Quelques comètes : indicatrice d'Euler, somme des diviseurs, nombre de décompositions de Goldbach..., janvier 2011.

Poursuite des expérimentations.

Quelques expérimentations autour de la Conjecture de Goldbach, février 2011.

Conjecture de Goldbach et systèmes de congruences du second degré, août 2011.

Pourquoi y a-t-il un lien entre les caractres résidu de $2p$ associés à x et $x + p$ lorsque $2p$ est un double d'impair ?.

Résultats démontrés faisant intervenir des résidus quadratiques.

Utiliser les congruences quadratiques pour trouver un décomposant de Goldbach d'un nombre pair, septembre 2011.

Conjecture de Goldbach et résidus quadratiques, septembre 2011.

Nombre de résidus quadratiques de n quelconque qui sont premiers à n.

Pourquoi tout nombre pair sauf 2 est-il la somme de deux nombres premiers ?, octobre 2011.

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair, octobre 2011.

Conjecture de Goldbach et résidus quadratiques, octobre 2011.

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair, octobre 2011.

Conjecture de Goldbach d'un point de vue analytique.

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair.

S'amuser avec les nombres, novembre 2011.

Vision algorithmique de la Conjecture de Goldbach.

Conjecture de Goldbach et nullité du déterminant d'une matrice de Sylvester, décembre 2011.

Quelques comètes : indicatrice d'Euler, somme des diviseurs, nombre de décompositions de Goldbach...

Denise Vella-Chemla

1.1.11

1 Cinq comètes

Les cinq graphiques ci-dessous, obtenus avec gnuplot, présentent les fonctions :

- indicatrice d'Euler (φ),
- somme des diviseurs d'Euler (σ). Une formule de calcul par récurrence de cette somme est fournie dans l'article "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs". Nous avons utilisé pour la calculer une autre formule de récurrence, fournie par Dominique Giard sur la toile dans la séquence A000203 de l'Encyclopédie en ligne des séquences d'entiers (OEIS),
- nombre de diviseurs,
- nombre de décompositions de Goldbach, i.e. nombre de façons différentes d'écrire un nombre pair $2n$ comme somme de deux nombres premiers.
- plus petit décomposant de Goldbach, i.e. associe à $2n$ le plus petit nombre premier p tel que $2n = p + q$ avec p et q premiers,
- et enfin, plus grand décomposant de Goldbach, i.e. associe à $2n$ le plus grand nombre premier inférieur ou égal à n p tel que $2n = p + q$ avec p et q premiers,

Toutes ces visualisations ont pu être réalisées grâce à des outils spécifiques fournis par Daniel Diaz, concepteur de Gnu-Prolog, que l'on remercie vivement.

On constate que la comète de la fonction φ semble comme inversée par rapport aux comètes de σ ou *Goldbach*, des bandes de points plus concentrés apparaissant "à l'intérieur" de la comète, la "première" d'entre elles se trouvant "tout en haut" de la comète.
Les deux comètes de σ et $Nombre\_de\_décompositions\_de\_Goldbach$ semblent présenter une structure similaire, même si l'apparence de celle de la somme des diviseurs est plus linéaire que celle du nombre des décompositions de Goldbach. Si on ramène les trois premières comètes sur un même graphique, la comète des nombres de décompositions de Goldbach se retrouve tout en bas, comme écrasée, car ses valeurs sont bien moindres que celles des deux autres comètes (Figure 7).

On constate que les comètes associées au nombre de diviseurs et au plus petit décomposant de Goldbach se "ressemblent". Visualisons-les sur un même graphique, la figure 8.

2 Mathématiques expérimentales

Dans la comète de Goldbach, on réussit à isoler les lignes de concentration des points qui correspondent aux nombres de décompositions de Goldbach des nombres de la forme $2p$, $6p$, $30p$, soit plus globalement $2kp$ avec p premier (Figures 9, 10 et 11).

On pense qu'on obtiendra également certaines concentrations de points par l'élévation à la puissance des nombres premiers. C'est ce que l'on constate sur la visualisation en figure 12 : les décompositions de Goldbach des nombres de la forme $2p^2$ avec p premier par exemple, se trouvent également dans la tige basse de la gerbe.

Quant aux décompositions de Goldbach des nombres de la forme $2p^3$ avec p premier par exemple, ils semblent se trouver sur les mêmes tiges que les nombres de la forme $2p$ ou $6p$ mais il faudrait le confirmer. Sur le graphique en figure 13, on voit les douze points rouges correspondant aux nombres de décompositions des doubles de cubes[1].

Dans la comète de la somme des diviseurs d'Euler, on réussit à reproduire les mêmes concentrations de points qui correspondent aux sommes des diviseurs des nombres de la forme $2p$, $6p$, $30p$, soit plus globalement $2kp$ avec p premier (Figures 14, 15 et 16).

On reproduit également la concentration de points par l'élévation au carré des nombres premiers. C'est ce que l'on constate sur la visualisation en figure 17 : les sommes des diviseurs des nombres de la forme $2p^2$ avec p premier par exemple, se trouvent également dans la tige basse de la gerbe[2].

Dans la comète de l'indicatrice d'Euler, on réussit à produire des concentrations de points qui correspondent aux sommes des diviseurs des nombres de la forme $2p$, $6p$, $30p$, soit plus globalement $2kp$ avec p premier (les $2p$ sont à peu près au milieu de la comète, les $6p$ plus bas et les $30p$ encore plus bas) (Figures 18, 19 et 20).

Ce sont les points d'abscisse p qui semblent fournir la limite haute de la comète de φ (Figure 21).

On reproduit enfin la concentration de points par l'élévation au carré des nombres premiers. C'est ce que l'on constate sur la visualisation en figure 22 : les sommes des diviseurs des nombres de la forme $2p^2$ avec p premier par exemple, se trouvent également dans la même tige de la gerbe que les $2p^3$.

