $43 < (175 - 1)/2$.

Annexe 2 : Nombre de résidus quadratiques non nuls des nombres de 1 à 100

$1 \to 0$	$21 \to 7$	$41 \to 20$	$61 \to 30$	$81 \to 30$
$2 \to 1$	$22 \to 11$	$42 \to 15$	$62 \to 31$	$82 \to 41$
$3 \to 1$	$23 \to 11$	$43 \to 21$	$63 \to 15$	$83 \to 41$
$4 \to 1$	$24 \to 5$	$44 \to 11$	$64 \to 11$	$84 \to 15$
$5 \to 2$	$25 \to 10$	$45 \to 11$	$65 \to 20$	$85 \to 26$
$6 \to 3$	$26 \to 13$	$46 \to 23$	$66 \to 23$	$86 \to 43$
$7 \to 3$	$27 \to 10$	$47 \to 23$	$67 \to 33$	$87 \to 29$
$8 \to 2$	$28 \to 7$	$48 \to 7$	$68 \to 17$	$88 \to 17$
$9 \to 3$	$29 \to 14$	$49 \to 21$	$69 \to 23$	$89 \to 44$
$10 \to 5$	$30 \to 11$	$50 \to 21$	$70 \to 23$	$90 \to 23$
$11 \to 5$	$31 \to 15$	$51 \to 17$	$71 \to 35$	$91 \to 27$
$12 \to 3$	$32 \to 6$	$52 \to 13$	$72 \to 11$	$92 \to 23$
$13 \to 6$	$33 \to 11$	$53 \to 26$	$73 \to 36$	$93 \to 31$
$14 \to 7$	$34 \to 17$	$54 \to 21$	$74 \to 37$	$94 \to 47$
$15 \to 5$	$35 \to 11$	$55 \to 17$	$75 \to 21$	$95 \to 29$
$16 \to 3$	$36 \to 7$	$56 \to 11$	$76 \to 19$	$96 \to 13$
$17 \to 8$	$37 \to 18$	$57 \to 19$	$77 \to 23$	$97 \to 48$
$18 \to 7$	$38 \to 19$	$58 \to 29$	$78 \to 27$	$98 \to 43$
$19 \to 9$	$39 \to 13$	$59 \to 29$	$79 \to 39$	$99 \to 23$
$20 \to 5$	$40 \to 8$	$60 \to 11$	$80 \to 11$	$100 \to 21$

Questions de fin d'été (Denise Vella-Chemla, 30.8.2016)

1) Premier problème :

J'ai lu que Dedekind a constaté que le déterminant d'un groupe cyclique $\begin{vmatrix} x & y & z \\ z & x & y \\ y & z & x \end{vmatrix}$ pouvait se calculer de 2 manières :

a) Par le calcul habituel,

$$\begin{aligned} & x(x^2-yz) - z(xy-z^2) + y(y^2-xz) \\ = \; & x^3 - xyz - xyz + z^3 + y^3 - xyz \\ = \; & x^3 + y^3 + z^3 - 3xyz. \end{aligned}$$

b) ou bien en posant $\omega = \frac{2i\pi}{3}$ (et donc en ayant $\omega = \omega^4$, $\omega^3 = 1$, $\omega + \omega^2 = -1$ et $\omega^2 + \omega^4 = -1$) et en calculant :

$$\begin{aligned} & (x+y+z)(x+\omega y+\omega^2 z)(x+\omega^2 y+\omega z) \\ = \; & (x+y+z)(x^2+\omega^2 xy+\omega xz+\omega xy+\omega^3 y^2+\omega^2 yz+\omega^2 xz+\omega^4 yz+\omega^3 z^2) \\ = \; & (x^3+\omega^2 x^2 y+\omega x^2 z+\omega x^2 y+\omega^3 xy^2+\omega^2 xyz+\omega^2 x^2 z+\omega^4 xyz+\omega^3 xz^2+x^2 y+\omega^2 xy^2+\omega xyz \\ & \quad +\omega xy^2+\omega^3 y^3+\omega^2 y^2 z+\omega^2 xyz+\omega^4 y^2 z+\omega^3 yz^2+x^2 z+\omega^2 xyz+\omega xz^2+\omega xyz+\omega^3 y^2 z \\ & \quad +\omega^2 yz^2+\omega^2 xz^2+\omega^4 yz^2+\omega^3 z^3) \\ = \; & x^3+y^3+z^3+xyz(\omega^2+\omega^4+\omega+\omega^2+\omega^2+\omega) \\ & \quad +x^2 y(\omega^2+\omega+1)+x^2 z(\omega+\omega^2+1)+xy^2(\omega^3+\omega^2+\omega) \\ & \quad +xz^2(\omega^3+\omega+\omega^2)+y^2 z(\omega^2+\omega^4+\omega^3)+yz^2(\omega^3+\omega^2+\omega^4) \\ = \; & x^3+y^3+z^3+xyz(\omega(2+3\omega+\omega^3)) \\ = \; & x^3+y^3+z^3+xyz(\omega(2+3e^{\frac{2i\pi}{3}}+e^{2i\pi})) \\ = \; & x^3+y^3+z^3+xyz(\omega(3+3e^{\frac{2i\pi}{3}})) \\ = \; & x^3+y^3+z^3+xyz(3\omega(1+e^{\frac{2i\pi}{3}})) \\ = \; & x^3+y^3+z^3+xyz(3e^{\frac{2i\pi}{3}}+3e^{-\frac{2i\pi}{3}}) \\ = \; & x^3+y^3+z^3+xyz(3(2\ cos\frac{2i\pi}{3}) \\ = \; & x^3+y^3+z^3+xyz(3(2(-\tfrac{1}{2}))) \\ = \; & x^3+y^3+z^3-3xyz. \end{aligned}$$

(on a utilisé le fait que $e^{ix} + e^{-ix} = 2cosx$).

J'aimerais savoir si ça marche aussi (s'il y a à nouveau égalité) en calculant le déterminant d'un groupe cyclique 4, 5, etc., c'est à dire si à chaque fois, on tombe sur une expression bien symétrique (bien posée sur ses n jambes) de la forme :

$$\sum_{i=1}^{n} x_i^n - n\prod_{i=1}^{n} x_i$$

et si oui, qu'est-ce qu'il faut mettre comme premier produit à calculer par la deuxième méthode, est-ce qu'il faut mettre toutes les combinaisons racine/variable) (et pourtant, ce n'est pas ce qui a été fait pour le degré 3 puisqu'on n'a pas mis d'ω, à quelque puissance que ce soit, devant x dans le deuxième calcul ci-dessus) ?

2) Second problème :

Euler p.249 de l'article *Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs* développe un produit puis effectue un certain nombre de calculs (entre autres des dérivations) pour trouver une formule récurrente de la somme des diviseurs. Le produit qu'il développe est :

$$(1-x)(1-x^2)(1-x^3)(1-x^4)\ldots$$

Que se passerait-il si des traitements similaires étaient effectués sur les produits suivants ?

$$(1-2x)(1-4x^2)(1-9x^3)(1-16x^4)\ldots$$

ou bien

$$(1-ix)(1-ix^2)(1-ix^3)(1-ix^4)\ldots$$

ou bien

$$(1-x)(1+x^2)(1-x^3)(1+x^4)\ldots$$

Indices (Denise Vella-Chemla, 7.9.2016)

On voudrait fournir les résultats d'un programme qui calcule les indices des nombres au sens de l'article 53 des Recherches arithmétiques de Gauss. Gauss explique que l'intérêt des indices est de faciliter les calculs des puissancs modulaires d'une manière similaire à celle dont l'addition des logarithmes facilite le calcul du logarithme d'un produit.

On peut voir sur l'image extraite du chapitre 3 concernant les résidus des puissances le traitement du cas du nombre premier 19. Pour les nombres premiers p, il y a systématiquement une partition de l'ensemble des nombres de 1 à $p-1$ en parties disjointes selon les diviseurs de $p-1$. Le cardinal de la partie associée à un diviseur donné est fourni par l'indicateur d'Euler du diviseur en question.

53. Pour nous faire entendre plus facilement, nous présenterons d'abord un exemple. Soit $p=19$, les nombres 1, 2, 3...18 peuvent se distribuer de la manière suivante relativement aux diviseurs de 18 :

$$1\{1,\quad 2\{18,\quad 3\{7,11,\quad 6\{8,12,\quad 9\{4,5,6,9,16,17,\quad 18\{2,3,10,13,14,15$$

Ainsi dans cas $\downarrow 1=1$, $\downarrow 2=1$, $\downarrow 3=2$, $\downarrow 6=2$, $\downarrow 9=6$, $\downarrow 18=6$. Avec une légère attention on voit qu'il y en a, relativement à chaque exposant, autant qu'il y a de nombres premiers avec cet exposant et non plus grands que lui, ou bien, en reprenant le signe du n° 40, que $\downarrow d=\varphi d$. Mais on peut démontrer généralement cette observation de la manière suivante :

Selon le module 37, les nombres 2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35 ont pour indice 36 (leur puissance $36^{ème}$ vaut 1 modulo 37), les nombres 11 et 27 ont pour indice 6 (leur puissance $6^{ème}$ vaut 1 modulo 37) tandis que les nombres 6 et 31 ont pour indice 4.

On calcule par programme pour les nombres n jusqu'à 100 l'indice des nombres compris entre 1 et $n-1$ et on constate, comme indiqué dans la note 53 de Gauss, que les nombres premiers ont la somme des indices des différentes puissances possibles qui vaut $n-1$. On constate par programme que pour les nombres composés, jusqu'à 100 tout du moins, la somme des indices des différentes puissances possibles est *inférieure* à $\frac{n-1}{2}$ (ce qui semble être dit dans l'article 54).

