Conjecture des nombres premiers jumeaux

- On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.
- 3 et 5 sont des nombres premiers jumeaux.
  29 et 31 sont des nombres premiers jumeaux.
- *Énoncé :*

  L'ensemble des nombres premiers jumeaux est infini.
- On appelle *primorielle* d'un nombre premier p_i le produit de tous les nombres premiers inférieurs ou égaux à p_i.

$$\#p_i = \prod_{\substack{2 \leq p_k \leq p_i, \\ p_k \text{ premier}}}^{p_i} p_k$$

Représentation par les restes

- Représentons les premiers entiers naturels par leurs restes modulo les nombres premiers successifs.
  Pour passer du "mot" des restes d'un nombre au mot des restes de son successeur au sens de l'arithmétique de Peano, on ajoute à ce *"mot"* le mot n-uplet infini $(1, 1, 1, 1, \ldots)$ qui représente l'entier naturel 1.

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

Définitions

- Notons $\mathbb{P}$ l'ensemble des nombres premiers.

- On définit la bijection p de $\mathbb{N}^*$ dans $\mathbb{P}$ qui associe à tout i, un entier naturel non-nul, $p(i) = p_i$, le i-ème plus petit nombre premier de $\mathbb{P}$.

- Deux nombres premiers impairs p_j et p_k sont jumeaux si $k = j + 1$. L'entier $2n_k = p_j + 1$ sera appelé le *père des jumeaux* (en fait, le pair entre les jumeaux).

Définitions

- Une suite de k nombres premiers distincts est appelée une *base modulaire* d'ordre k.

- La suite $B_k = (p_1 = 2, p_2 = 3, ..., p_k)$ des k premiers nombres premiers est appelée une base modulaire fondamentale d'ordre k.

  Désormais, l'expression base modulaire désignera une telle base fondamentale.

- Un nombre n étant donné, sa projection dans B_k est la suite des restes r_j de la divison de n par les p_j $(j \leq k)$.

  r_j est appelé la j-ème *composante* de n dans B_k.

Propriétés

Propriété 1 :

- Un entier naturel a tous ses restes selon les nombres premiers intervenant dans sa décomposition en facteurs premiers qui sont nuls.

- En conséquence,

Propriété 2 :

En particulier, un nombre premier a comme seul reste nul son reste modulo lui-même.

Propriétés

Propriété 3 :

- Dans B_{j-1}, les k-èmes $(k < j)$ composantes de $2n_j$ (père des jumeaux p_j et p_{j+1}) sont différentes de 1 et de $p_k - 1$.

- Preuve :

Supposons que l'une des k-èmes $(k < j)$ composantes de $2n_j$ soit égale à 1.
Alors $2n_j = \prod_1^{j-1} p_r^{\alpha_r} = c(k)p_k^{\alpha_k} + 1$ de sorte que $2n_j - 1 = p_j = c(k)p_k^{\alpha_k}$: par suite, quel que soit

k, la k-ème composante de p_j dans B_{j-1} est nulle, ce qui est en contradiction avec la propriété 2

pour le nombre premier p_j.

De façon similaire, supposons que l'une des k-èmes $(k < j)$ composantes de $2n_j$ soit égale à $p_k - 1$, alors $2n_j = \prod_1^{j-1} p_r^{\alpha_r} = c(k)p_k^{\alpha_k} - 1$ de sorte que $2n_j + 1 = p_{j+1} = c(k)p_k^{\alpha_k}$: par suite, quel que soit k, la k-ème composante de p_{j+1} dans B_{j-1} est nulle, ce qui est en contradiction avec la propriété 2 pour le nombre premier p_{j+1}.

Propriétés

Propriété 4 :

- Dans B_{j-1}, les k-èmes ($k < j$) composantes de n_j (la moitié du père $2n_j$ de 2 jumeaux p_j et p_{j+1}) sont différentes de $\frac{p_k-1}{2}$ et de $\frac{p_k+1}{2}$.

- Cela découle du fait que :

$$\begin{aligned} & 2n_j \not\equiv p_k - 1 \,(mod\ p_k) \\ \Longleftrightarrow \quad & n_j \not\equiv \tfrac{p_k-1}{2} \,(mod\ p_k) \end{aligned}$$

et d'autre part :

$$\begin{aligned} & 2n_j \not\equiv 1 \,(mod\ p_k) \\ \Longleftrightarrow \quad & 2n_j \not\equiv p_k + 1 \,(mod\ p_k) \\ \Longleftrightarrow \quad & n_j \not\equiv \tfrac{p_k+1}{2} \,(mod\ p_k) \end{aligned}$$

Un lemme de Gauss

Lemme :

- *(127) : Dans la progression* $1, 2, 3, 4, \ldots, n$*, il ne peut y avoir plus de termes divisibles par un nombre quelconque h, que dans la progression* $a, a+1, a+2, \ldots, a+n-1$*, qui a le même nombre de termes.*

- En effet, on voit sans peine que si n est divisible par h, il y a dans chaque progression $\frac{n}{h}$ termes divisibles par h ; sinon soit $n = he + f$, f étant $< h$; il y aura dans la première série e termes, et dans la seconde e ou $e+1$ termes divisibles par h.

