Nombres premiers jumeaux

L'année 2015 verra peut être la conjecture des nombres premiers jumeaux s'éteindre. De grandes avancées ont été réalisé ces deux dernières années à la suite d'une publication de Yitang Zhang. Celle ci prouve qu'il existe une infinité de couples (p, p') de nombres premiers tels que la différence $p'-p$ est inférieure à $70\ 10^6$.
Un groupe "polymath8" a même été crée, il regroupe des mathématiciens illustres tel Terence Tao. Son objectif est d'améliorer la majoration trouvée par Yitang Zhang et si possible la ramener à 2. Le travail d'un jeune mathématicien, James Maynard, a déjà permis de la ramener à quelques centaines. Pour en savoir plus www.larecherche.fr/savoirs/palmares/reduire-ecart-entre-nombres-premiers.

Le moment me paraît donc bien choisi pour sensibiliser les élèves de classes terminales et leurs professeurs sur un sujet qui défit l'esprit depuis des siècles:

" Existe t il une infinité de paires de nombres premiers jumeaux?"

Le court texte qui suit ne cherche pas à démontrer la conjecture, ni à donner, en une poignée de secondes, la liste des paires de nombres premiers jumeaux inférieures à 10 000 000.
Dans une première partie il donne une interprétation géométrique du résultat de Yitang Zhang qui mène à l'énoncé d'une conjecture équivalente à celle des nombres premiers jumeaux et dans une deuxième partie il met en évidence un crible qui permet de déterminer les premières paires en s'inspirant du crible d'Ératosthène pour les nombres premiers.
Le logiciel Xcas permet de mettre en œuvre le crible.
La lecture est aisée pour un élève qui s'intéresse aux mathématiques. Seule une allusion au postulat de Bertrand : "pour $n > 1$, il existe un nombre premier strictement compris entre n et $2n$", sort du programme.
Il me semble que les amateurs de dénombrement, comme le fut certainement Viggo Brun en son temps, en tirerons profit pour faire quelques pas vers la conjecture, des pas qui sans nul doute les mèneront vers le Capitole.

Sommaire

Notation
p1(n) désigne le plus petit diviseur premier de *n, pr*(*n*) est le nombre premier qui suit immédiatement *p1*(*n*). Exemple : *p1*(55) =5 et *pr*(55)=7. .
De même si *p* désigne un nombre premier, *p*++ est le nombre premier qui suit immédiatement *p*.

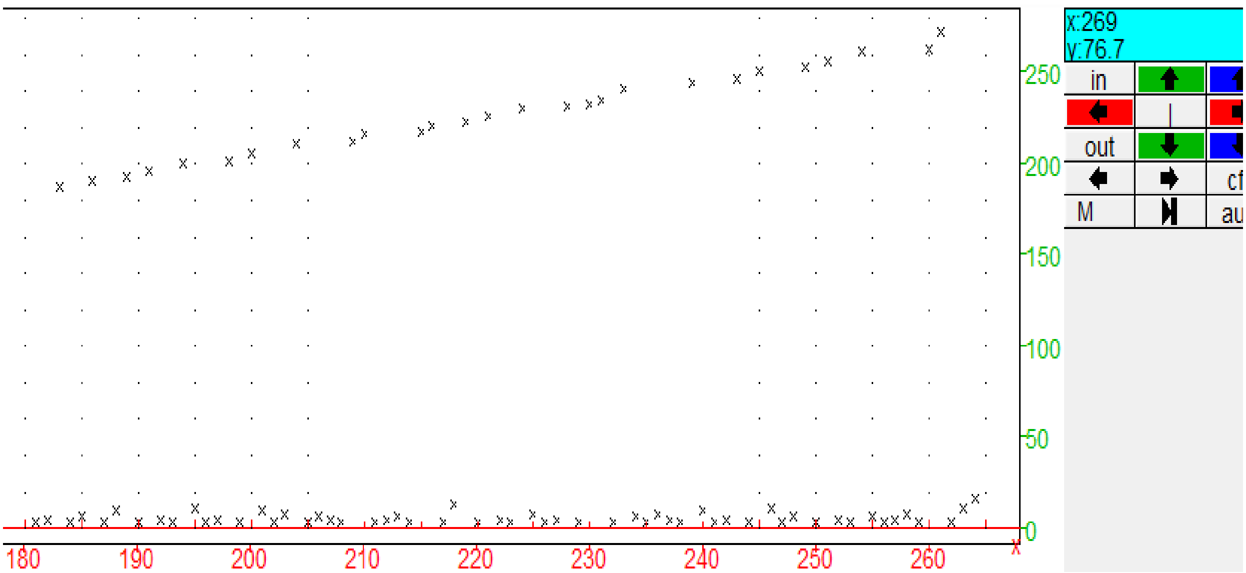
Définition
(*p*, *p*++) est une paire de nombres premiers jumeaux si et seulement si *p* est premier et *p*++= *p* + 2.
La conjecture des nombres premiers jumeaux affirme qu'il en existe une infinité.

