Infinité de l'ensemble des nombres premiers jumeaux

Denise Vella-Chemla

15/6/2012

1 Introduction

Dans cette note, on essaie de démontrer la conjecture des nombres premiers jumeaux en utilisant une approche, que l'on pourrait qualifier de lexicale, qui utilise des mots de représentation des entiers par leurs restes modulaires selon les nombres premiers successifs.

2 Énoncé

On appelle *nombres premiers jumeaux* deux nombres premiers dont la différence est 2.
Exemples :

  3 et 5 sont des nombres premiers jumeaux.
  29 et 31 sont des nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux stipule que l'ensemble des nombres premiers jumeaux est infini.

3 Représentation par les restes

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

*selon l'arithmétique de Peano

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	...

Observons quelques représentations par les restes qui sont pertinentes par rapport à la conjecture des nombres premiers jumeaux.

6, le nombre pair juste entre les deux nombres premiers jumeaux 5 et 7 a pour représentation 0 0 1 6 6 6 .... Il a un 1 en troisième position parce que 5 a un 0 à cette position (un nombre premier est congru à 0 modulo lui-même, jamais congru à 0 modulo un nombre premier qui lui est strictement inférieur et congru à lui-même modulo tout nombre premier qui lui est strictement supérieur). 6 a un 6 en quatrième position parce que 7 a un 0 à cette position-là (le reste de 7 modulo lui-même). Les deux premières lettres du mot de représentation du nombre 6 ne sont ni des 1 ni des $p_k - 1$ (ni 1 ni 1 dans la colonne correspondant au nombre premier 2, ni 1 ni 2 dans la colonne correspondant au nombre premier 3) car si tel était le cas, l'un ou l'autre de 5 ou 7 serait composé.

18, entre 17 et 19, a pour représentation 0 0 3 4 7 5 1 18 ... : il n'a ni 1 ni $p_k - 1$ parmi ses six premières lettres, correspondant à ses restes modulo $2, 3, 5, 7, 11$ et 13. Le mot de 18 a un 1 en septième position (correspondant à son reste modulo 17 : $18 = 17 + 1$) et 18 a un reste de 18 en huitième position (correspondant à son reste modulo $19 = 18 + 1$).

Un nombre pair $p_i + 1$ juste entre deux nombres premiers jumeaux p_i et $p_i + 2$ a son écriture qui est caractérisée par le fait qu'elle ne contient ni 1 ni $p_k - 1$ pour tout module p_k strictement inférieur à p_i.

4 Démonstration par récurrence

On va ci-après essayer de construire un nombre pair juste entre deux nombres premiers jumeaux qui est entre deux primorielles successives. Ainsi, on aura autant de couples de nombres premiers jumeaux que de nombres premiers, i.e. une infinité de couples de nombres premiers jumeaux.

1) initialisation de la récurrence : entre 2.3=6 et 2.3.5=30, il existe un nombre pair juste entre deux nombres premiers, par exemple le nombre pair 18, entre 17 et 19.

2) passage d'une primorielle à la suivante : supposons qu'on a trouvé un nombre pair *pairPrécédent* juste entre deux jumeaux entre les primorielles successives $\#p_{i-1}$ et $\#p_i$. Montrons que l'on peut trouver un nombre pair juste entre deux nombres premiers jumeaux entre les primorielles successives $\#p_i$ et $\#p_{i+1}$.

Pour cela, analysons quelques cas :
$\#p_i + 2$ ne peut convenir puisqu'il est congru à $p_k - 1$ pour $p_k = 3$.
De même, tout nombre de la forme $\#p_i + 6m + 2$ ne peut convenir pour la même raison.
$\#p_i + 4$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 3$.
De même, tout nombre de la forme $\#p_i + 6n + 4$ ne peut convenir pour la même raison.
Etudions quelques nombres de la forme $\#p_i + 6s$.
$\#p_i + 6$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 5$.
$\#p_i + 12$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 11$.
$\#p_i + 18$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 17$.
$\#p_i + 24$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 23$.
$\#p_i + 30$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 29$.
$\#p_i + 36$ ne peut convenir puisqu'il est congru à $p_k - 1$ pour $p_k = 37$.
$\#p_i + 42$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 41$.
$\#p_i + 48$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 47$.
$\#p_i + 54$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 53$.
$\#p_i + 60$ ne peut convenir puisqu'il est congru à 1 pour $p_k = 59$.
$\#p_i + 66$ ne peut convenir puisqu'il est congru à $p_k - 1$ pour $p_k = 67$.