Pour que ces visualisations soient lisibles, on doit comprendre que les outils permettent de n'afficher qu'un certain nombre de points pris au hasard dans un fichier de données. Si l'on choisit d'afficher tous les nombres de décompositions, on obtient le graphique de la figure 23 ci-dessous, ininterprétable.

Fournissons quelques valeurs du nombre de décompositions de Goldbach des doubles de premiers (qui fournissent les valeurs minimales, en bas de la comète).

[1] Il n'y a que 12 petits points rouges à retrouver sur la tige des $2p$ et sur celle des $6p$ en s'arrachant un peu les yeux mais les zooms-écrans permettent de les retrouver aisément.

[2] Il n'y a que 25 petits points rouges à retrouver sur la tige basse ; à nouveau, les zoom-écrans ne laissent pas de place au doute...

[3] Il y a quelques petits points rouges à retrouver sur la tige des $2p$; à nouveau, les zoom-écrans ne laissent pas de place au doute...

n	$NbDecompG(n)$	$Log(n)$
$9999998 \sim 10^7$	28983	7
$19999982 \sim 2.10^7$	53364	7.3
$29999962 \sim 3.10^7$	75777	7.47
$39999998 \sim 4.10^7$	97514	7.6
$49999966 \sim 5.10^7$	118760	7.69
$59999998 \sim 6.10^7$	139046	7.77
$69999938 \sim 7.10^7$	159569	7.84
$79999966 \sim 8.10^7$	179764	7.9
$89999942 \sim 9.10^7$	199455	7.95
$99999982 \sim 10^8$	218411	8

On constate que le rapport $\frac{218411}{28983} = 7.53$ semble proche du logarithme[4].

Il semblerait également, au vu de ces seules valeurs, que la fonction $NbDecompG$ est additive mais non pas au sens habituel utilisé en théorie des nombres qui veut que $f(a.b) = f(a) + f(b)$ mais plutôt au sens général qui fait que $f(a + b) = f(a) + f(b)$. On constate non seulement que $f(a + b) \sim f(a) + f(b)$ mais également que $f(\lambda a) \sim \lambda f(a)$.

Testons si la fonction NbDecompG est multiplicative. Pour cela, fournissons-en quelques valeurs :

n	$NbDecompG(n)$
$2026 = 2.1013$	32
$4054 = 2.2027$	55
$4106702 = 2.1013.2027$	13561
$8213404 = 2.1013.2.2027$	24549
$2053352 = 1013.2027 + 1$	9187

$NbDecompG(a.b)$ a une valeur différente de $NbDecompG(a).NbDecompG(b)$.

Enfin, fournissons les valeurs et la visualisation des nombres de décompositions de Goldbach de certains multiples des primorielles équitablement répartis jusqu'à 10 millions.

[4] A noter : les nombres premiers 4 999 999, 19 999 999 et 29 999 999 sont particulièrement rigolos. On peut tester la primalité des nombres en utilisant le logiciel de factorisation par la méthode des courbes elliptiques à l'adresse http://www.alpertron.com.ar/ECM.HTM

n	$NbDecompG(n)$
6	1
30	3
210	19
2310	114
30030	905
60060	1564
90090	2135
150150	3215
210210	4273
330330	6181
390390	7094
510510	9493
1021020	17075
1531530	24044
2552550	37302
3573570	49655
5615610	73205
6636630	84638
8678670	106360
9699690	124180

Comme on peut le constater, ces nombres semblent fournir les valeurs limites hautes de la comète (Figure 24).

Les outils permettent enfin, et cela n'est pas la moindre des choses, de voir si une fonction définie par l'utilisateur minore ou pas le nombre de décompositions de Goldbach (combien de fois, pour qui, etc).

J'ai choisi de visualiser sur la figure 25 la fonction de minoration suivante, découlant de la méthode dite par "pliage du tissu" dans laquelle le produit s'effectue sur les nombres p premiers impairs inférieurs ou égaux à $2\sqrt{x}+1$:

$$MinoreGoldbach(x) = \left\lfloor \frac{x-1}{2} \right\rfloor \prod_{p} \left(1 - \frac{2}{p}\right)$$

Des tests plus poussés montrent que, quoique proche du nombre de décompositions de Goldbach (la différence maximum enregistrée entre le résultat de cette fonction et le nombre de décompositions de Goldbach est de 43 jusqu'à 10^7), elle ne le minore pas.

Par contre, en divisant le résultat de la fonction proposée par $log(x)$ ou bien par $log(log(x))$, on obtient une minoration systématique, mais en obtenant des résultats en moyenne plus éloignés des points de la comète (les outils permettent d'obtenir un rapport moyen de 13.94 dans le premier cas et de 2.5 dans le deuxième cas). La première formule, bien que non minorante, permettait d'obtenir un rapport moyen de 0.92, qui représente le fait que la formule "collait" bien aux points de la comète.

Je remercie vivement le professeur Claude-Paul Bruter qui m'a encouragée tout au long de ces expérimentations.

[H]

