Infinitude de l'ensemble des nombres premiers de la forme $6n+1$, puis de l'ensemble des nombres premiers jumeaux qui en découle presque (Denise Chemla, 5 juin 2012)

1 Rappels

Rappelons le contenu du Triangle de Pascal qui contient les coefficients binomiaux.

								1									→	1
							1		1								→	2
						1		2		1							→	4
					1		3		3		1						→	8
				1		4		6		4		1					→	16
			1		5		10		10		5		1				→	32
		1		6		15		20		15		6		1			→	64
	1		7		21		35		35		21		7		1		→	128
1		8		28		56		70		56		28		8		1	→	256

La somme de tous les coefficients de la $n^{ième}$ ligne vaut : 2^n.

$$\sum_{p=1}^{n} C_n^p = 2^n$$

Rappelons que le nombre de façons d'avoir au moins un zéro parmi 4 nombres est égal à $\sum_{p=1}^{n} C_n^p - 1$:

0	−	−	−	1
−	0	−	−	2
−	−	0	−	3
−	−	−	0	4
0	0	−	−	1
0	−	0	−	2
0	−	−	0	3
−	0	0	−	4
−	0	−	0	5
−	−	0	0	6
0	0	0	−	1
0	0	−	0	2
0	−	0	0	3
−	0	0	0	4
0	0	0	0	1

Rappelons enfin quelles sont les écritures par les restes modulo les nombres premiers successifs des premiers entiers. On ajoute à chaque "mot" de restes le mot n-uplet $(1, 1, 1, 1, \ldots)$.

mod	2	3	5	7	11	13	...
1	1	1	1	1	1	1	...
2	0	2	2	2	2	2	...
3	1	0	3	3	3	3	...
4	0	1	4	4	4	4	...
5	1	2	0	5	5	5	...
6	0	0	1	6	6	6	...
7	1	1	2	0	7	7	...
8	0	2	3	1	8	8	...
9	1	0	4	2	9	9	...
10	0	1	0	3	10	10	...
11	1	2	1	4	0	11	...
12	0	0	2	5	1	12	...
13	1	1	3	6	2	0	...

2 Infinitude de l'ensemble des nombres premiers de la forme $6n + 1$

On démontre par récurrence la propriété $P(p_i)$ qui est qu'il y a toujours un nombre premier de la forme $6n+1$ supérieur à $\#p_{i-1}$ et inférieur à $\#p_i$. On rappelle que la primorielle $\#p_i$ est le produit des nombres premiers compris entre 2 et p_i.

1) initialisation de la récurrence : la propriété est vraie pour $p_3 = 5$. Il y a un nombre premier 7 de la forme $6n + 1$ compris entre $\#3 = 2.3 = 6$ et $\#5 = 2.3.5 = 30$.

2) Passage de $P(p_i)$ à $P(p_{i+1})$: la propriété est vraie pour p_i signifie qu'il y a un nombre premier compris entre $\#p_{i-1}$ et $\#p_i$. Montrons qu'il y a un nombre premier de plus de la forme $6n + 1$ compris entre $\#p_i$ et $\#p_{i+1}$. De $\#p_i$ à $\#p_{i+1}$, il y a $\#p_i(p_{i+1} - 1)$ nombres différents. Mais parmi ces nombres, seuls $2^{i+1} - 1$ contiennent au moins un zéro dans leur écriture par les restes. Puisque $\#p_i(p_{i+1} - 1)$ est très supérieur à $2^{i+1} - 1$ (voir l'inégalité ci-après pour $p_i = 7$), les nombres restant ayant une écriture par les restes qui ne contient aucun zéro sont premiers. Seuls $\frac{1}{6}$ des nombres en question sont de la forme $6n - 1$. Ils ne peuvent tous être de la forme $6n - 1$. L'un des nombres qui n'est pas de la forme $6n - 1$ est de la forme $6n + 1$. Il n'avait pas été trouvé jusque-là car les nombres compris entre $\#p_i$ et $\#p_{i+1}$ sont tous différents de ceux déjà rencontrés jusqu'à $\#p_i$.

Pour $p_i = 7$, on a l'inégalité suivante :

$$\#p_i(p_{i+1} - 1) \gg 2^{i+1} - 1$$
$$2.3.5.7.(11 - 1) \gg 2.2.2.2.2 - 1$$

3 Infinitude de l'ensemble des nombres premiers jumeaux

Comme on peut le voir puis le comprendre dans le tableau qui fournit les écritures par les restes des premiers entiers, il y a autant de couples de nombres premiers jumeaux que de nombres pairs "coincés" entre deux nombres premiers jumeaux. Observons l'écriture par les restes de tels nombres. Un nombre pair $p_i + 1$ qui est entre les nombres premiers jumeaux p_i et $p_i + 2$ doit être :

- congru à 1 (mod p_i) ;
- non congru à $p_k - 1$ et non congru à 1 pour tout $k < i$.