Nombres de résidus cubiques, biquadratiques, quintiques et sixtiques des nombres premiers ou composés

Denise Vella-Chemla

3.9.2016

On souhaite fournir ici les constats résultant de l'étude du nombre de résidus cubiques, biquadratiques (pour puissances $4^{ème}$), quintiques (pour puissances $5^{ème}$) et sixtiques (pour puissances $6^{ème}$) non nuls des entiers inférieurs à 100. On rappelle qu'on ne compte que les résidus non-nuls des puissances des nombres de 1 à $n-1$ modulo n, i.e. le reste obtenu lorsqu'on divise ces puissances par n.

On note $R_3(n)$ le nombre de résidus cubiques non nuls de n, $R_4(n)$ le nombre de résidus biquadratiques non nuls de n, $R_5(n)$ le nombre de résidus quintiques non nuls de n et $R_6(n)$ le nombre de résidus sixtiques non nuls de n.

Concernant les résidus cubiques, il semblerait que :

- Si n est un nombre de la forme $3k+1$:
  - si $R_3(n)$ est égal à $(n-1)/3$ alors n est un nombre premier ;
  - si $R_3(n)$ est supérieur à $(n-1)/3$ alors n est un nombre composé ;
- Si n est un nombre de la forme $3k+2$ (avec une exception pour 17) :
  - si $R_3(n)$ est égal à $n-1$ alors n est un nombre premier ;
  - si $R_3(n)$ est inférieur à $n-1$ alors n est un nombre composé.

Cette hypothèse est infirmée par programme : 935 est un nombre composé et son nombre de résidus cubiques est 934. Les hypothèses ci-dessous seraient vraisemblablement infirmées également, on ne les teste pas.

On essaie cependant d'obtenir un tout petit élément de compréhension en cherchant une régularité derrière ces nombres composés n qui ont pile $n-1$ résidus cubiques : on factorise les 8 plus grands nombres pour lesquels ceci s'est produit pour "voir la tête de leur factorisation" et on est surpris de constater la chose suivante :

$9095 = 5.17.107$, $9185 = 5.11.167$, $9515 = 5.11.173$, $9545 = 5.23.83$, $9605 = 5.17.113$, $9635 = 5.41.47$, $9845 = 5.11.179$, $9911 = 11.17.53$ et il y avait le cas auquel on s'est intéressé le premier $935 = 5.11.17$.

Tous ces nombres sont produits de 3 nombres premiers tout trois de la forme $6k-1$.

Concernant les résidus biquadratiques (résidus des puissances $4^{èmes}$), il semblerait que :

- Si n est un nombre de la forme $4k+3$:
  - si $R_4(n)$ est égal à $(n-1)/2$ alors n est un nombre premier ;
  - si $R_4(n)$ est inférieur à $(n-1)/2$ alors n est un nombre composé ;
- Si n est un nombre de la forme $4k+1$:
  - si $R_4(n)$ est égal à $(n-1)/4$ alors n est un nombre premier ;
  - si $R_4(n)$ est supérieur à $(n-1)/4$ alors n est un nombre composé.

63% des nombres de 1 à 100 ont un résidu biquadratique qui est un nombre premier, ça semble une proportion extraordinaire.

Concernant les résidus quintiques (résidus des puissances $5^{èmes}$), il semblerait que :

- Si n est un nombre de la forme $5k+1$:
  - si $R_5(n)$ est égal à $(n-1)/5$ alors n est un nombre premier ;
  - si $R_5(n)$ est supérieur à $(n-1)/5$ alors n est un nombre composé ;

- Si n est un nombre de la forme $5k+2$:
  - si $R_5(n)$ est égal à $n-1$ alors n est un nombre premier ;
  - si $R_5(n)$ est inférieur à $n-1$ alors n est un nombre composé ;

- Si n est un nombre de la forme $5k+3$:
  - si $R_5(n)$ est égal à $n-1$ alors n est un nombre premier ;
  - si $R_5(n)$ est inférieur à $n-1$ alors n est un nombre composé ;

- Si n est un nombre de la forme $5k+4$:
  - si $R_5(n)$ est égal à $n-1$ alors n est un nombre premier ;
  - si $R_5(n)$ est inférieur à $n-1$ alors n est un nombre composé.

Concernant les résidus sixtiques (résidus des puissances $6^{èmes}$), on ne constate rien de bien probant, vraisemblablement parce que 6 est composé :

- Si n est un nombre de la forme $6k+1$:
  - on souhaiterait que si $R_6(n)$ est égal à $(n-1)/6$ alors n soit un nombre premier mais ce souhait est mis en défaut par 43, 61 ou 67.

- Si n est un nombre de la forme $6k-1$:
  - on souhaiterait que si $R_6(n)$ est égal à $(n-1)/2$ alors n soit un nombre premier mais ce souhait est mis en défaut par 47.

Annexe 1 : Nombre de résidus cubiques non nuls des nombres de 1 à 100

Ici, ce qui est surprenant, c'est le fait que les images soient quasiment la suite des entiers décalée de 1 par rapport à la suite des antécédents (on met des étoiles entre parenthèses pour le montrer et les nombres premiers apparaissent en bleu).

1 → 0 (∗)	21 → 8	41 → 40 (∗)	61 → 20	81 → 20
2 → 1 (∗)	22 → 21 (∗)	42 → 17	62 → 21	82 → 81 (∗)
3 → 2 (∗)	23 → 22 (∗)	43 → 14	63 → 8	83 → 82 (∗)
4 → 2	24 → 14	44 → 32	64 → 36	84 → 26
5 → 4 (∗)	25 → 20	45 → 14	65 → 24	85 → 84 (∗)
6 → 5 (∗)	26 → 9	46 → 45 (∗)	66 → 65 (∗)	86 → 29
7 → 2	27 → 6	47 → 46 (∗)	67 → 22	87 → 86 (∗)
8 → 4	28 → 8	48 → 29	68 → 50	88 → 54
9 → 2	29 → 28 (∗)	49 → 14	69 → 68 (∗)	89 → 88 (∗)
10 → 9 (∗)	30 → 29 (∗)	50 → 41	70 → 29	90 → 29
11 → 10 (∗)	31 → 10	51 → 50 (∗)	71 → 70 (∗)	91 → 14
12 → 8	32 → 18	52 → 14	72 → 14	92 → 68
13 → 4	33 → 32 (∗)	53 → 52 (∗)	73 → 24	93 → 32
14 → 5	34 → 33 (∗)	54 → 13	74 → 25	94 → 93 (∗)
15 → 14 (∗)	35 → 14	55 → 54 (∗)	75 → 62	95 → 34
16 → 9	36 → 8	56 → 14	76 → 20	96 → 56
17 → 16	37 → 12	57 → 20	77 → 32	97 → 32
18 → 5	38 → 13	58 → 57 (∗)	78 → 29	98 → 29
19 → 6	39 → 14	59 → 58 (∗)	79 → 26	99 → 32
20 → 14	40 → 24	60 → 44	80 → 49	100 → 62

Annexe 2 : Nombre de résidus biquadratiques non nuls des nombres de 1 à 100

On met entre parenthèses le nombre de résidus quadratiques quand il est différent du résidu biquadratique pour montrer les ressemblances, les puissances quatrièmes étant des carrés particuliers.

1 → 0	21 → 7	41 → 10 (20)	61 → 15 (30)	81 → 27 (30)
2 → 1	22 → 11	42 → 15	62 → 31	82 → 21 (41)
3 → 1	23 → 11	43 → 21	63 → 15	83 → 41
4 → 1	24 → 3 (5)	44 → 11	64 → 5 (11)	84 → 15
5 → 1 (2)	25 → 5 (10)	45 → 7 (11)	65 → 7 (20)	85 → 9 (26)
6 → 3	26 → 7 (13)	46 → 23	66 → 23	86 → 43
7 → 3	27 → 9 (10)	47 → 23	67 → 33	87 → 15 (29)
8 → 1 (2)	28 → 7	48 → 3 (7)	68 → 9 (17)	88 → 11 (17)
9 → 3	29 → 7 (14)	49 → 21	69 → 23	89 → 22 (44)
10 → 3 (5)	30 → 7 (11)	50 → 11 (21)	70 → 15 (23)	90 → 15 (23)
11 → 5	31 → 15	51 → 9 (17)	71 → 35	91 → 15 (27)
12 → 3	32 → 3 (6)	52 → 7 (13)	72 → 7 (11)	92 → 23
13 → 3 (6)	33 → 11	53 → 13 (26)	73 → 18 (36)	93 → 31
14 → 7	34 → 9 (17)	54 → 19 (21)	74 → 19 (37)	94 → 47
15 → 3 (5)	35 → 7 (11)	55 → 11 (17)	75 → 11 (21)	95 → 19 (29)
16 → 1 (3)	36 → 7	56 → 7 (11)	76 → 19	96 → 7 (13)
17 → 4 (8)	37 → 9 (18)	57 → 19	77 → 23	97 → 24 (48)
18 → 7	38 → 19	58 → 15 (29)	78 → 15 (27)	98 → 43
19 → 9	39 → 7 (13)	59 → 29	79 → 39	99 → 23
20 → 3 (5)	40 → 3 (8)	60 → 7 (11)	80 → 3 (11)	100 → 11 (21)

Annexe 3 : Nombre de résidus quintiques non nuls des nombres de 1 à 100

Ici, ce qui est surprenant, c'est à nouveau le fait que les images soient, au début tout du moins, quasiment la suite des entiers décalée de 1 par rapport à la suite des antécédents (on met des étoiles entre parenthèses pour le montrer) mais ça cesse rapidement.