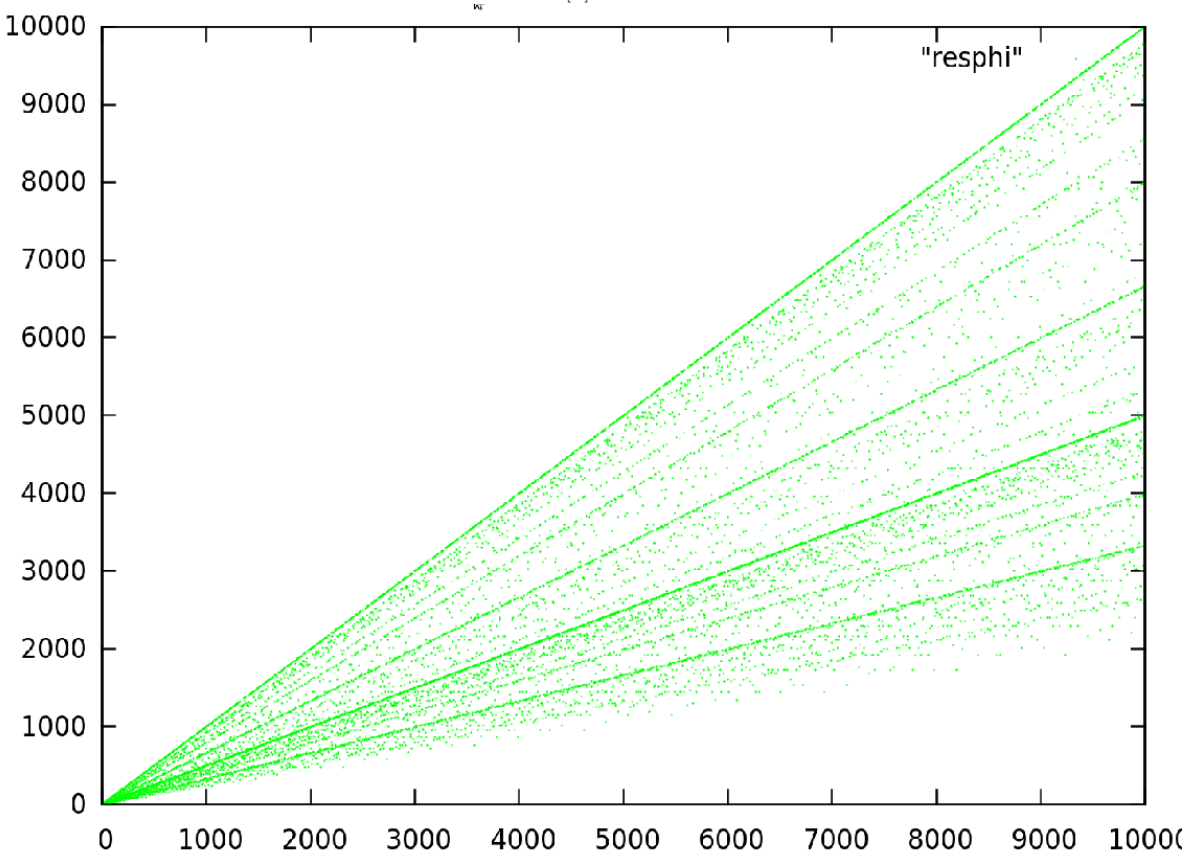


Fig. 1 : Indicateur d'Euler

[H]

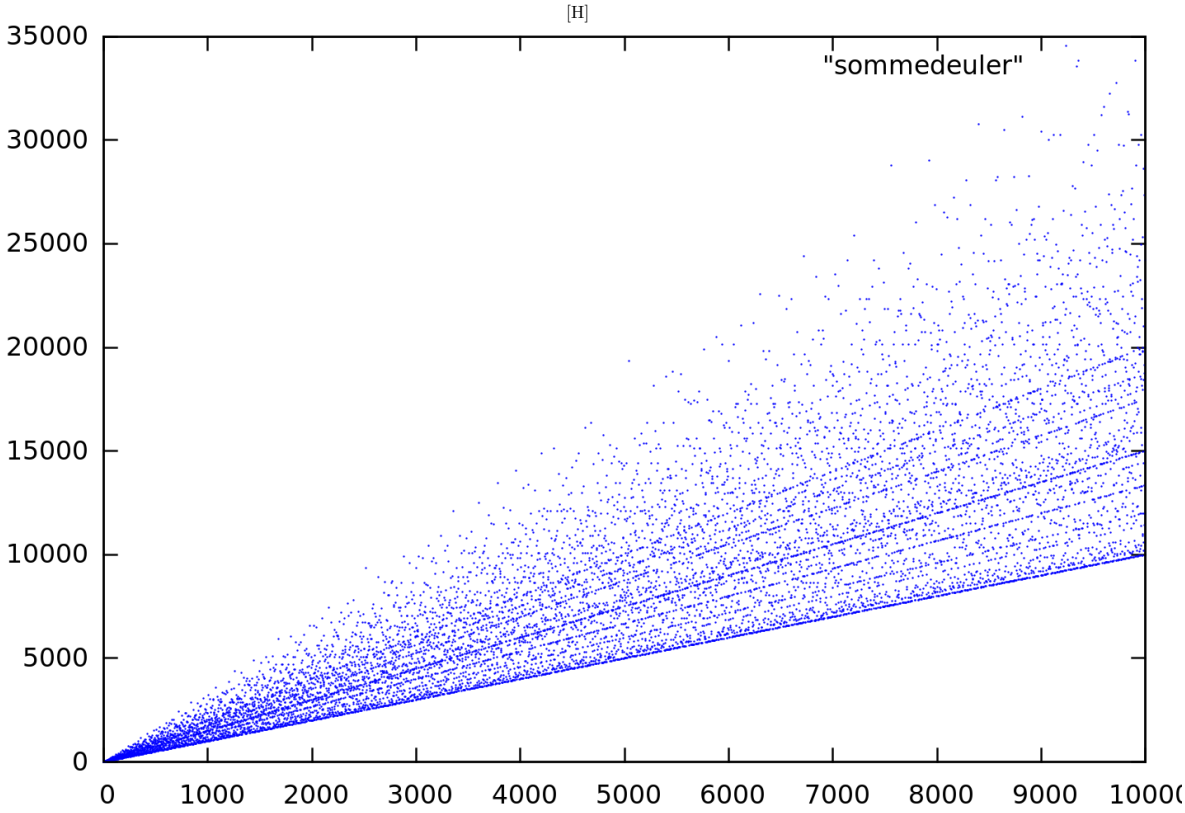


Fig. 2 : Somme des diviseurs

[H]