Un lemme de Gauss

- Il suit de là, comme corollaire, que $\frac{a(a+1)(a+2)(a+3)\ldots(a+n-1)}{1 \quad 2 \quad 3 \quad\quad n}$ est toujours un nombre entier : proposition connue par la théorie des nombres figurés, mais qui, si je ne me trompe, n'a encore été démontrée directement par personne.

- Enfin on aurait pu présenter plus généralement ce lemme comme il suit :

  Dans la progression $a, a+1, a+2, \ldots, a+n-1$, il y a au moins autant de termes congrus suivant le module h à un nombre donné quelconque, qu'il y a de termes divisibles par h dans la progression $1, 2, 3, \ldots, n$.

A la recherche d'un père de jumeaux

- On souhaite démontrer qu'il y a toujours entre deux primorielles consécutives un père de jumeaux.
- Si l'on considère tous les nombres pairs entre deux primorielles consécutives $\#p_i$ et $\#p_{i+1}$, ces nombres sont les doubles de nombres consécutifs compris quant à eux entre deux moitiés de primorielles.
- Il faudrait être capable de démontrer que parmi eux, l'un forcément est la moitié d'un père de jumeaux.
- Par exemple, tous les pairs compris entre $30 = 2.3.5$ et $210 = 2.3.5.7$ sont les doubles de nombres consécutifs compris entre 15 et 105.

A la recherche d'un père de jumeaux : un exemple

- Dans le tableau suivant, on consigne dans la première ligne les restes de 51 selon tous les modules inférieurs à 105 (modules en tête des colonnes), ainsi que dans les deuxième et troisième lignes les restes interdits $\frac{p_k-1}{2}$ et $\frac{p_k+1}{2}$.

p_k	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
$51 \ mod \ p_k$	1	0	1	2	7	12	0	13	5	22	20	14	10	8	4	51
$\frac{p_k-1}{2}$		1	2	3	5	6	8	9	11	14	15	18	20	21	23	...
$\frac{p_k+1}{2}$		2	3	4	6	7	9	10	12	15	16	19	21	22	24	...

- 51 vérifie les conditions requises pour que son double soit un père de jumeaux.
- Effectivement, $102 = 2 \times 51$ est entre les deux nombres premiers 101 et 103.

Utilisation du lemme de Gauss pour garantir l'existence d'un père de jumeaux entre deux primorielles

- Ce que nous dit le lemme de Gauss, c'est que la quantité de nombres compris entre deux valeurs a et b et qui ne sont congrus ni à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ selon tout module p_k inférieur à un nombre donné c est au moins égale à la quantité de nombres compris entre 1 et $b-a+1$ qui ne sont congrus ni à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ selon tout module p_k inférieur à c.

Quelques résultats

- Le tableau suivant présente quelques résultats pour les premières primorielles.
  L'expression *"satisf"* est utilisé pour représenter la quantité de nombres qui ne sont ni congrus à $\frac{p_k-1}{2}$ ni à $\frac{p_k+1}{2}$ pour tout p_k inférieur à $\frac{\#p_{i+1}}{2}$.

$\frac{\#p_i}{2}$	$\frac{\#p_{i+1}}{2}$	*Diff*	*satisf sur* $[1, Diff]$	*satisf sur* $[\frac{\#p_i}{2}, \frac{\#p_{i+1}}{2}]$
3	15	12	1	2
15	105	90	3	6
105	1 155	1 050	23	28
1 155	15 015	13 860	169	196

Vers une démonstration de la conjecture des nombres premiers jumeaux

- Le fait de se ramener ainsi à des ensembles de nombres consécutifs à partir de 1 devrait permettre de montrer qu'au fur et à mesure de l'augmentation des primorielles, on est assuré de toujours trouver un nombre entre 2 moitiés de primorielles qui ne soit jamais congru à $\frac{p_k-1}{2}$ ou à $\frac{p_k+1}{2}$ pour tout p_k inférieur à une moitié de primorielle donnée $\frac{\#p_{i+1}}{2}$.

- Le double de ce nombre n'est quant à lui ni congru à 1 ni congru à $p_k - 1$ selon tout module p_k inférieur à $\frac{\#p_{i+1}}{2}$, ce qui assure qu'il est un père de jumeaux.