1 → 0 (∗)	21 → 20 (∗)	41 → 8	61 → 12	81 → 50
2 → 1 (∗)	22 → 5	42 → 41 (∗)	62 → 13	82 → 18
3 → 2 (∗)	23 → 22 (∗)	43 → 42 (∗)	63 → 48	83 → 73
4 → 2	24 → 14	44 → 8	64 → 33	84 → 58
5 → 4 (∗)	25 → 4	45 → 34	65 → 64 (∗)	85 → 73
6 → 5 (∗)	26 → 25 (∗)	46 → 45 (∗)	66 → 17	86 → 74
7 → 6 (∗)	27 → 18	47 → 46 (∗)	67 → 66 (∗)	87 → 74
8 → 4	28 → 20	48 → 26	68 → 50	88 → 16
9 → 6	29 → 28 (∗)	49 → 42	69 → 68 (∗)	89 → 77
10 → 9 (∗)	30 → 29 (∗)	50 → 9	70 → 69 (∗)	90 → 59
11 → 2	31 → 6	51 → 50 (∗)	71 → 14	91 → 76
12 → 8	32 → 16	52 → 38	72 → 34	92 → 60
13 → 12 (∗)	33 → 8	53 → 52 (∗)	73 → 72 (∗)	93 → 22
14 → 13 (∗)	34 → 33 (∗)	54 → 37	74 → 73 (∗)	94 → 75
15 → 14 (∗)	35 → 34 (∗)	55 → 14	75 → 14	95 → 78
16 → 8	36 → 20	56 → 34	76 → 55	96 → 40
17 → 16 (∗)	37 → 36 (∗)	57 → 56 (∗)	77 → 21	97 → 74
18 → 13	38 → 37 (∗)	58 → 57 (∗)	78 → 74	98 → 68
19 → 18 (∗)	39 → 38 (∗)	59 → 58 (∗)	79 → 73	99 → 25
20 → 14	40 → 24	60 → 44	80 → 42	100 → 21

Annexe 4 : Nombre de résidus sixtiques non nuls des nombres de 1 à 100

$1 \to 0$	$21 \to 3$	$41 \to 20$	$61 \to 19$	$81 \to 30$
$2 \to 1$	$22 \to 11$	$42 \to 8$	$62 \to 16$	$82 \to 43$
$3 \to 1$	$23 \to 11$	$43 \to 9$	$63 \to 11$	$83 \to 44$
$4 \to 1$	$24 \to 3$	$44 \to 15$	$64 \to 9$	$84 \to 22$
$5 \to 2$	$25 \to 10$	$45 \to 9$	$65 \to 17$	$85 \to 40$
$6 \to 3$	$26 \to 5$	$46 \to 24$	$66 \to 32$	$86 \to 34$
$7 \to 1$	$27 \to 3$	$47 \to 26$	$67 \to 20$	$87 \to 43$
$8 \to 1$	$28 \to 3$	$48 \to 6$	$68 \to 25$	$88 \to 20$
$9 \to 1$	$29 \to 14$	$49 \to 11$	$69 \to 31$	$89 \to 52$
$10 \to 5$	$30 \to 11$	$50 \to 26$	$70 \to 23$	$90 \to 33$
$11 \to 5$	$31 \to 5$	$51 \to 21$	$71 \to 44$	$91 \to 30$
$12 \to 3$	$32 \to 4$	$52 \to 12$	$72 \to 12$	$92 \to 32$
$13 \to 2$	$33 \to 11$	$53 \to 28$	$73 \to 22$	$93 \to 30$
$14 \to 3$	$34 \to 17$	$54 \to 15$	$74 \to 27$	$94 \to 51$
$15 \to 5$	$35 \to 5$	$55 \to 23$	$75 \to 35$	$95 \to 32$
$16 \to 2$	$36 \to 3$	$56 \to 9$	$76 \to 18$	$96 \to 14$
$17 \to 8$	$37 \to 7$	$57 \to 14$	$77 \to 26$	$97 \to 40$
$18 \to 3$	$38 \to 8$	$58 \to 34$	$78 \to 26$	$98 \to 39$
$19 \to 3$	$39 \to 5$	$59 \to 35$	$79 \to 27$	$99 \to 38$
$20 \to 5$	$40 \to 7$	$60 \to 19$	$80 \to 15$	$100 \to 37$

Racines, chemins pour atteindre l'unité, cardinaux (Denise Vella-Chemla, 10.9.2016)

On voudrait ici fournir les derniers constats qu'on a effectués sur des résultats de programmes. On procède par une méthode assez expérimentale, rappelant celle préconisée par la Fondation La main à la pâte : on programme un résultat dont on a trouvé des exemples simples dans la littérature, on observe les résultats du programme, on émet de nouvelles hypothèses, qu'on cherche à retrouver dans la littérature, le but ultime et idéal étant d'aboutir à une démonstration des conjectures émises au fur et à mesure de l'expérimentation.

Le constat est que de même qu'un nombre premier p a un nombre maximum $\frac{p-1}{2}$ de résidus quadratiques[1], il y a également un nombre maximum (égal à $\varphi(p) = p-1$) de nombres qui sont inférieurs à p et qui ont une puissance égalant l'unité modulo p (cf l'article 54 des Recherches arithmétiques de Gauss).

Le point de départ des travaux en cours est l'article 53 des Recherches arithmétiques. On dispose de deux fichiers résultats de programmes :

- le fichier racunit500.pdf qui fournit pour un nombre n inférieur à 500 ses *"racines de l'unité"* r_i, i.e. les nombres dont une certaine puissance α_i est égale à 1 modulo le nombre n considéré ($r_i^{\alpha_i} \equiv 1\ (mod\ n)$) ;
- le fichier montreplusgrandepuiss2016.pdf qui fournit seulement les exposants qui permettent d'atteindre 1 (sans les racines).

Les constats sont les suivants :

- la puissance $p-1^{ème}$ permet d'atteindre l'unité pour les modules p premiers, c'est un fait connu et démontré ; dans le cas où p est un nombre premier, et seulement dans ce cas, il semblerait que, pour chaque puissance possible α_i, il y a $\varphi(\alpha_i)$ nombres qui élevés à cette puissance permettent d'aboutir à 1 ; Gauss explique cela dans son article 54 ($\varphi(x)$ désigne l'indicateur d'Euler de x, i.e. le nombre de nombres y inférieurs à x et qui lui sont premiers (tels que $(x,y) = pgcd(x,y) = 1)$) ; il y a donc pour les nombres premiers p un nombre maximum $(p-1)$ de nombres qui ont une puissance qui égale l'unité ;
- dans le cas où p est un nombre premier, les puissances successives qui permettent d'atteindre l'unité sont un ensemble de nombres constitué d'un plus grand nombre et de tous ses diviseurs (à l'époque de Gauss, elles étaient appelées les "parties aliquotes" de $p-1$) ; cette propriété n'est pas vérifiée par les nombres composés : par exemple, pour 203, la liste des puissances est $84, 42, 28, 21, 14, 12, 7, 6, 4, 3, 2, 1$;
- les puissances possibles permettant à des nombres d'atteindre l'unité modulo n (qu'il soit premier ou composé) sont toujours des diviseurs de $\varphi(n)$ (cela est dû au théorème d'Euler) ;
- aucun nombre non premier à n (i.e. partageant un facteur supérieur ou égal à 2 avec n) n'a une puissance égale à l'unité ; on imaginerait bien affecter comme puissance aux nombres en question ∞ de manière à ce que tout nombre de 1 à $n-1$ se voit pourvu d'un exposant à la puissance duquel il atteint l'unité (cet exposant fût-il infini) ;
- pour un nombre de la forme 2^k, 2^{k-2} est la plus grande puissance permettant d'atteindre l'unité, les autres puissances étant les puissances décroissantes de 2 ;
- pour un nombre de la forme p^k avec p premier, la plus grande puissance possible qui permet d'atteindre l'unité est $p^k - p^{k-1}$;
- un nombre et son double ont presque toujours le même ensemble de puissances permettant à des racines d'atteindre l'unité (cela n'est pas vérifié pour certains multiples de 16) ;
- pour les nombres impairs dont la factorisation est un produit de plusieurs facteurs premiers différents, c'est un peu plus complexe : il semblerait que les puissances possibles pour atteindre l'unité soient des diviseurs du produit $\prod(p_i - 1)$, les p_i étant les facteurs intervenant dans la factorisation de n. C'est aussi une conséquence du théorème d'Euler.

[1] On s'est intéressé à ce fait dans une note précédente carresimple.pdf.

Observons un phénomène qui nous intrigue, bien qu'il soit certainement connu des mathématiciens, et qui permet encore de distinguer les nombres premiers des nombres composés.

Considérons le nombre composé 203, d'indicateur d'Euler égal à $\varphi(203) = 168$. Les exposants à utiliser pour atteindre l'unité modulo 203 sont les suivants, dont on fournit pour chacun l'indicateur d'Euler corrrespondant entre parenthèses.

84 ($\varphi(84) = 24$) 42 (12) 28 (12) 21 (12) 14 (6) 12 (4) 7 (6) 6 (2) 4 (2) 3 (2) 2 (1) 1 (1)

La somme des indicateurs d'Euler entre parenthèses est égal à 84, inférieur à $\varphi(203)$.

Si on considère plutôt le nombre premier 101, d'indicateur d'Euler égal à $\varphi(101) = 100$. Les exposants à utiliser pour atteindre l'unité modulo 101 sont les suivants, dont on fournit pour chacun l'indicateur d'Euler corrrespondant.

100 ($\varphi(100) = 40$) 50 (20) 25 (20) 20 (8) 10 (4) 5 (4) 4 (2) 2 (1) 1 (1)

La somme des indicateurs d'Euler entre parenthèses est égal à 100, égal à $\varphi(101)$.

Si on observe maintenant les cardinaux des ensembles de racines qui à telle ou telle puissance atteignent l'unité, ils sont bien égaux aux indicateurs d'Euler successifs dans le cas des nombres premiers, mais ils en sont différents dans le cas des nombres composés. Dans le cas du nombre composé 203, les cardinaux des ensembles successifs de racines sont indiqués entre parenthèses ci-dessous et à comparer aux indicateurs d'Euler fournis plus haut.