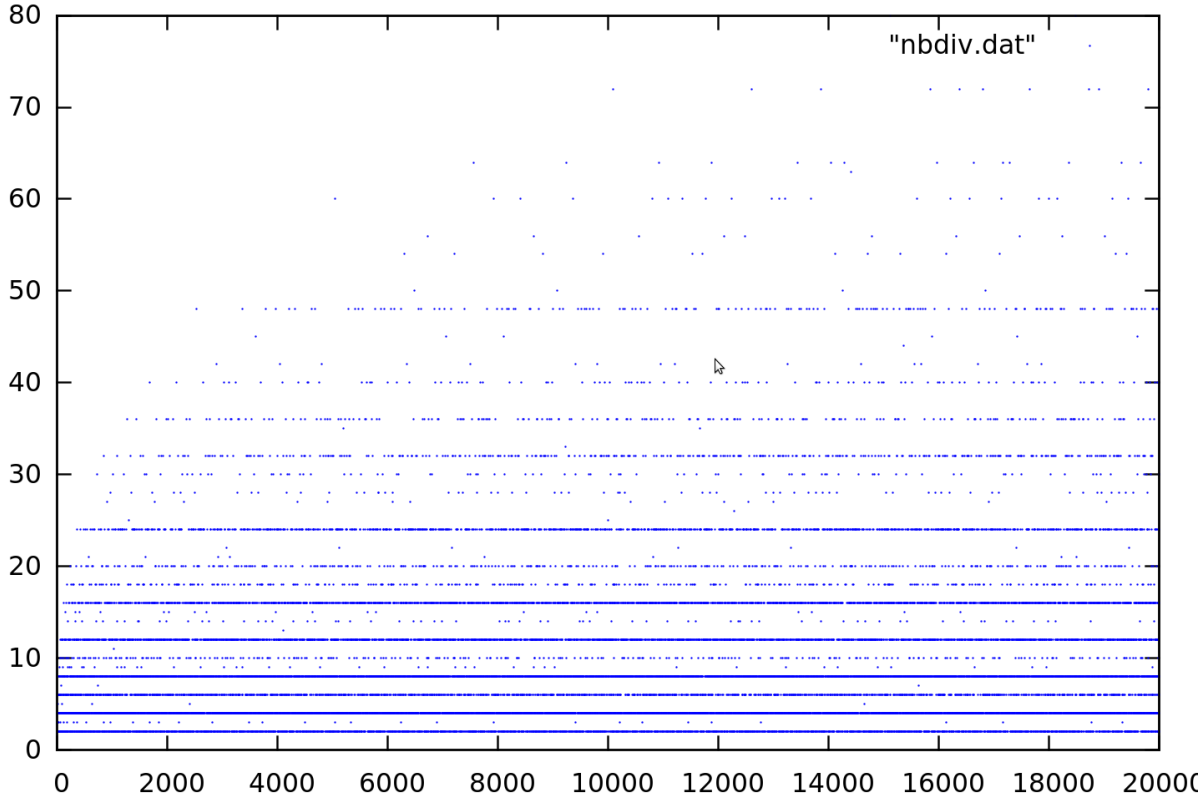


Fig. 3 : Nombre de diviseurs

[H]

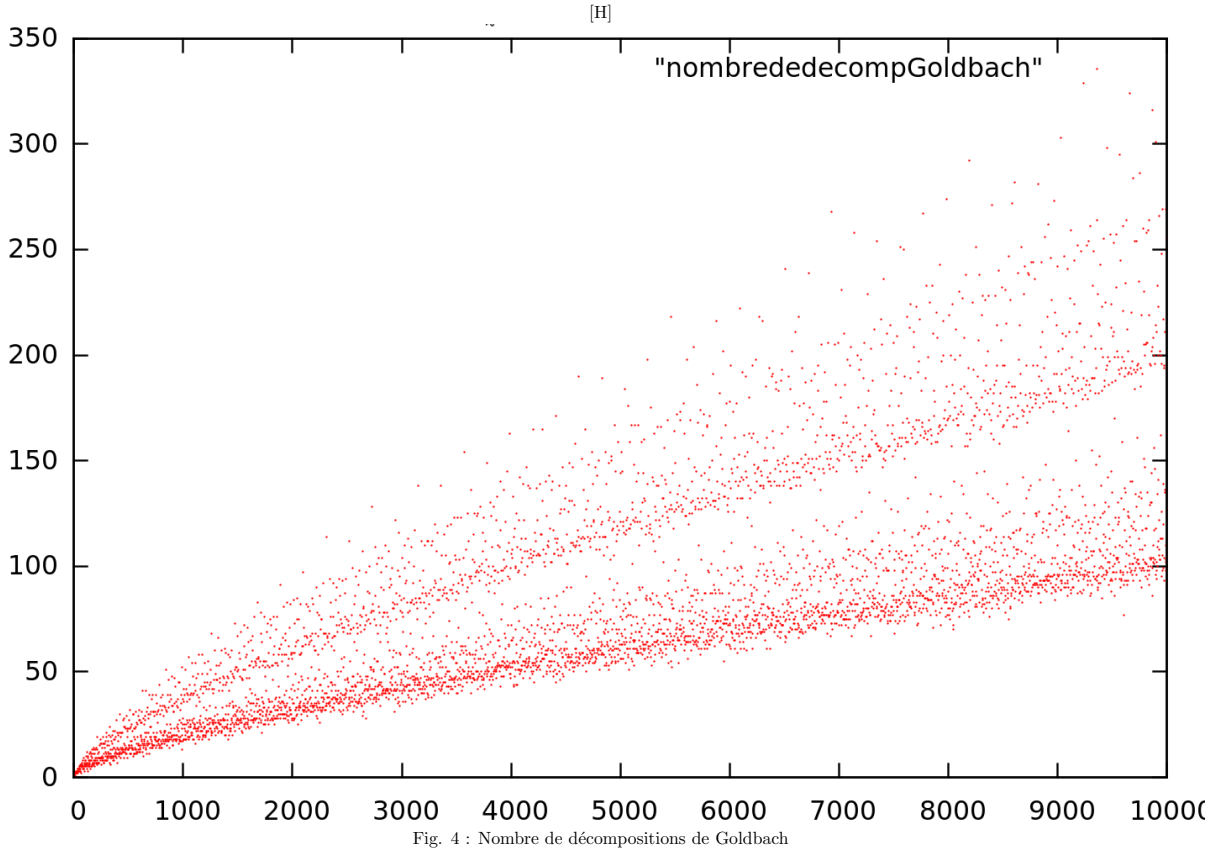


Fig. 4 : Nombre de décompositions de Goldbach

[H]