Interprétation géométrique du résultat de Yitang Zhang

Représentation de la fonction définie dans N* par

$$z \ : \ n \ \rightarrow \ \frac{3+pr(2n+1)}{2} \ .$$

La fonction *z* se représente par un ensemble de points dont voici une représentations sur l' intervalle [181, 264].



On constate deux alignements de points dont l'un semble oblique.
Bien que les points semblent s'agglutiner sur l'axe des abscisses, celui ci n'intercepte pas le "nuage" de points. Il en va de même pour la droite d'équation y = 6. Nous verrons pourtant que la droite d'équation y=4 l'intercepte en une infinité de points ainsi que tout un faisceau de droites horizontales.

Existe t il une droite qui, pour l'alignement oblique, rencontre le nuage de points une infinité de fois? La découverte de Yitang Zhang permet de répondre à cette question par l'affirmative.
La conjecture des nombres premiers jumeaux se veut plus précise. Elle prétend donner l'équation d' une telle droite!

Pour montrer ces résultats nous devons en savoir plus sur la fonction *z*.

Propriétés élémentaires de la fonction *z*. $z(n)=\frac{3+pr(2n+1)}{2}$

E_1 Pour tout n, $z(n) \geq 4$ car la plus petite valeur pour $pr(2n+1)$ est 5.

E_2 On vérifie facilement que les solutions de l'équation $z(n) = 4$ sont les entiers congrus à 1 modulo 3.

E_3 Si $2n + 1$ est premier on dit que *n* est propulsé et on a $z(n) \geq n + 3$.

E_4 Si $z(n) > n$ alors n est propulsé.

Montrons la propriété E_4.

On vérifie facilement que la propriété est vérifiée pour les huit premiers nombres

n	1	2	3	4	5	6	7	8
z(*n*)	4	5	7	4	8	10	4	11

Supposons $n > 8$ et raisonnons par l'absurde,
supposons $z(n) > n$ et *n* non propulsé,
$\frac{3+pr(2n+1)}{2}>n$ implique $pr(2n+1)\geq 2\mathrm{n}-1$ par ailleurs, *n* non propulsé entraîne
$p1(2n+1)\leq\sqrt{(2\mathrm{n}+1)}$ qui pour $n > 8$ donne $p1(2n+1)\leq\sqrt{(2\mathrm{n}+1)}<\frac{n}{2}$
Le "postulat de Bertrand" implique $pr(2n+1)<n$ d'où une contradiction.

Remarque : 4 est point fixe car $z(4)=4$ et n'est pas propulsé.