84 ($\#(84) = 48$) 42 (36) 28 (24) 21 (12) 14 (14) 12 (8) 7 (6) 6 (6) 4 (4) 3 (2) 2 (3) 1 (1)

Concernant l'article 92, on trouve bien, comme l'indique Gauss, pour 1001 comme exposant maximum permettant à des nombres d'atteindre l'unité le nombre 60 qui est le plus petit commun multiple des nombres 6, 10 et 12, les nombres précédents les facteurs de $1001 = 7.11.13$, mais ce n'est pas le ppcm qui fournit la plus grande puissance possible pour le nombre $2009 = 41.7^2$ comme on peut le constater dans le fichier dim20160911am.pdf qui fournit aussi les ppcm des nombres précédents les facteurs du nombre considéré ainsi que la somme des indicateurs d'Euler des exposants possibles pour atteindre l'unité.

Notre objectif serait d'établir des fonctions entre ensembles de mêmes suites de puissances : par exemple, les exposants pour 60 sont 4, 2 et 1 et ce sont les mêmes puissances qui caractérisent le nombre 5. Par contre, les cardinaux des ensembles associés aux exposants sont différents (8,7,1 pour 60 et 2,1,1 pour 5). Il faudrait trouver un moyen d'envoyer les éléments dans les ensembles de 60 sur ceux dans les ensembles de 5.

```
#include <iostream>
#include <cmath>
#include <stdio.h>
#include <set>
#include <algorithm>
#include <functional>
#include <climits>

int tabfacteurs[2018], tabpuiss[2018], tabexpo[2018], residfacteurs[2018] ;

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 pgcd(int m, int n)
{
  while (m  != 0)
    {
      int r ;

      r = n % m ;
      n = m ;
      m = r ;
    }
  return(n) ;
}

int main (int argc, char* argv[]) {
  int i, j, k, p, nbdiv, nbdivmax, nbresid, nbresidbas, nbresidhaut, tempo,
dejavu, expo, puiss, x, y, prodpmoinsun, tmp, indic ;
  float residfacteurs[2018] ;
  bool boolpremier ;
  int tab[2018] ;

  for (i = 1 ; i <= 2016 ; ++i)
    //i = 5 ;
    {
      std::cout << "\n\n" << i << " -> " ;
      prodpmoinsun=1 ;
      tab[i] = 1 ;
      tabfacteurs[i] = 1 ;
      tabpuiss[i] = 1 ;
      tabexpo[i] = 1 ;
      residfacteurs[i] = 1.0 ;
      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] << "." ;
  for (tmp = 1 ; tmp <= tabexpo[k] ; ++tmp)
    prodpmoinsun = prodpmoinsun*(tabfacteurs[k]-1) ;
}

indic = 1 ;
for (tmp=2 ; tmp <= i-1 ; ++tmp) if (pgcd(i,tmp)==1) indic++ ;
std::cout << "\nphi -> " << indic ;

std::cout << "\n" ;

std::cout << "puissances -> " ;
tab[1] = 1 ;
for (j = 2 ; j <= i-1 ; ++j)
```

```
      {
        puiss = (j*j) % i ;
        expo = 2 ;
        while ((puiss != 1) && (puiss != j) && (expo <= i-1))
          {
            puiss = (puiss * j) % i ;
            expo = expo+1 ;
          }
        if (puiss == 1)
          {
            tab[j] = expo ;
          }
        else tab[j] = 0 ;
      }
      for (x = i-1 ; x >= 1 ; --x)
      {
        boolpremier = true ;
        for (y = 1 ; y <= i-1 ; ++y)
          {
            if (tab[y] == x)
            {
              if (boolpremier == true)
                {
                  std::cout << x << "  " ;
                  boolpremier = false ;
                }
            }
          }
      }
    }
}
```

Pgcd et diagonales de booléens (Denise Vella-Chemla, 22.10.2016)

Dans une note récente, on a calculé par programme les racines de l'unité (notées x) des entiers successifs (notés n), i.e. les nombres dont la division d'une puissance x^k par n avait pour reste 1 (x est tel que $\exists k, 1 \leqslant k \leqslant n-1,\ x^k \equiv 1\ (mod\ n)$). On rappelle que deux nombres *premiers entre eux* ont un plus grand commun diviseur ($pgcd(x,n)$) égal à 1. On a réalisé en étudiant les racines de l'unité que seul un nombre *premier à n* peut avoir l'une de ses puissances congrue à 1 modulo n.

On se propose ici d'étudier une table de booléens associés à la relation *premier à* qui lie deux nombres. Dans cette table, pour les nombres x compris entre 3 et 51, on note pour chaque nombre y compris entre 1 et $\left\lfloor \frac{x}{2} \right\rfloor$ la valeur de vérité (booléenne) de $(x,y) = 1$ (le booléen de la case (x,y) de la table vaut donc 1 pour tout nombre y premier à x et 0 pour les autres s'il y en a)[1]. On note en rouge les diagonales de 1 "issues" du nombre premier 23.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
3 :	1																								
4 :	1	0																							
5 :	1	1																							
6 :	1	0	0																						
7 :	1	1	1																						
8 :	1	0	1	0																					
9 :	1	1	0	1																					
10 :	1	0	1	0	0																				
11 :	1	1	1	1	1																				
12 :	1	0	0	0	1	0																			
13 :	1	1	1	1	1	1																			
14 :	1	0	1	0	1	0	0																		
15 :	1	1	0	1	0	0	1																		
16 :	1	0	1	0	1	0	1	0																	
17 :	1	1	1	1	1	1	1	1																	
18 :	1	0	0	0	1	0	1	0	0																
19 :	1	1	1	1	1	1	1	1	1																
20 :	1	0	1	0	0	0	1	0	1	0															
21 :	1	1	0	1	1	0	0	1	0	1															
22 :	1	0	1	0	1	0	1	0	1	0	0														
23 :	1	1	1	1	1	1	1	1	1	1	1														
24 :	1	0	0	0	1	0	1	0	0	0	1	0													
25 :	1	1	1	1	0	1	1	1	1	0	1	1													
26 :	1	0	1	0	1	0	1	0	1	0	1	0	0												
27 :	1	1	0	1	1	0	1	1	0	1	1	0	1												
28 :	1	0	1	0	1	0	0	0	1	0	1	0	1	0											
29 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1											
30 :	1	0	0	0	0	0	1	0	0	0	1	0	1	0	0										
31 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1										
32 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0									
33 :	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1									
34 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0								
35 :	1	1	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1								
36 :	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0							
37 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1							
38 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0						
39 :	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	1						
40 :	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0					
41 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1					
42 :	1	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	1	0	1	0	0				
43 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
44 :	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0			
45 :	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1			
46 :	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0		
47 :	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
48 :	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	
49 :	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	
50 :	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0
51 :	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1	1	0	1

Aux nombres premiers correspondent ainsi des diagonales de plus grands communs diviseurs valant 1 :

$$\forall\ p\ premier, \quad \forall x, 1 \leqslant x \leqslant \lfloor \tfrac{p-1}{3} \rfloor, (p-x, x) = 1.$$
$$\forall x, 1 \leqslant x \leqslant p-1, (p+x, x) = 1.$$

[1] On note parfois le plus grand commun diviseur de x et y ($pgcd(x,y)$) en utilisant le symbole $\wedge$ (et logique) : $x \wedge y = 1$).

Pgcd et trajets de booléens (Denise Vella-Chemla, 22.10.2016)

Dans une note récente, on a calculé par programme les racines de l'unité (notées x) des entiers successifs (notés n), i.e. les nombres dont la division d'une puissance x^k par n avait pour reste 1 (x est tel que $\exists k, 1 \leqslant k \leqslant n-1,\ x^k \equiv 1\ (mod\ n)$). On rappelle que deux nombres x et n *premiers entre eux* ont leur plus grand commun diviseur ($pgcd(x,n)$) égal à 1. On a réalisé en étudiant les racines de l'unité que seul un nombre *premier à* n peut avoir l'une de ses puissances congrue à 1 modulo n.

On se propose ici d'étudier une table de booléens associés à la relation *premier à* qui lie deux nombres. Dans cette table, pour les nombres x compris entre 1 et 52, on note pour chaque nombre y compris entre 1 et 26 la valeur de vérité (booléenne) de $(x,y) = 1$ (le booléen de la case (x,y) de la table vaut donc 1 pour tout nombre y premier à x et 0 pour les autres s'il y en a)[1]. On note en couleur quelques trajets de nombres à observer.

On constate (table suivante) que des nombres $p-1$ précédant ou $p+1$ succédant à un nombre premier p (sur le bord gauche de la table) partent des trajets (de couleur rouge), constituées exclusivement de plus grands communs diviseurs valant 1 à cause des relations :

$$\begin{array}{rl} \forall\ p\ premier, & \forall x, 1 \leqslant x \leqslant p-1, (p-x,x) = 1. \\ & \forall x, 1 \leqslant x \leqslant p-1, (p+x,x) = 1. \end{array}$$

Du coup, on a comme l'impression que 23 nous "a amenée" à 29.

On constate aussi que les mots correspondant aux trajets montant et descendant de deux nombres séparés de 2 sont identiques. On a coloré dans la deuxième table les mots associés à 5 et 7 en rouge, à 17 et 19 en vert, ou encore à 24 et 26 en cyan.

[1] On note parfois le plus grand commun diviseur de x et y ($pgcd(x,y)$) en utilisant le symbole $\wedge$ (et logique) : $x \wedge y = 1$).