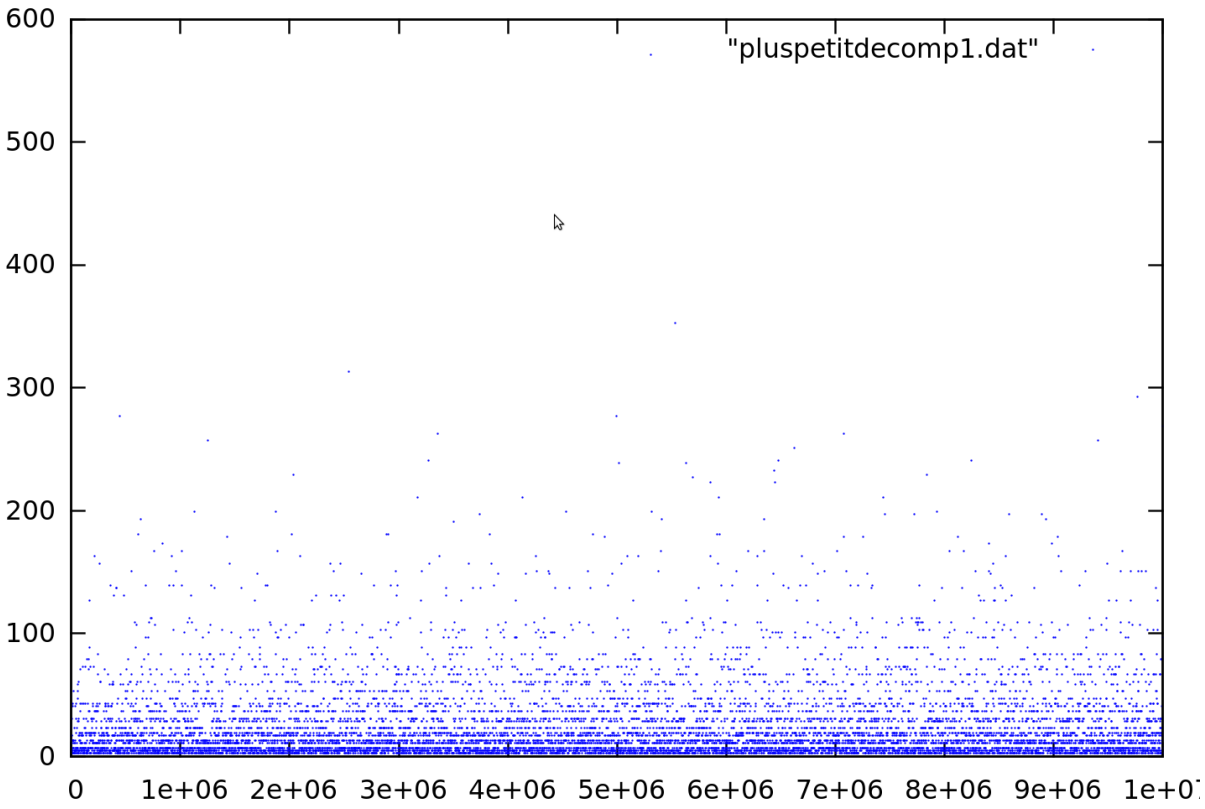


Fig. 5 : Plus petit nombre premier intervenant dans une décomposition de Goldbach

[H]