Retour sur le résultat de Yitang Zhang

L'existence d'une infinité de couples (p , p') de nombres premiers tels que $p'-p \leq 70.10^6$ entraîne l'existence d'au moins un nombre pair $2k$ compris entre 1 et 70.10^6 tel qu'il existe une infinité de couples (q , q') de nombres premiers tels que $q'-q = 2k$. En effet entre 1 et 70.10^6 il n'y a qu'un nombre fini de nombres donc au moins l'un d'entre eux est différence une infinité de fois.
Comme $q'-q \geq q{+}{+}-q$, par le même raisonnement on en déduit l'existence d'une infinité de couples (p , p++) de nombres premiers tels que $p{+}{+}-p = 2h$ avec $2h \leq 2k$.
En posant $n=\frac{p-1}{2}$ on a $z(n)=n+2+h$.
Il existe donc une droite d'équation y = x + 2 + *h* qui rencontre une infinité de fois le nuage.
La conjecture des nombres premiers jumeaux affirme que h peut être égal à 1. Peut être existe t il tout un faisceau de droites parallèles ayant la même propriété ? (*On pourrai alors lui faire correspondre le faisceau de droites horizontales dont on a déjà parlé par une rotation suivie d''une autre transformation....?).*

Équivalence de deux conjectures
Nous pouvons maintenant démontrer la propriété suivante:

(2n + 1, 2n+3) est une paire de nombres premiers jumeaux **si et seulement si** $z(n) = n + 3$.

Si (2n + 1, 2n+3) est une paire de nombres premiers jumeaux alors $p1(2n + 1) = 2n + 1$ et $pr(2n + 1) = 2n + 3$ donc $z(n) = n + 3$ d'après la définition de z.
Réciproquement
Si $z(n) = n + 3$ alors $pr(2n + 1) = 2n + 3$ et d'après E_4 n est propulsé donc $p1(2n + 1) = 2n + 1$.
(2n + 1, 2n+3) est une paire de nombres premiers jumeaux.

La conjecture des nombres premiers jumeaux affirme que la droite d'équation y = x +3 intercepte le nuage en une infinité de points.

Réciproquement si la droite d'équation y = x +3 intercepte le nuage en une infinité de points alors il existe une infinité de paires de nombres premiers jumeaux.

La nécessité se fait sentir de mieux connaître ces nombres premiers jumeaux, d'où l'idée de créer un crible à la façon d'Ératosthène afin de trouver les premiers couples de premiers jumeaux.

Le crible d'Ératosthène pour les nombres premiers jumeaux

Pour construire le crible il est nécessaire d'étudier la relation antécédent – image.
Antécédents
Remarquons que d''après E_1 si b est une image alors $b \geq 4$.
On a la propriété suivante :
E_5 b est une image par z si et seulement si $2b - 3$ est premier.
La condition est évidemment nécessaire, cela résulte directement de la définition de la fonction z.
Elle est suffisante car d'après la remarque précédente, b est différent de 3 donc 2b-3 aussi ; le nombre premier impair qui précède $2b$-3 existe, appelons le p, alors $n_0 = \frac{p-1}{2}$ est un antécédent propulsé de b.
En effet $2n_0+1 = p$ donc n_0 est propulsé et $p{+}{+} = 2b$-3 donc $z(n_0) = \frac{3+2b-3}{2} = b$.
Remarque :
1- Un nombre multiple 3 ne possède pas d'antécédent.
2- Les nombres b, images par la fonction z : 4, 5, 7,8, 10, 11, 13, 16, 17....sont en correspondance avec les nombres premiers :3, 5, 7, 11, 13, 17, 19, 23, 29, ….
par exemple :$p = 3$ et $p{+}{+} = 5$ $4 = \frac{3+5}{2}$ …..... $16 = \frac{3+29}{2}$ $p = 23$ et $p{+}{+} = 29$

Écriture d'un antécédent de *b*.
Posons $q = 2b - 3$ et supposons q premier. Soit p le nombre premier qui précède q.
n est antécédent de b si $p = p1(2n + 1)$ donc $2n + 1 = pQ$ avec comme condition sur Q :

$Q = 1$ ou les diviseurs premiers de Q sont supérieurs ou égaux à p.
Un antécédent de b s'écrit donc $n = \frac{pQ-1}{2}$ pour certaines valeurs de Q.
b possède une infinité d'antécédents donc la droite d'équation y = b rencontre une infinité de fois le nuage de points.
Le plus petit antécédent $n_0 = \frac{p-1}{2}$ est obtenu pour $Q = 1$. Il est propulsé donc plus petit que b.
l'antécédent immédiatement supérieur à n_0, $n_1 = \frac{p^2-1}{2}$ est obtenu pour $Q=p$. Il est strictement supérieur à b dès que p est plus grand que 3. Il n'est jamais propulsé puisque $2n_1 + 1$ n'est pas premier.