Intéressons-nous maintenant au nombre pair $\#p_i + pairPrécédent$ où $pairPrécédent$ est le nombre pair que l'on a trouvé comme étant juste entre deux nombres premiers tout en étant compris entre $\#p_{i-1}$ et $\#p_i$†.

On déduit de l'hypothèse de récurrence que $\#p_i + pairPrécédent$ ne peut être congru à 1 ou $p_k - 1$ pour tout p_k inférieur ou égal à $pairPrécédent - 1$ puisque l'hypothèse de récurrence fait que $pairPrécédent$ vérifie ces conditions et que $\#p_i$ est congru à 0 selon tous les modules en question‡ : Faux, $\#p_i$ est congru à 0 seulement selon les modules inférieurs ou égaux à p_i.

On sait que $pairPrécédent$ est juste entre deux jumeaux que l'on appelle j_{inf} et j_{sup}. $pairPrécédent$ est congru à 1 $(mod\ j_{inf})$ et à $pairPrécédent\ (mod\ p_k)$, pour tout p_k supérieur ou égal à j_{sup}.

Montrons pourquoi $pairPrécédent$ ne peut être congru à 1 ou bien à $p_k - 1$ modulo tout p_k compris entre j_{sup} et p_i. Pour tous les modules p_k, de j_{sup} à p_i, on a vu que $pairPrécédent$ est congru à lui-même, étant inférieur aux modules considérés.

$$\#p_{i-1} < j_{inf} < pairPrécédent < j_{sup} < \#p_i$$

Si $pairPrécédent \equiv 1\ (mod\ p_k)$, p_k compris entre j_{sup} et p_i, alors $j_{inf} = pairPrécédent - 1 \equiv 0\ (mod\ p_k)$ ce qui est impossible car j_{inf}, étant un nombre premier, ne peut être congru à 0 que modulo lui-même.

De même, si $pairPrécédent \equiv p_k - 1\ (mod\ p_k)$, p_k compris entre j_{sup} et p_i, alors $j_{sup} = pairPrécédent + 1 \equiv 0\ (mod\ p_k)$ ce qui est impossible car j_{sup}, étant un nombre premier, ne peut être congru à 0 que modulo lui-même.

Montrons maintenant que pour tout p_k compris entre p_i et $\#p_i + pairPrécédent - 1$, on ne peut obtenir $p_k - 1$ comme reste modulo p_k. Les p_k en question étant tous strictement supérieurs à p_i sont strictement supérieurs à $pairPrécédent + 1$ et $pairPrécédent$ ayant pour reste lui-même modulo tous ces nombres premiers, il n'est pas possible d'obtenir un reste de 1 ou de $p_k - 1$ selon les modules p_k en question.

On a ainsi trouvé un nombre pair $nouveauPair = \#p_i + pairPrécédent$ entre $\#p_i$ et $\#p_{i+1}$ qui est juste entre deux nombres premiers dans la mesure où il n'est congru ni à 1 ni à $p_k - 1$ modulo p_k, tout nombre

†Ce nombre $pairPrécédent$ est de la forme $\#p_{i-1} + \Delta$ avec Δ strictement inférieur à p_i.
‡On applique la règle d'addition des congruences

$$a \equiv b\ (mod\ m)\ et\ c \equiv d\ (mod\ m) \iff a + c \equiv b + d\ (mod\ m)$$

premier qui est inférieur à son prédécesseur.

Il y a donc autant de couples de nombres premiers jumeaux que de nombres premiers, soit une infinité.