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
3	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
4	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
5	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1
6	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
7	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1
8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
9	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
10	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
11	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1
12	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
13	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0
14	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0
15	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	1	0	0	1
16	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
18	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1
20	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
21	1	1	0	1	1	0	0	1	0	1	1	0	1	0	0	1	1	0	1	1	0	1	1	0	1	1
22	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
23	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1
24	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
25	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1
26	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0
27	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
28	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0
29	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	1	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	0	0
31	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
32	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
33	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1
34	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0
35	1	1	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	1	0	0	1	1	1	0	1
36	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
37	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
38	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0
39	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	1	1	0	1	1	0	1	0
40	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
41	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
42	1	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
43	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
44	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
45	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	1	0	0	1
46	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0
47	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
48	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
49	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1
50	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
51	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1	1	0	1	1
52	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0

1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
3	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
4	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
5	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1
6	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
7	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	1	0	1	1	1	1
8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
9	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
10	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
11	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1
12	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
13	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	0
14	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0
15	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	1	0	0	1
16	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1
18	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1
20	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
21	1	1	0	1	1	0	0	1	0	1	1	0	1	0	0	1	1	0	1	1	0	1	1	0	1	1
22	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
23	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1
24	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
25	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1	1	1	1	0	1
26	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0
27	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
28	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0
29	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	1	0	0	0	0	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	0	0
31	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
32	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
33	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1
34	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0
35	1	1	1	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	1	0	0	1	1	1	0	1
36	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
37	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
38	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0
39	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	1	1	0	1	1	0	1	0
40	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
41	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
42	1	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
43	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
44	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0
45	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1	1	0	1	0	0	1	1	0	0	1
46	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0
47	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
48	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0
49	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1	1	1	1
50	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	0	0
51	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1	1	0	1	1
52	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	1	0	1	0	1	0	1	0

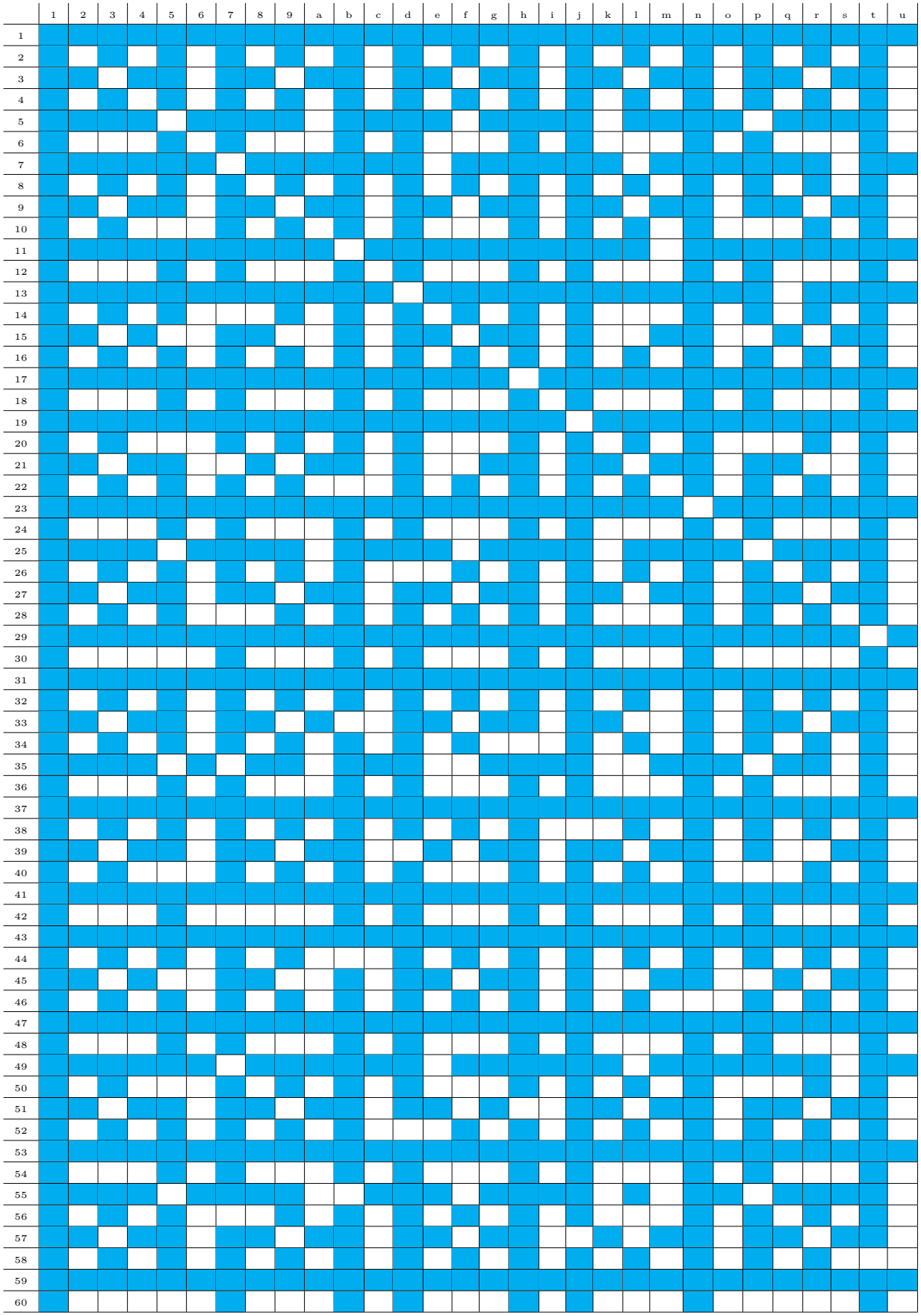
Table de la relation "premier à" (Denise Vella-Chemla, 23.10.2016)

On continue d'étudier une table de booléens associés à la relation "*premier à*" qui lie deux nombres. Cette relation est symétrique.

Dans cette table, on colorie une case si elle contient le booléen vrai et on la laisse blanche sinon. On choisit de noter $x \wedge y$ le plus grand commun diviseur de x et y. Pour x compris entre 1 et 60 et pour y compris entre 1 et 30, la case (x, y) code la valeur de vérité (booléenne) de l'assertion logique $x \wedge y = 1$ (le booléen de la case (x, y) de la table vaut donc 1 pour tout nombre y premier à x et 0 pour les autres s'il y en a).

Cette table est telle que toute ligne (celle de x) contient les mêmes éléments que ceux d'une diagonale montante (celle de $x - 1$) ou que ceux d'une diagonale descendante (celle de $x + 1$). Ces propriétés de la table découlent du fait que $\forall x, y \in \mathbb{N}^*$ avec $\mathrm{y} < \mathrm{x}, \mathrm{x} \wedge \mathrm{y} = (\mathrm{x} - \mathrm{y}) \wedge \mathrm{y}$ et $\forall x, y \in \mathbb{N}^*, x \wedge y = (x + y) \wedge y$.

Aux nombres premiers correspondent des lignes (et diagonales associées) quasi-continues. Les lettres a à u entête de colonnes correspondent aux nombres de 10 à 30 (pour ne pas augmenter la largeur des colonnes par des nombres à 2 chiffres).


1 2 3 4 5 6 7 8 9 a b c d e f g h i j k l m n o p q r s t u
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60

Papier pointé (Denise Vella-Chemla, 24.10.2016)

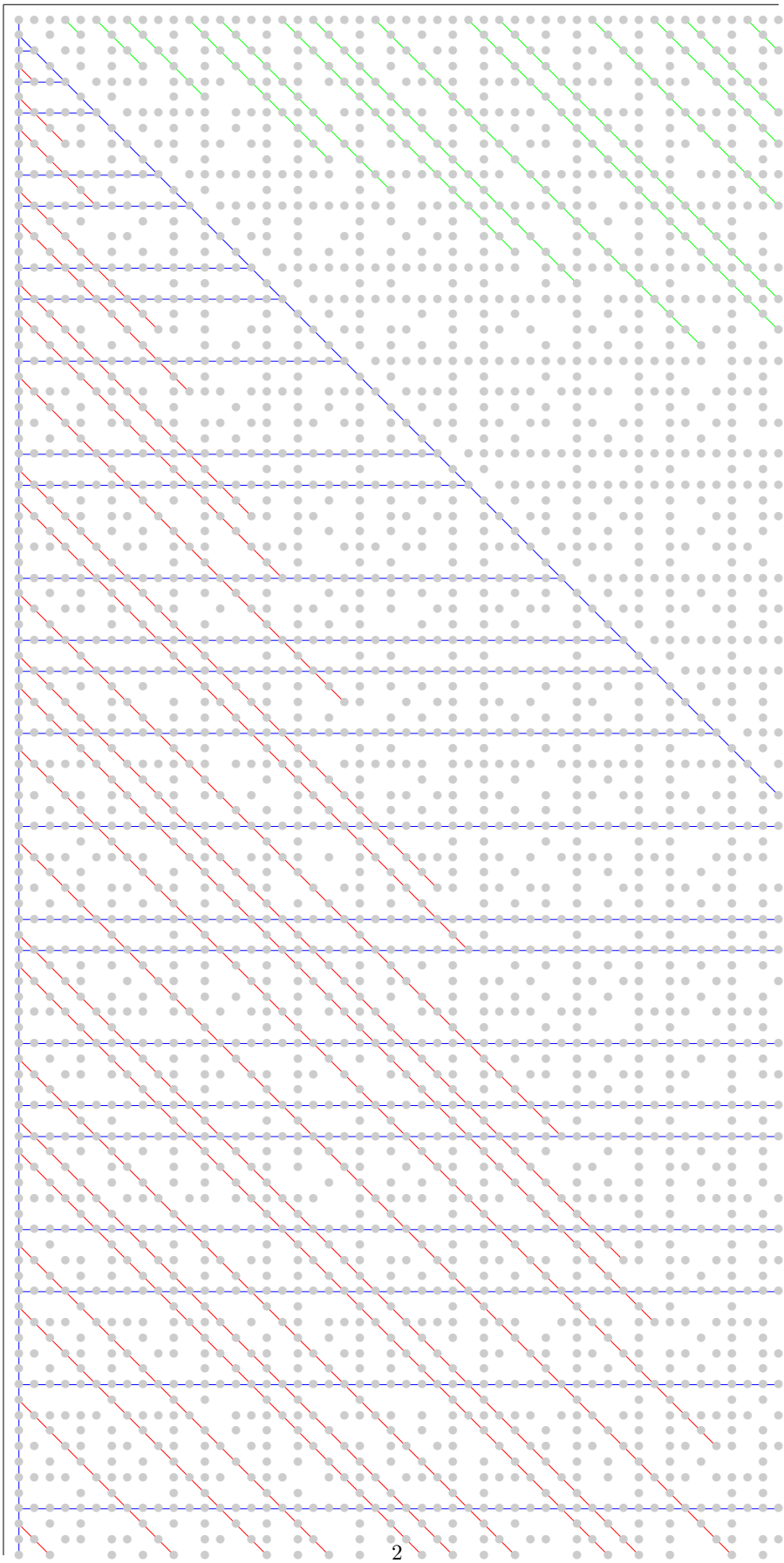
On continue d'étudier une représentation graphique de la relation x *premier* à y qui lie deux nombres, elle est noté par un point gris en (x, y) sur le graphique ci-après. Cette relation est symétrique.