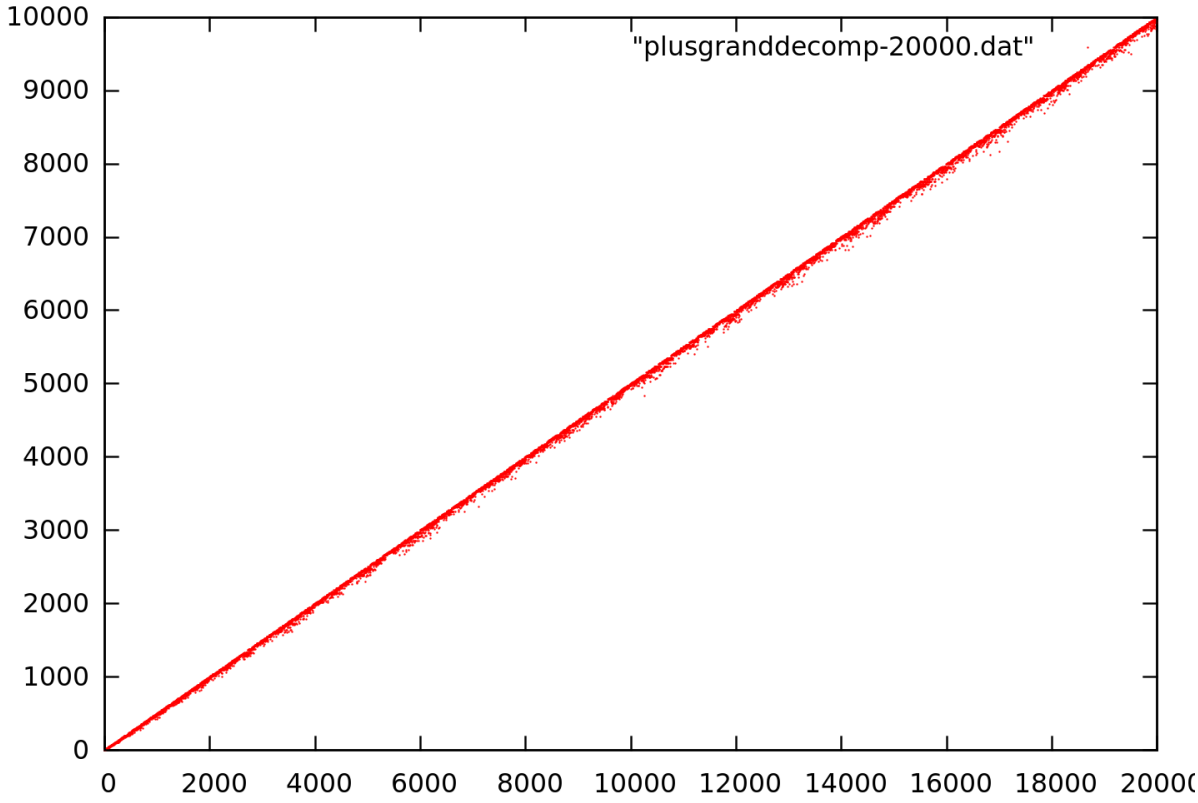


Fig. 6 : Plus grand nombre premier intervenant dans une décomposition de Goldbach

[H]

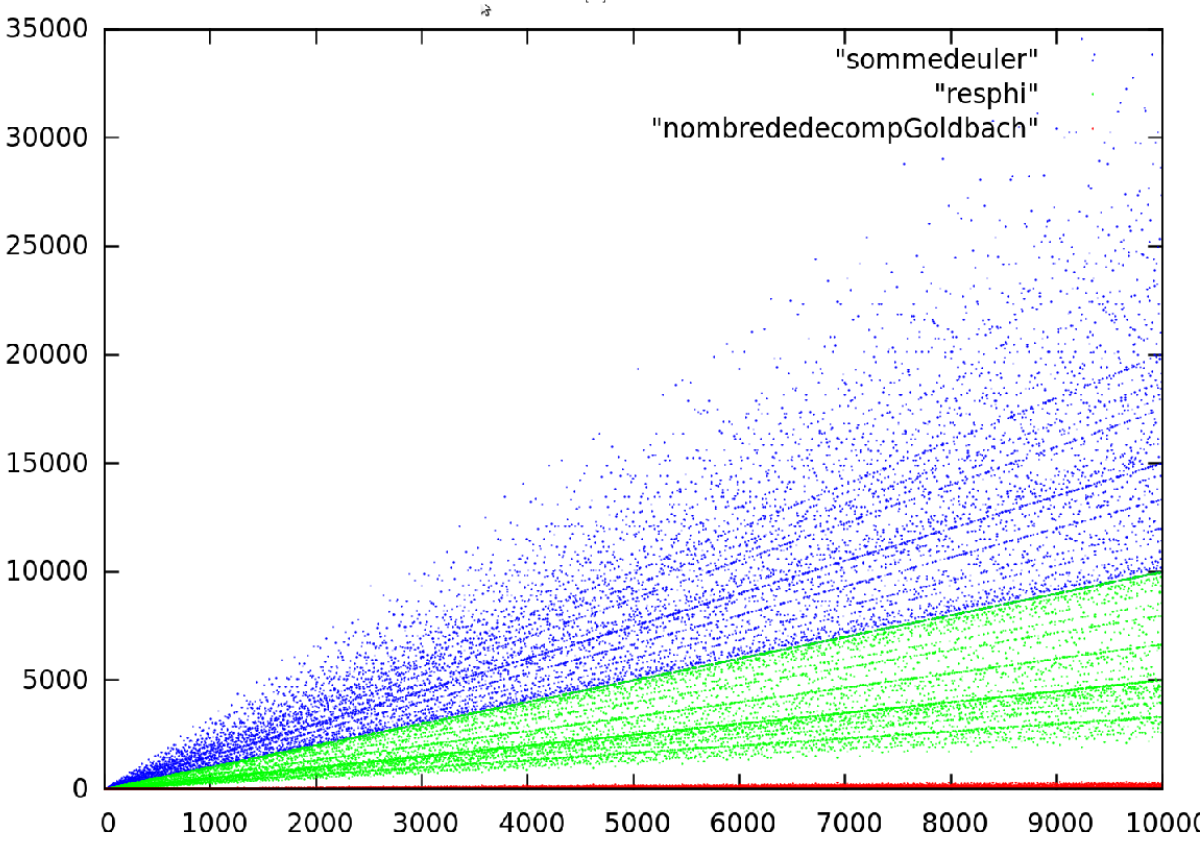


Fig. 7 : σ, φ et Nombre de décompositions de Goldbach

[H]

