

Conjecture de Goldbach et les impairs (Denise Vella-Chemla, 2.6.2019)

Après avoir écouté une conférence de Timothy Gowers, présentant les leçons de Pólya pour résoudre un problème (ici <https://vimeo.com/331192239>), ainsi qu'un interview qu'il a donné dans le cadre des Heidelberg Laureate Forum (ici <https://www.youtube.com/watch?v=7F97Q1DGOkE>), on a l'idée d'appliquer des éléments de connaissance qui nous ont été utiles pour comprendre la conjecture de Goldbach forte (tout nombre pair supérieur à 6 est la somme de deux nombres premiers impairs) aux cas des nombres impairs et cela nous amène à une curieuse découverte. La conjecture de Goldbach pour les nombres impairs exprime que tout nombre impair est la somme de 3 nombres premiers. Harald Helfgott a proposé une démonstration de la conjecture de Goldbach pour les impairs en 2013. La conjecture de Goldbach pour les impairs découlerait trivialement de la conjecture de Goldbach forte (en effet, tout nombre impair étant la somme d'un nombre pair et de 3, si tout nombre pair était la somme de deux nombres premiers, alors tout nombre impair serait la somme de ces deux nombres premiers et de 3, et donc la somme de trois nombres premiers). Ce n'est pas à cela qu'on s'intéresse ici. Il s'agit plutôt d'étudier quel est le complémentaire à un nombre impair n d'un nombre premier qui n'a aucun reste commun avec n (dans les divisions par les nombres premiers inférieurs à \sqrt{n}).

Précisons l'idée : pour trouver les décomposants de Goldbach d'un nombre pair n , on a pris l'habitude d'utiliser un crible particulier : le crible d'élimination des restes modulaires de n ; par exemple, si on cherche les décomposants de Goldbach de 98, qui est égal à 2 modulo 3, à 3 modulo 5 et à 0 modulo 7, on va éliminer tous les nombres impairs qui sont égaux soit à 0 soit à 98, modulo 3 ou bien modulo 5 ou bien modulo 7. Ce faisant, on obtiendra tous les décomposants de Goldbach de 98 compris entre la partie entière de la racine carrée de 98 et la moitié de 98. On a symbolisé ceci par des petits dessins tels que celui ci-dessous, dans lequel les croix montrent les nombres impairs qui ne sont pas égaux à 0 ou bien à 98, modulo 3, modulo 5 et modulo 7.

$n = 98, n \equiv 2 (3), n \equiv 3 (5), n \equiv 0 (7) \text{ sol} \equiv 1 (3), \text{ sol} \equiv 1, 2, 4 (5), \text{ sol} \equiv 1, 2, 3, 4, 5, 6 (7)$																		
$(\text{mod } 7)$		×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	
$(\text{mod } 5)$		×		×	×	×		×	×	×		×	×	×		×	×	×
$(\text{mod } 3)$		×			×			×			×			×			×	
					37			31			19							

On décide de réappliquer le même crible aux nombres impairs n , pour voir si le complémentaire d'un nombre premier p qui ne partagerait aucun de ses restes avec n impair aurait des propriétés particulières.

On utilise le programme suivant :

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

int tabfacteurs[2021], tabpuiss[2021], tabexpo[2021], residfacteurs[2021] ;

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 factorise(int i) {
    int k, p, nbdiv, tempo, expo ;
    int tab[2018] ;

    std::cout << i << "\n" ;
    tab[i] = 1 ;
    tabfacteurs[i] = 1 ;
    tabpuiss[i] = 1 ;
    tabexpo[i] = 1 ;
    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 = nbdiv ; k >= 1 ; --k) {
        std::cout << tabfacteurs[k] << "^" ;
        std::cout << tabexpo[k] << "." ;
    }
}

int main (int argc, char* argv[]) {
    int x, y, module ;
    bool restesdifférents ;

    for (x = 7 ; x <= 2020 ; x = x+2) {
        std::cout << "\n\n" << x << "□-->□\n" ;
        for (y = sqrt(x) ; y <= x/2 ; ++y)
            if (prime(y)) {
                restesdifférents = true ;
                for (module = 3 ; module <= sqrt(x) ; module = module+2) {
                    if (prime(module))
                        restesdifférents = restesdifférents && ((x % module) != (y % module)) ;
                }
                if (restesdifférents) {
                    std::cout << "\n" << y << "□+□" ;
                    factorise(x-y) ;
                    std::cout << "\n" ;
                }
            }
    }
}

```

Le résultat de ce programme est consultable ici : <http://denise.vella.chemla.free.fr/resetlesimpairs.pdf>.

On constate avec surprise qu'il semblerait qu'un nombre impair puisse toujours s'écrire $p_1 + 2^k p_2$ avec $k \geq 1$ et p_1 et p_2 premiers. Cette constatation est peut-être aussi difficile à démontrer que la conjecture de Goldbach.

L'intérêt cependant d'une telle découverte, si elle s'avérait juste, est simplement qu'elle fournit une généralisation de la conjecture de Goldbach, la conjecture forte pour les pairs pouvant être vue comme une réécriture de la formule proposée pour les impairs, avec $k = 0$, i.e. pouvant s'écrire pour tout n pair supérieur ou égal à 6, selon une écriture de la forme $n = p_1 + 2^0 p_2$.

Tentative de démonstration du fait que s'il existe, pour un nombre impair donné n , un nombre premier $p_1 \leq \frac{n}{2}$ qui lui est incongru selon tout module inférieur à sa racine carrée, alors le complémentaire à n de p_1 est un nombre de la forme $2^k p_2$ avec p_2 premier et $k \geq 1$

Soit n un nombre impair et supposons qu'il existe une décomposition additive de n de la forme $p_1 + n'$ avec $p_1 \not\equiv n \pmod{m}$ pour tout m premier tel que $3 \leq m \leq \sqrt{n}$. Montrons qu' n' est alors nécessairement de la forme $2^k p_2$ avec $k \geq 1$ et p_2 premier.

n étant impair, n' est forcément pair. Voyons pourquoi, sous la condition que p_1 existe, alors n' ne contient dans sa factorisation qu'un seul nombre premier (qu'on appellera p_2), en plus d'un certain nombre d'occurrences du facteur premier 2. On a :

$$\frac{n}{2} \leq n' \leq n$$

et

$$p_1 \not\equiv n \pmod{m} \text{ pour tout } m \text{ premier tel que } 3 \leq m \leq \sqrt{n} \quad (1)$$

Cela a pour conséquence que les deux diviseurs premiers autres que 2 de n' devraient être supérieurs à \sqrt{n} (car (1) $\iff n - p_1 \not\equiv 0 \pmod{m}$ avec les mêmes conditions); mais si tel était le cas, i.e. si $n' = 2p'p''$ avec $p' > \sqrt{n}$ et $p'' > \sqrt{n}$ alors n' serait supérieur à $2n$, ce qui est en contradiction avec l'hypothèse $\frac{n}{2} \leq n' \leq n$.

Le complémentaire de p_1 à n est alors forcément de la forme $2^k p_2$ avec $k \geq 1$ et p_2 premier impair. On n'est cependant pas assuré de l'existence obligatoire de p_1 .