Remarque importante

pour chaque couple (b, p) l'équation $z(n)=b$ possède dans l'ensemble 1, 2, 3,....., $\frac{p^2-1}{2}$ exactement deux solutions dont une seule est propulsée $\frac{p-1}{2}$.
De plus l'équation $z(n)=b'$ pour $b' > b$ possède au plus une solution propulsée dans cet ensemble.
Ainsi, si nous rayons de cet ensemble tous les nombres qui sont solutions des équations $z(n)=b''$ pour $b'' \leq b$ en prenant garde de ne pas rayer la plus petite alors les nombres non rayés restants sont propulsés. En effet ils sont : soit première solution d'une équation $z(n) = b''$ ou $z(n) = b'$.

À la manière d'Ératosthène

Le tableau suivant donne les deux premiers antécédents pour les premières valeurs de b. Il nous sera utile pour nos exemples.

b	p	$\frac{p-1}{2}$	$\frac{p^2-1}{2}$
4	3	1	4
5	5	2	12
7	7	3	24
8	11	5	60

Le principe sur un exemple

Le problème à résoudre "Trouver tous les"premiers jumeaux" inférieurs à 50″.
Écrivons tous les nombres de 1 à 25.
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 16, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25

Apparition des tandems
Marquons en rouge les nombres qui vérifient $z(n)=4$ sauf la plus petite qui est 1. Ce sont les nombres congrus à 1 modulo 3

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
Par « marquons » il faut comprendre « supprimons, rayons ».
Nous voyons apparaître des tandems de deux nombres consécutifs (en noir) entre deux nombres rayés avec une exception pour 1,2 et 3 qui donnent deux tandems.

(1,2), (2,3), (5,6), (8,9), (11,12), (14,15), (17,18), (20,21), (23,24)

Suppression des tandems

Marquons en bleu les nombres qui ne sont pas rayés et qui vérifient $z(n)=5$ sauf la plus petite qui est 2. Nous verrons plus loin comment les trouver.
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24
Toute marque dans un tandem supprime ce tandem. (11,12) et (17,18) disparaissent. Les tandems restants sont

(1,2), (2,3), (5,6), (8,9), (14,15), (20,21), (23,24)

Marquons en vert les nombres qui vérifient $z(n)=7$ sauf le premier.
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24
Cela revient à rayer 24 donc à faire disparaître le tandem (23,24). Il reste

(1,2), (2,3), (5,6), (8,9), (14,15), (20,21)

On s'arrête ici car la première solution non propulsée de l'équation $z(n)=8$ est 60 donc supérieure à 24. Il en sera de même pour les équations suivantes $z(n)=10$, …....
Tous les tandems qui subsistent sont formés d'éléments propulsés qui donnent les premières paires de nombres premiers jumeaux inférieures à 50, ceci par l'application x->2x+1
(1,2)----->(3,5) (5,6)----->(11,13) (14,15)----->(29,31)
(2,3)----->(5,7) (8,9)----->(17,19) (20,21)----->(41,43)
Remarques
1-On a utilisé trois couleurs pour mettre en évidence les nouveaux nombres rayés,mais la couleur rouge est suffisante.
2-Comment rayer les solutions de l'équation $z(n)=5$ sauf la première ?
Il suffit de rayer les nombres de la suite arithmétique $u_t=2+5t$ sauf 2. car $2u_t+1=5(1+2t)$ et $p1(2u_t+1)=5$ ou $p1(2u_t+1)=3$ donc $z(u_t)=5$ ou $z(u_t)=4$ dans ce dernier cas u_t a déjà été rayé.
Par ailleurs si $z(n)=5$ alors $n=\frac{5Q-1}{2}$ et Q est impair $Q=2t+1$ donc $x=2+5t$ c'est un terme de la suite. On raye bien toutes les solutions de $z(n)=5$.
De même pour rayer les solutions de l'équation $z(n)=7$ sauf la première , Il suffit de rayer les nombres de la suite arithmétique $u_n=3+7n$ sauf 3 puisqu'ils vérifieront $z(n)=7$ ou $z(n)=5$ ou $z(n)=3$ et dans les deux derniers cas ils auront déjà été rayés. Ainsi de suite.