On cherche sur ce graphique des polygones délimités par des lignes de points contigus (y compris contigus selon les diagonales).

On rappelle que la relation invariante qui caractérise la relation x *premier* à y (qu'on note $x \wedge y = 1$) est (cf l'algorithme de calcul du *pgcd* d'Euclide) :

$$\forall x, \forall a, 1 \leqslant x, 1 \leqslant a < x, x \wedge a = (x - a) \wedge a = (x + a) \wedge a.$$

On ajoute sur le graphique les trapèzes délimités par des lignes de points contigus correspondant aux nombres premiers. On ajoute également les diagonales de points contigus correspondant aux nombres premiers qui découlent de la relation invariante ci-dessus. La relation étant symétrique, on peut se concentrer sur la partie triangulaire inférieure gauche du graphique.



Une formule récurrente pour l'indicateur d'Euler trouvée sur la toile (6.11.2016)

Dans la séquence $A000010$ de l'On-line Encyclopedia Integer Sequences de N. J. A. Sloane (https://oeis.org/A000010), on trouve, fournie par Jon Perry le 2.3.4 la formule récurrente suivante pour l'indicateur d'Euler :

$$\varphi(n) = \frac{n(n+1)}{2} - \sum_{i=1}^{n-1} \varphi(i) \left\lfloor \frac{n}{i} \right\rfloor$$

Effectivement, pour 28 (avec $\frac{1}{2}.28.29 = 406$) par exemple, on a les valeurs suivantes :

i	$\varphi(i)$	$\left\lfloor \frac{28}{i} \right\rfloor$	$\varphi(i)\left\lfloor \frac{n}{i} \right\rfloor$
1	1	28	28
2	1	14	14
3	2	9	18
4	2	7	14
5	4	5	20
6	2	4	8
7	6	4	24
8	4	3	12
9	6	3	18
10	4	2	8
11	10	2	20
12	4	2	8
13	12	2	24
14	6	2	12
15	8	1	8
16	8	1	8
17	16	1	16
18	6	1	6
19	18	1	18
20	8	1	8
21	12	1	12
22	10	1	10
23	22	1	22
24	8	1	8
25	20	1	20
26	12	1	12
27	18	1	18
			$somme = 394$
28	12		

$406 - 394 = 12$ qui est bien la valeur de $\varphi(28)$.

Puisque $\varphi(p) = p - 1$ si p est premier, on doit avoir pour les nombres premiers

$$\sum_{i=1}^{n-1} \varphi(i) \left\lfloor \frac{n}{i} \right\rfloor = \frac{1}{2}(n^2 - n + 2).$$

Suites arythmiques (Denise Vella-Chemla, 2.1.2017)

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

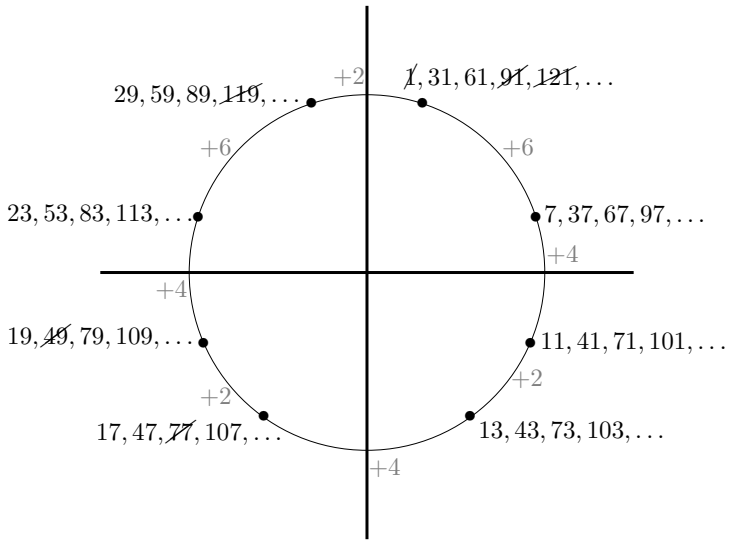
Gauss, dans les Recherches arithmétiques, distinguait les nombres de la forme $4k+1$ de ceux de la forme $4k+3$. On passe des uns aux autres en ajoutant systématiquement 2 et rien ne permet de se situer dans cette suite d'additions successives. D'autres, considérant la divisibilité par 2 et par 3, s'intéressent 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)

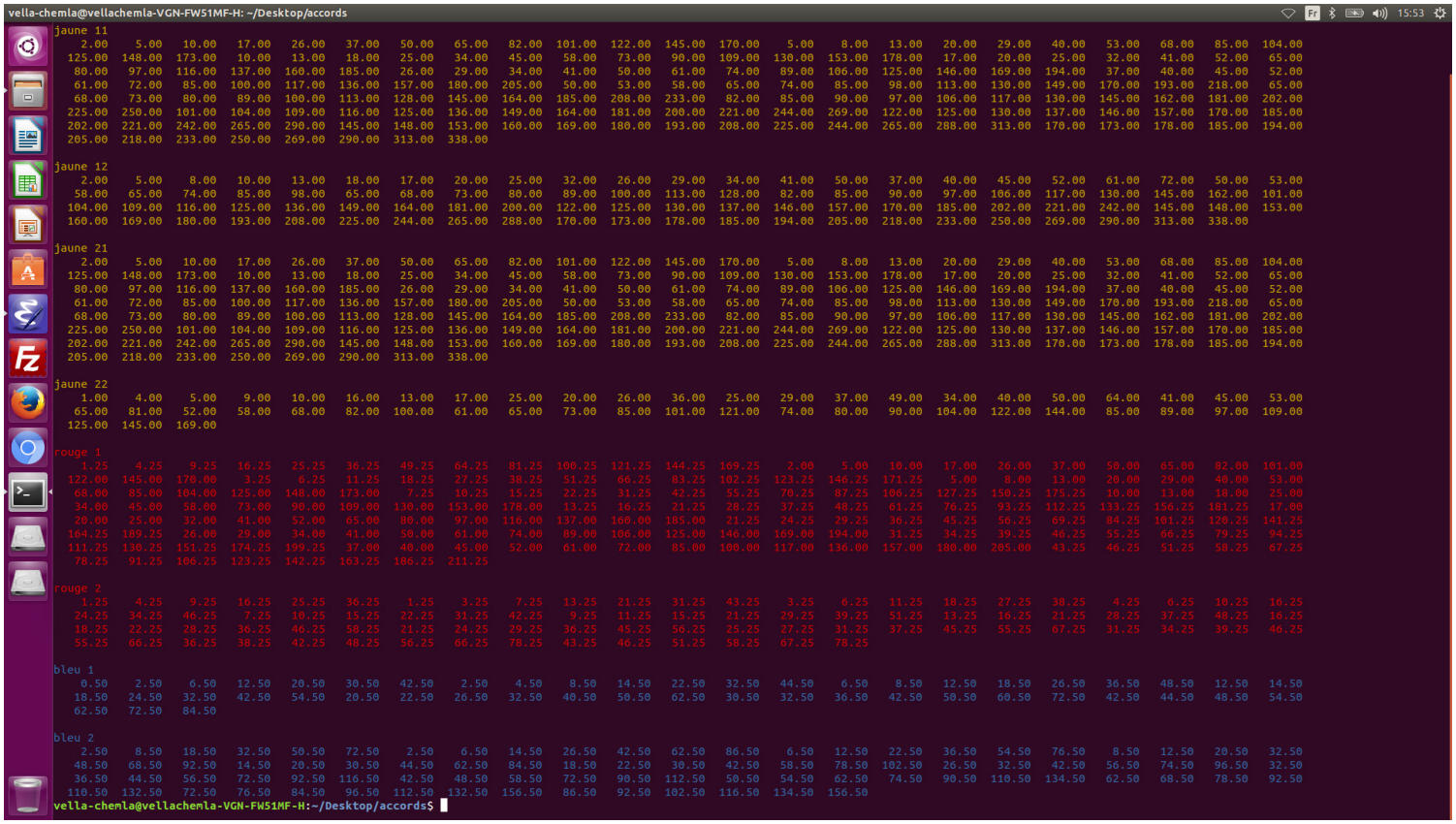
Premiers à 35 : 1,2,3,4,6,8,9,11,12,13,16,17,18,19,22,23,24,26,27,29,31,32,33,34,...,121
(+1,+1,+1,+2,+2,+1,+2,+1,+1,+3,+1,+1,+1,+3,+1,+1,+2,+1,+2,+2,+1,+1,+1,+2)