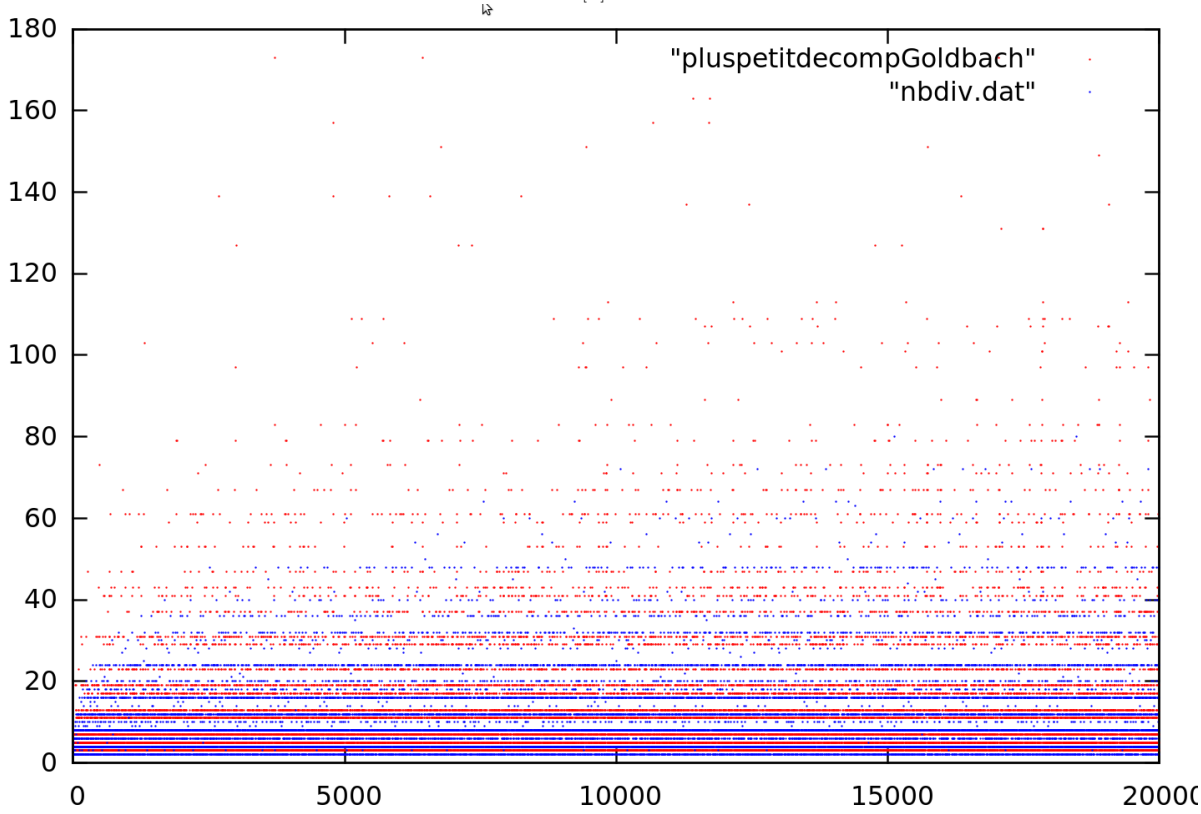


Fig. 8 : Plus petit nombre premier intervenant dans une décompositon de Goldbach et nombre de diviseurs

[H]

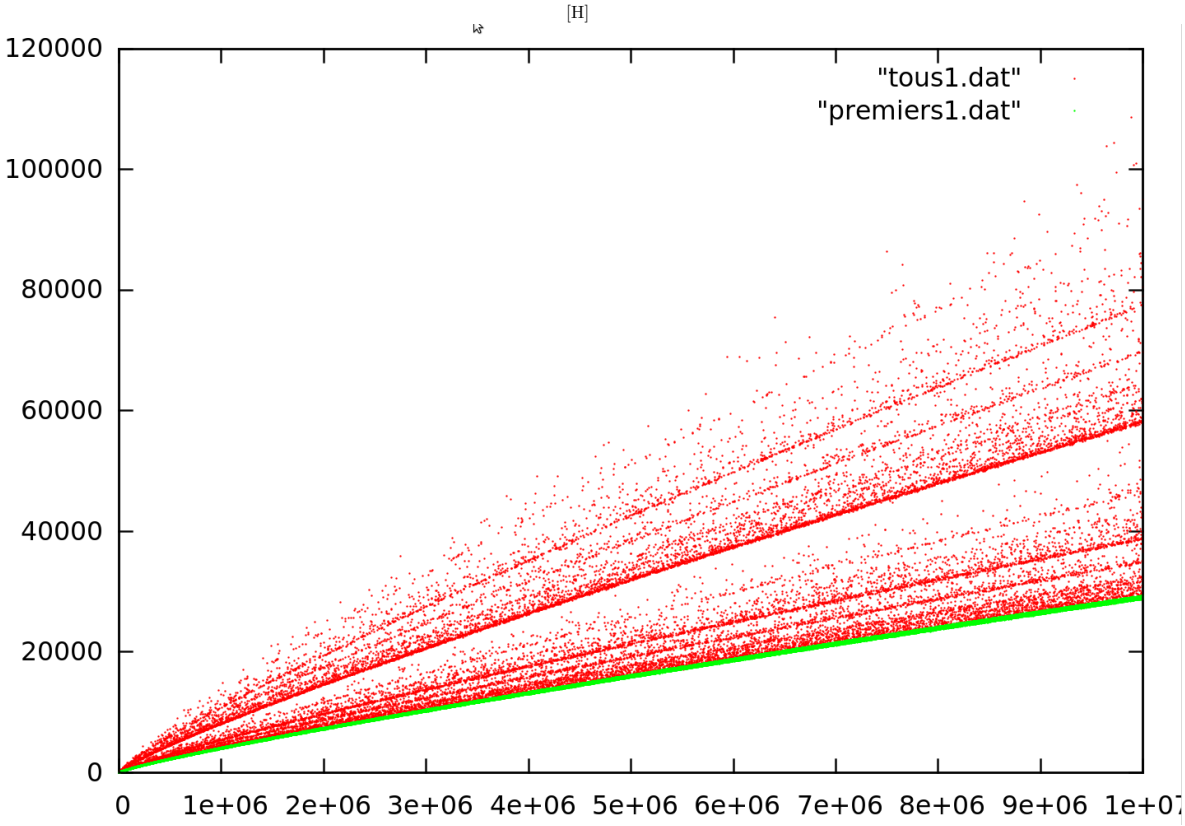


Fig. 9 : Nombre de décompositions de Goldbach des nombres de la forme $2p$ (doubles de premiers)

[H]