Énoncé du Principe

Le problème à résoudre "Trouver tous les"premiers jumeaux" inférieurs à N."
On écrit tous les nombres de 1 à $\frac{N}{2}$
On raye les termes de la suite arithmétique $u_t=1+3t$ sauf le premier".
Les tandems apparaissent
On raye les termes de la suite arithmétique $u_t=2+5t$ sauf le premier".
Certains tandems disparaissent.
…..
…..
On continue jusqu'à

On raye les termes de la suite arithmétique $u_t = \dfrac{p-1}{2} + pt$ sauf le premier".

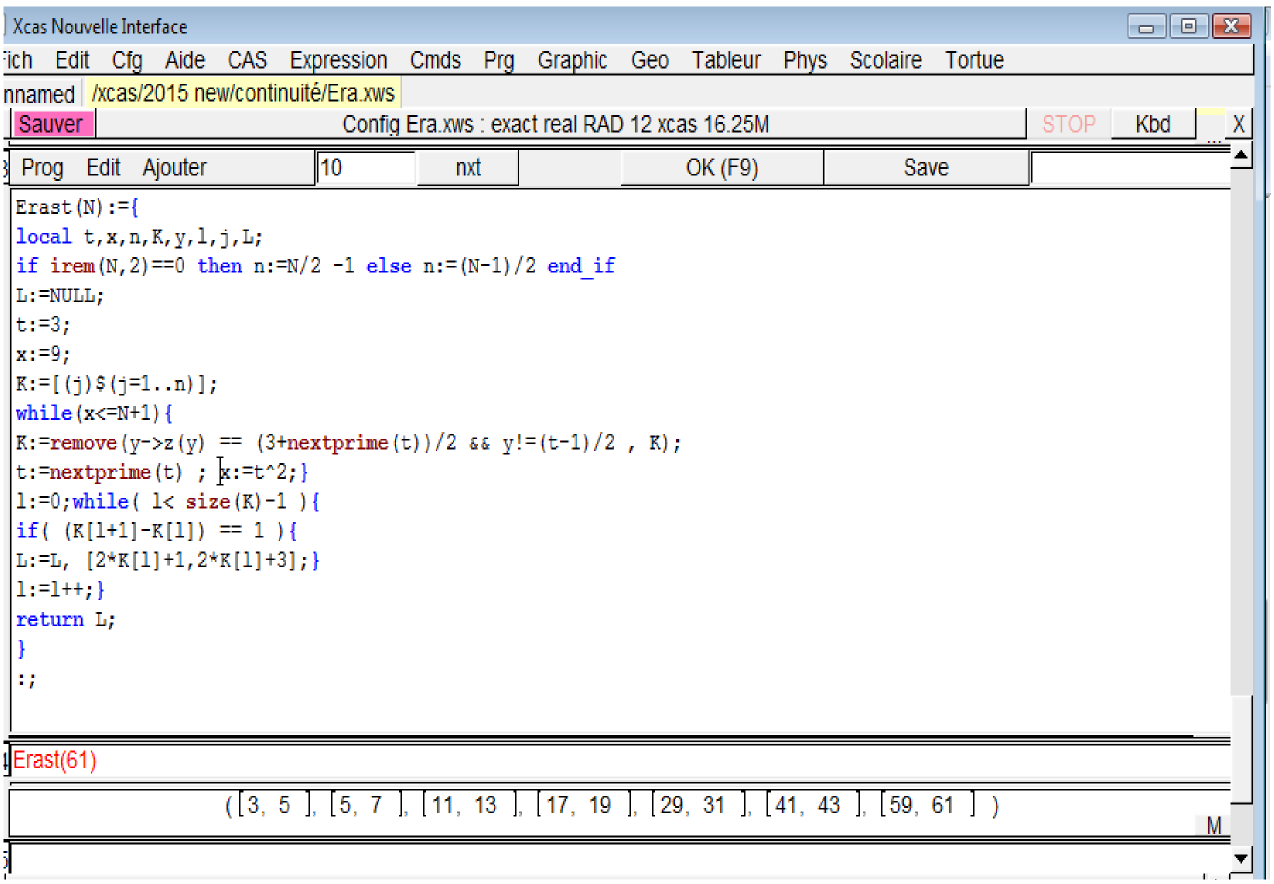
Avec p qui est le plus grand nombre premier vérifiant $p^2 \leq N+1$ c-à -d $\dfrac{p^2-1}{2} \leq \dfrac{N}{2}$.