Vers une démonstration de la conjecture des nombres premiers jumeaux

- Pour être assuré de toujours trouver une moitié de père de jumeaux entre 2 moitiés de primorielles, on minore la quantité de nombres non-congrus à $\frac{p_k-1}{2}$ ou à $\frac{p_k+1}{2}$ pour tout p_k inférieur à la moitié de primorielle $\frac{\#p_{i+1}}{2}$ par une quantité de nombres à calculer sur l'intervalle de nombres $[1, \Delta]$, où $\Delta = \frac{\#p_{i+1} - \#p_i}{2}$.

- En effet, la quantité de nombres compris entre 1 et $\frac{\#p_{i+1} - \#p_i}{2}$ et qui sont non-congrus à $\frac{p_k-1}{2}$ selon tout module premier p_k inférieur à $\frac{\#p_{i+1}}{2}$ est minorable par la quantité de nombres premiers compris entre 1 et $\frac{\#p_{i+1} - \#p_i}{2}$ selon le lemme de Gauss, la congruence à 0 advenant avec autant d'occurrence que la congruence à $\frac{p_k-1}{2}$ $(mod\ p_k)$.

Vers une démonstration de la conjecture des nombres premiers jumeaux

- On doit noter également que si $x \equiv \frac{p_k-1}{2}$ $(mod\ p_k)$ alors $x+1 \equiv \frac{p_k+1}{2}$ $(mod\ p_k)$ (i.e. les nombres congrus à $\frac{p_k+1}{2}$ sont les successeurs au sens de Peano des nombres congrus à $\frac{p_k-1}{2}$).

- Le nombre de moitiés de père de jumeaux augmente strictement lorsqu'on passe de l'intervalle $[1, \frac{\#p_{i+1}-\#p_i}{2}]$ à l'intervalle $[1, \frac{\#p_{i+2}-\#p_{i+1}}{2}]$.

- Cela devrait permettre d'assurer qu'un père de jumeaux existe toujours entre deux primorielles consécutives.

Un exemple d'application de l'algorithme de recherche d'une moitié de père de jumeaux

- Les restes interdits sont entourés dans chaque colonne.

p_k	3	5	7	11	13	
3	0	3	3	3	3	*
4	1	4	4	4	4	*
5	2	0	5	5	5	*
6	0	1	6	6	6	*
7	1	2	0	7	7	*
8	2	3	1	8	8	*
9	0	4	2	9	9	
10	1	0	3	10	10	*
11	2	1	4	0	11	*
12	0	2	5	1	12	*
13	1	3	6	2	0	*
14	2	4	0	3	1	*
15	0	0	1	4	2	
reste interdit $(\frac{p_k-1}{2})$	1	2	3	5	6	
reste interdit $(\frac{p_k+1}{2})$	2	3	4	6	7	

Un exemple d'application de l'algorithme de recherche d'une moitié de père de jumeaux

-

p_k	3	5	7	11	13	
1	1	1	1	1	1	*
2	2	2	2	2	2	*
3	0	3	3	3	3	*
4	1	4	4	4	4	*
5	2	0	5	5	5	*
6	0	1	6	6	6	*
7	1	2	0	7	7	*
8	2	3	1	8	8	*
9	0	4	2	9	9	
10	1	0	3	10	10	*
11	2	1	4	0	11	*
12	0	2	5	1	12	*
reste interdit $(\frac{p_k-1}{2})$	1	2	3	5	6	
reste interdit $(\frac{p_k+1}{2})$	2	3	4	6	7	

Un exemple d'application de l'algorithme de recherche d'une moitié de père de jumeaux

- Constat : le nombre de solutions est plus élevé sur l'intervalle dont les bornes sont plus grandes.

- Les lignes concernant les nombres de l'intervalle $[3, 12]$ sont communes aux deux tableaux. Le fait qu'il y ait plus de nombres qui respectent les contraintes imposées sur l'intervalle $[13, 15]$ que sur l'intervalle $[1, 2]$ puisqu'il contient un nombre de plus garantit que l'on trouvera systématiquement des moitiés de pères de jumeaux sur nos intervalles successifs.

Programmation de la recherche des moitiés de pères de jumeaux sur quelques intervalles

-

$\#p_i$	$\#p_{i+1}$	*moitie du pere*	*pere*	*module max*	*nombres*
$\#3$	$\#5$	$[3, 15]$	$[6, 30]$	15	$9, 15$
$\#5$	$\#7$	$[15, 105]$	$[30, 210]$	105	$54, 69, 75, 90, 96, 99$
$\#7$	$\#11$	$[105, 1155]$	$[210, 2310]$	1155	$615, 639, 645, 651, 660, 714, 726, 741, 744, 804, 810, 834, 849, 861, 894, 936, 939, 966, 975, 999, 1014, 1041, 1044, 1056, 1065, 1071, 1119, 1134, 1155$

Conclusion

- On a utilisé un *Système de NUmération par les Restes dans les Parties Finies de* $\mathbb{N}$.

- On se situe dans le cadre d'une *théorie lexicale des nombres*, selon laquelle *"les nombres sont des mots"*.