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


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" ;
}
```

Compositions (Denise Vella-Chemla, 7.1.2017)

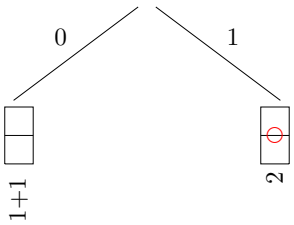
On cherche ce que les nombres premiers symétrisent.

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.

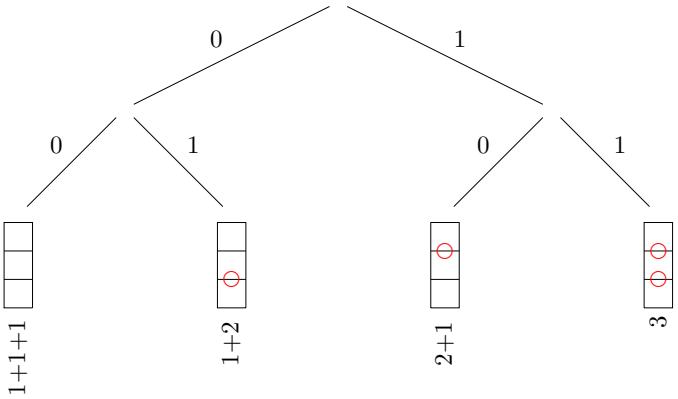
Cherchons d'autres formes de symétrie en étudiant les compositions des nombres. On prend comme référence l'article de wikipedia https://fr.wikipedia.org/wiki/Composition_(*combinatoire*).

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



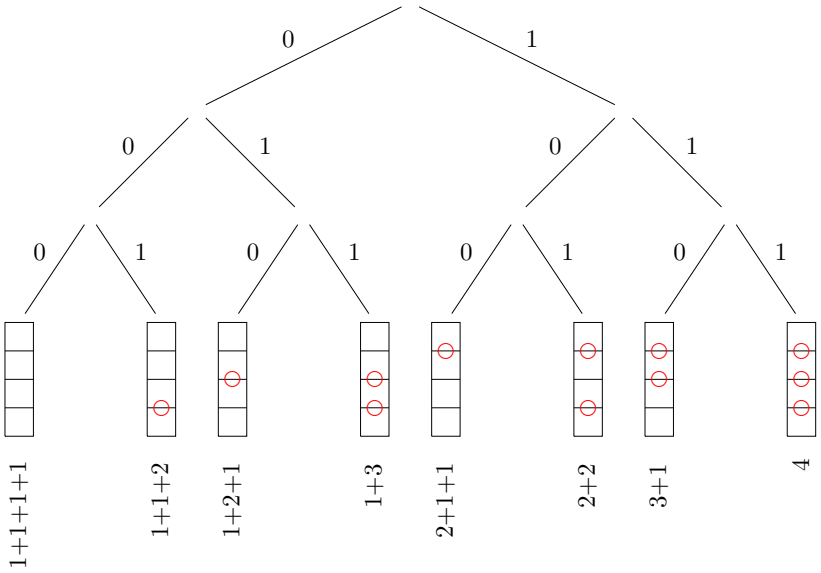
Arbre binaire des compositions de 3 (lire les dessins de haut en bas)



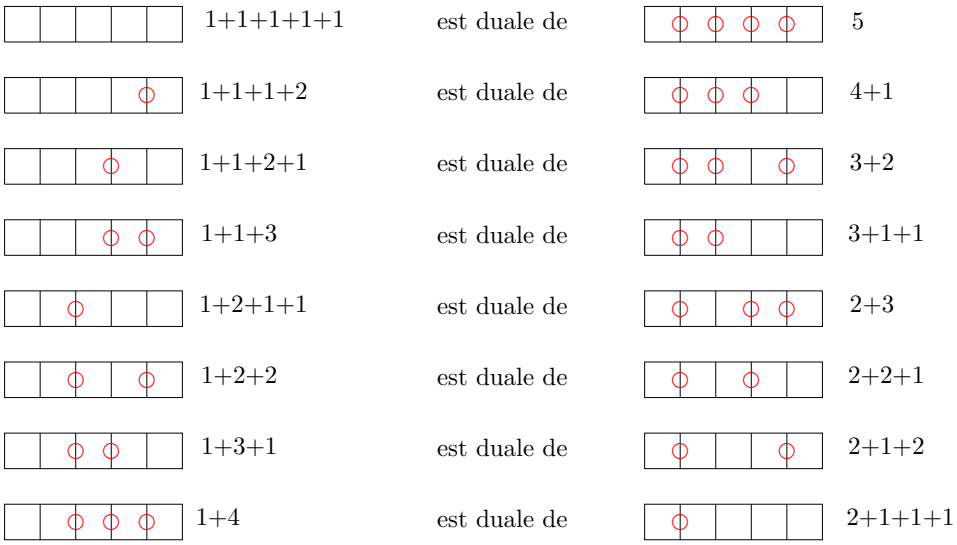
Pour obtenir une composition de $n+1$ à partir d'une composition de n, il suffit soit d'ajouter un sommant $1+$ au début de la composition de n, soit de remplacer le premier sommant de la composition de n par son successeur, en obtenant à partir de la composition $n = s_0 + A$ la composition $n+1 = (1+s_0)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

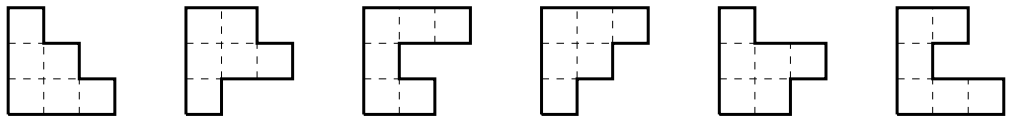


Un nombre composé est notamment caractérisé par le fait que l'une de ses compositions au moins, différente de la composition triviale composée uniquement de 1 de la forme 1+1+...+1, est telle que, quelle que soit la permutation qu'on pourrait effectuer entre 2 de ses sommants, cette composition reste 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.

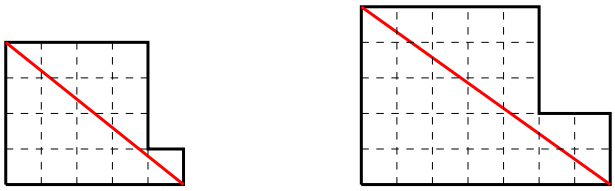
[1] On ne sait pas encore si cette définition présente une utilité.

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)

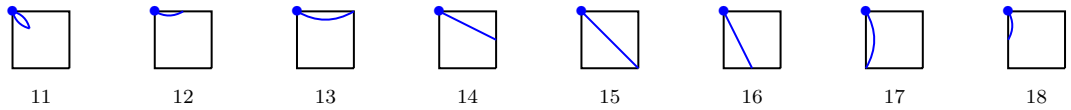
Annexe 2 : Valeurs des majorants des périmètres minima de surface d'aire n pour n impair inférieur à 100

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 (-)

Traverser un carré (Denise Vella-Chemla, 21.1.2017)

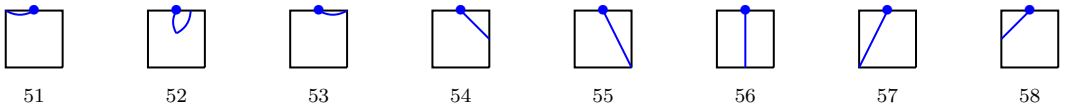
On étudie les différentes possibilités pour les points d'hyperboles d'équations de la forme $xy = n$ de traverser une maille-unité du plan. Le carré a 4 sommets, 4 côtés. On voit quels sont les seuls cas conservés parmi les $64 = 8 \times 8$ cas possibles.

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.



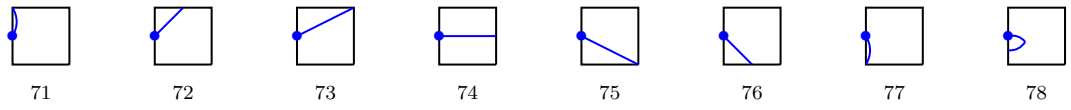
2) 3) et 4) Si l'hyperbole entre dans la maille par l'un des 3 autres coins, on se ramène au cas 1) ci-dessus.

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



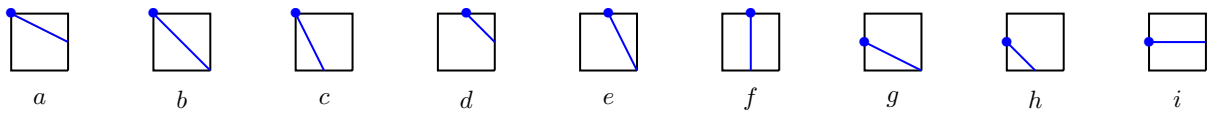
6) L'hyperbole ne peut entrer dans la maille par le côté bas.