Par l'application x----> 2x + 1

Les tandems restants donnent les premiers "premiers jumeaux" inférieurs à *N*.

Remarque:
Chaque ligne "On raye les termes de la suite arithmétique $u_t =$ ......sauf le premier" peut être remplacée par "On raye les solutions de l'équation $z(n) =$ …..sauf la première"

Le programme



Quelques remarques concernant le programme ci-dessus.

La variable locale n sert à écrire la liste initiale. Pourquoi ne pas prendre $n = \dfrac{N}{2}$?

Si pour N pair on prend $n = \dfrac{N}{2}$ alors $2n + 1 = N + 1$et le programme pourrai renvoyer la paire [N -1, N +1]. En prenant $n = \dfrac{N}{2} - 1$ la liste initiale s'arrête à N-1 ce qui n'est pas grave car N étant pair, il ne peut être dans une paire de "premiers jumeaux ".

Si N est impair, le choix $n=\frac{N-1}{2}$ conduit à $2n+1=N$ ce qui est satisfaisant.
K:=[(j)$(j=1..n)] permet d'écrire l'ensemble 1, 2, 3,...., n sous forme de liste pour pouvoir, par la suite, la transformer par des fonctions.
La variable t remplace p et la condition condition $x \leq N+1$ traduit $p^2 \leq N+1$
L'application "remove" de Xcas convient très bien pour faire les éliminations.

La fonction y------> z(y) se construit à l'aide de deux programmes annexes.
Dans le premier on récupère dans une liste L, les diviseurs premiers de n que fournit l'application ifactors de Xcas. On ordonne avec l'application sort la lite. sort(L)[0] est son premier élément.
L'application nextprime achève la détermination de pr(n).

La fonction pr pour n > 1

```
pr(n):={ local K, L, j ;
L:=NULL;
K:=ifactors(n);
for(j:=0; j<size(K); j:= j+2) {L:= L, K[j];}
return nextprime( sort(L)[0] );
}:;
```

La fonction *z*

```
z(n):={
return ( ( 3 + pr(2*n+1))/2 );
}:;
```

Un dernier point sur le faisceau de droites horizontales

Revenons sur la résolution de l'équation $z(n) = b$ lorsque celle ci possède des solutions. On a appelé p le nombre premier qui vient juste avant $2b$-3. Pour connaître l'ensemble des solutions, il suffit de connaître les solutions sur l'ensemble 1, 2, …., 3*5*7*11…...*p puis de translater indéfiniment ces solutions en ajoutant 3*5*7*11…...*p. Cela laisse présager des complications dans la correspondance faisceau oblique – faisceau horizontal.

Vers la conjecture des nombres premiers jumeaux

..........vous avez la main !