Pour démontrer par récurrence qu'il existe toujours un tel nombre pair différent de ceux précédemment rencontrés entre $\#p_{i-1}$ et $\#p_i$, il faut démontrer que le nombre de nombres pairs "coincés" entre deux nombres premiers jumeaux (que l'on appellera $NbPairsMilieuxJumeaux$ est toujours supérieur strictement à 1. La "nouveauté" des nombres compris entre $\#p_i$ et $\#p_{i+1}$ garantit qu'on a trouvé un nouveau nombre pair entre deux nouveaux nombres premiers jumeaux et ainsi que l'ensemble des nombres premiers jumeaux est infini.

$$NbPairsMilieuxJumeaux = \frac{1}{p_i}\left[\#p_i(p_{i+1}-1) - \left(\sum_{k=1}^{i-1} 2^k.C_{i-1}^k - 1\right)\right]$$

La multiplication par $\frac{1}{p_i}$ est nécessitée pour calculer le nombre de mots qui contiennent un 1 en dernière lettre (i.e. $(mod\ p_i)$).

L'expression $\#p_i(p_{i+1}-1)$ compte le nombre de mots entre $\#p_i$ et $\#p_{i+1}$.

On soustrait de ce nombre de mots total la valeur de $\sum_{k=1}^{i-1} 2^k.C_{i-1}^k - 1$ qui correspond au nombre de mots contenant au moins un $p_k - 1$ ou un 1 comme lettre parmi les $i-1$ premières lettres de leur écriture par les restes (i.e. $(mod\ p_k)$, pour tout p_k inférieur strictement à i). Le reste 1 correspond au fait que le nombre p_i précédant le nombre pair p_i+1 n'est pas premier tandis que le reste $p_k - 1$ correspond au fait que le nombre p_i+2 suivant le nombre pair p_i+1 n'est pas premier). Le nombre de mots à éliminer étant égal à 3^{i-1} est comme dans la section précédente bien inférieur au nombre de mots total et on est ainsi assuré de toujours trouver entre deux primorielles sucessives un nombre pair "coincé" entre deux nombres premiers.

4 Existence d'un décomposant de Goldbach pour tout nombre pair supérieur ou égal à 6

La Conjecture de Goldbach (7 juin 1742) stipule que tout nombre pair supérieur ou égal à 6 est la somme de deux nombres premiers impairs. Si on note $\mathbb{P}^*$ l'ensemble des nombres premiers impairs :

$$\mathbb{P}^* = \{p_1 = 3, p_2 = 5, p_3 = 7, p_4 = 11, \ldots\},$$

on peut écrire la Conjecture de Goldbach ainsi :

$$\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*,\ p \leq n/2,\ \exists\, q \in \mathbb{P}^*,\ q \geq n/2,\ \ n = p+q.$$

Dans la suite, n étant donné, on note : $\mathbb{P}^*(n) = \{x \in \mathbb{P}^* / x \leq n\}$,

Un nombre premier qui n'est jamais congru à n, un nombre pair supérieur ou égal à 6 donné, selon aucun module de $\mathbb{P}^*(n)$, est un décomposant de Goldbach de n.
En effet,

$$\begin{aligned}\forall\, n \in 2\mathbb{N}\backslash\{0,2,4\},\ \exists\, p \in \mathbb{P}^*(n),\ \forall\, m \in \mathbb{P}^*(n), \quad & p \not\equiv n\ (mod\ m) \\ \Leftrightarrow\ & n - p \not\equiv 0\ (mod\ m) \\ \Leftrightarrow\ & n - p\ premier.\end{aligned}$$

On va chercher pour n un nombre pair compris entre deux primorielles successives $\#p_i$ et $\#p_{i+1}$ un nombre premier inférieur à $\#p_i$ non congru à n selon tout module premier inférieur à p_i. On va montrer que parmi les nombres inférieurs à $\#p_i$, il y en a au moins un qui n'est congru ni à 0 (donc il est premier) ni à n (donc il ne partage aucun de ses restes avec n). On a vu dans la section précédente que 3^i nombres inférieurs à $\#p_i$ ont au moins l'un de leurs restes qui est nul ou bien égal à une valeur donnée (en l'occurrence le reste de n selon le module considéré). Mais 3^i est toujours très inférieur à $\#p_i$ donc il existe toujours un nombre inférieur à $\#p_i$ qui n'est congru à 0 selon aucun module et qui n'est jamais congru à n selon aucun module inférieur à p_i. Ce nombre est un décomposant de Goldbach de n.

$$Si \quad \#p_i < n < \#p_{i+1} \quad alors \quad NbDecompGoldbach(n) > \#p_i - 3^i > 1.$$