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 $81 = 9 \times 9$.

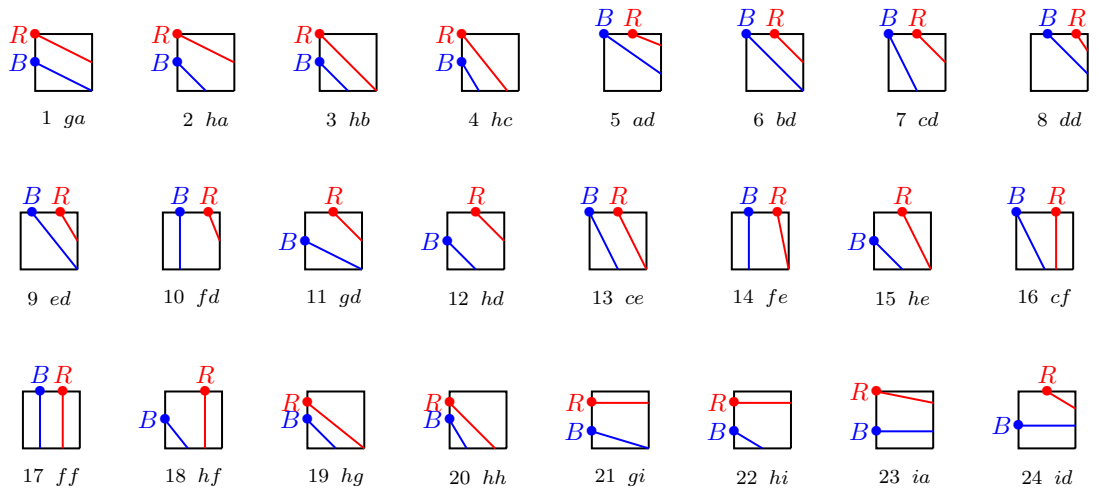
De visu en plaçant les configurations dans une maille, on arrive d'ores et déjà à réduire le nombre de cas possibles à 24 sur 81.

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.

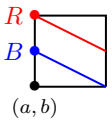
Un autre type d'impossibilités provient du fait que deux hyperboles associées à deux entiers successifs se croisent dans la maille, ce qui est impossible. C'est le cas pour les configurations : gc, ae, de, af, bf, df, ef, gf, gh, ai, bi, ci, ei, fi, ib, ic, ie, if, ig et ih.

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)).

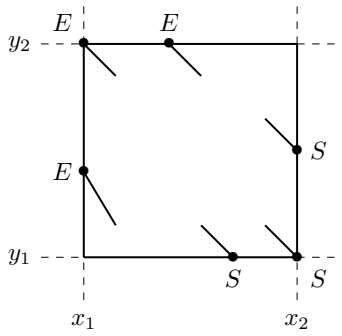


Les égalités ou inégalités sur les points d'entrée-sortie sont :

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

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 $f^{-1}(y_1) = x_2$.

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.

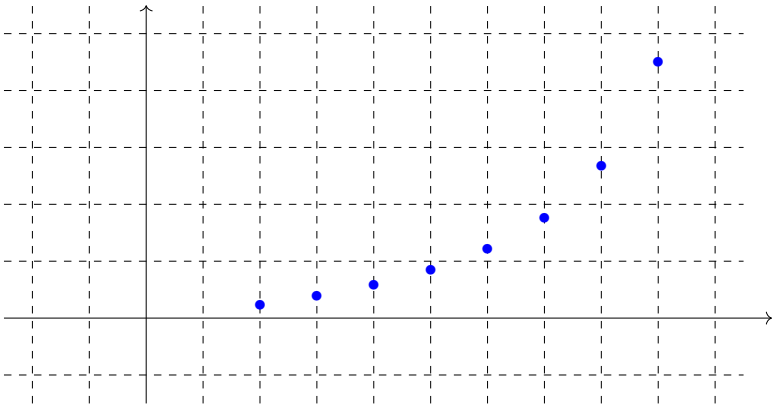
En mettant les nombres en regard à la manière dont Gauss l'a fait pour trouver, enfant, à la demande de son professeur, que la somme des 100 premiers entiers vaut 5050, on comprend aisément la raison d'une telle possibilité de définition.

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.

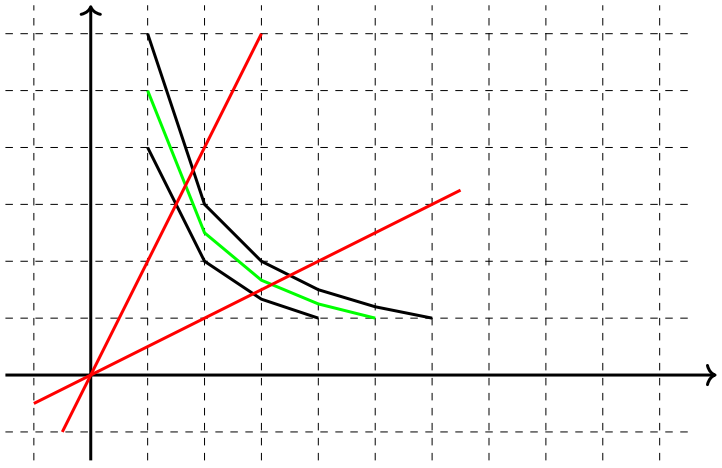
De même, 11, à qui est associé l'ensemble de fractions $\left\{\frac{9}{2}, \frac{8}{3}, \frac{7}{4}, \frac{6}{5}, \frac{5}{6}, \frac{4}{7}, \frac{3}{8}, \frac{2}{9}\right\}$, est premier.

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.

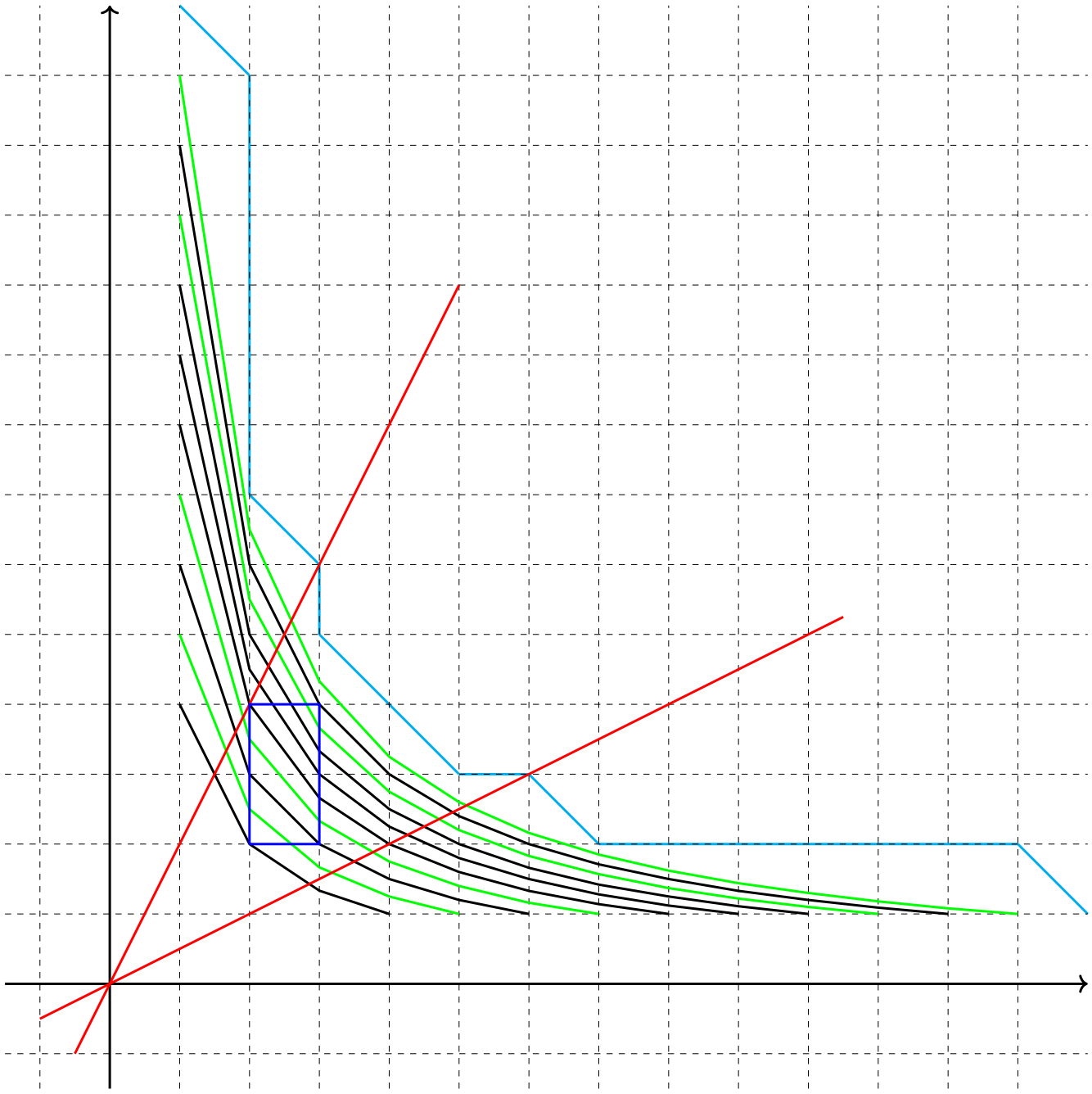
Si l'on représente chaque fraction de la forme $\frac{a}{b}$ par le point du plan de coordonnées $\left(a, \frac{a}{b}\right)$, voyons ci-dessous, les points d'ordonnées non entières, appartenant à une hyperbole, associés au nombre pemier 11.



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 $y = x/2$.

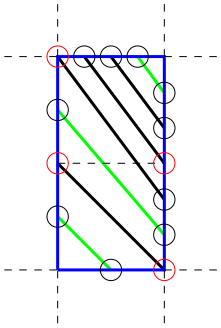


Courbe complétée jusqu'à $n = 13$ (5, 7, 11 et 13, premiers, en vert).



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).

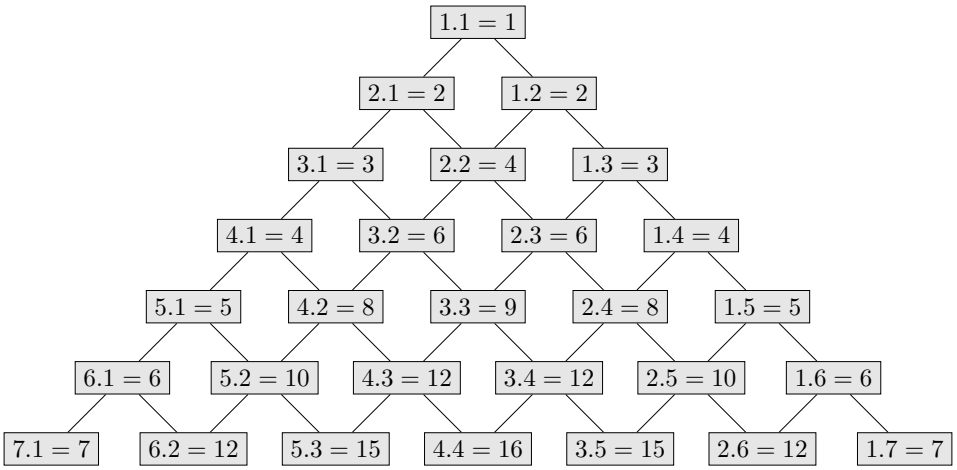
Les hyperboles successives n'ont aucun point commun. Cette méthode de comptage semble également fonctionner pour une zone avec points entiers intérieurs (ne serait-ce qu'un seul). Prenons la zone carrée de 2×2 entre les points bas-gauche $(3,5)$ et haut-droit $(5,7)$. 19 hyperboles (correspondant à $5\times 7-3\times 5-1$ 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.

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.