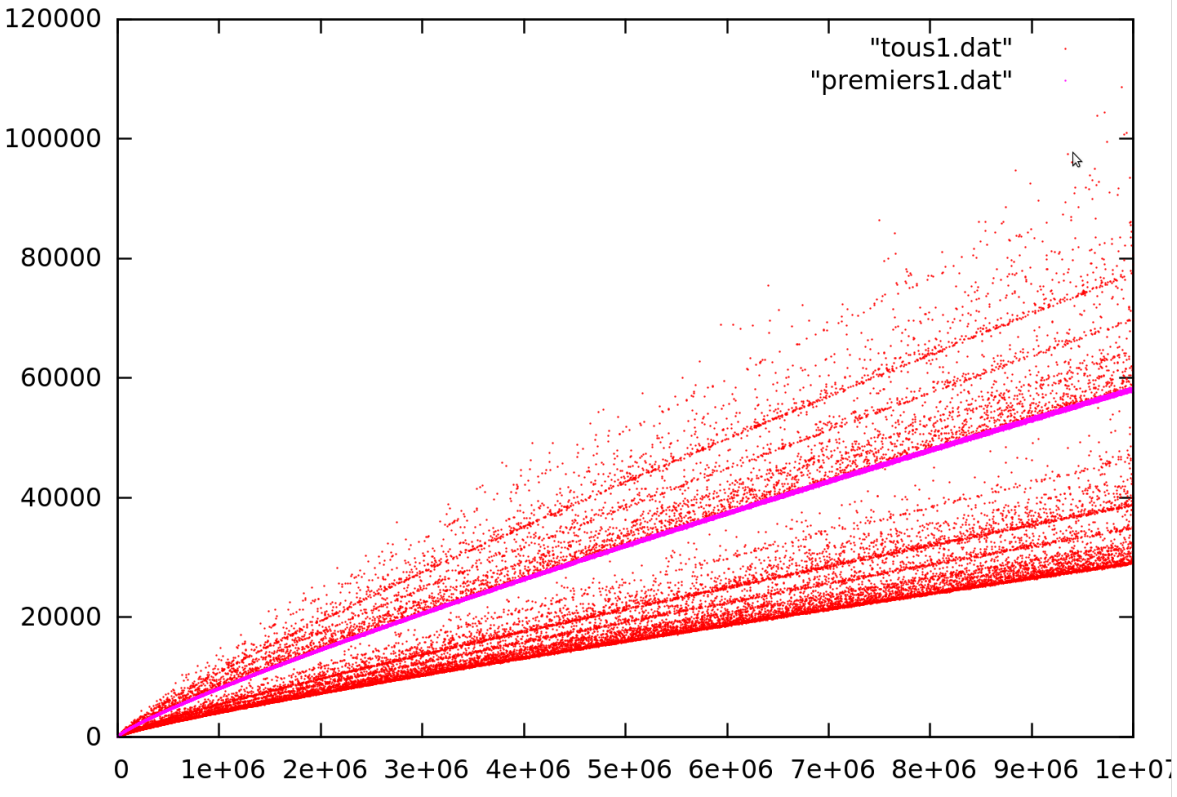


Fig. 10 : Nombre de décompositions de Goldbach des nombres de la forme $6p$

[H]

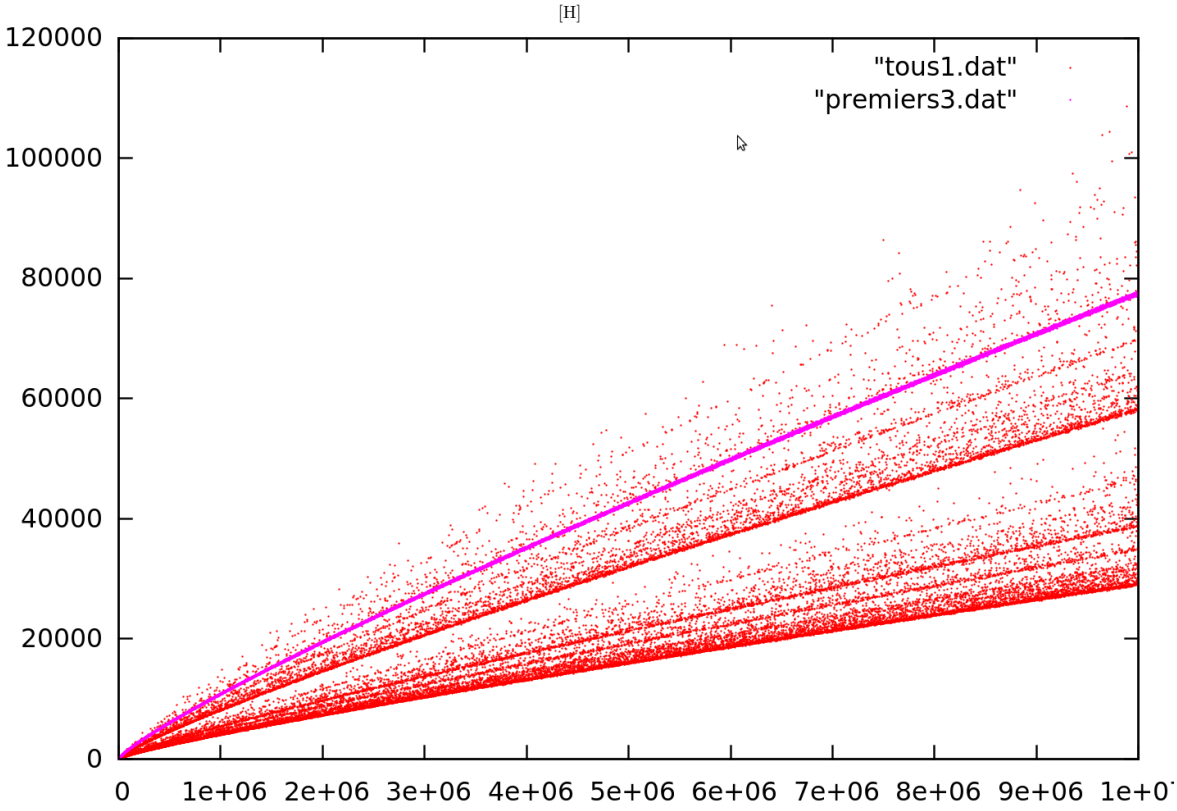


Fig. 11 : Nombre de décompositions de Goldbach des nombres de la forme $30p$

[H]

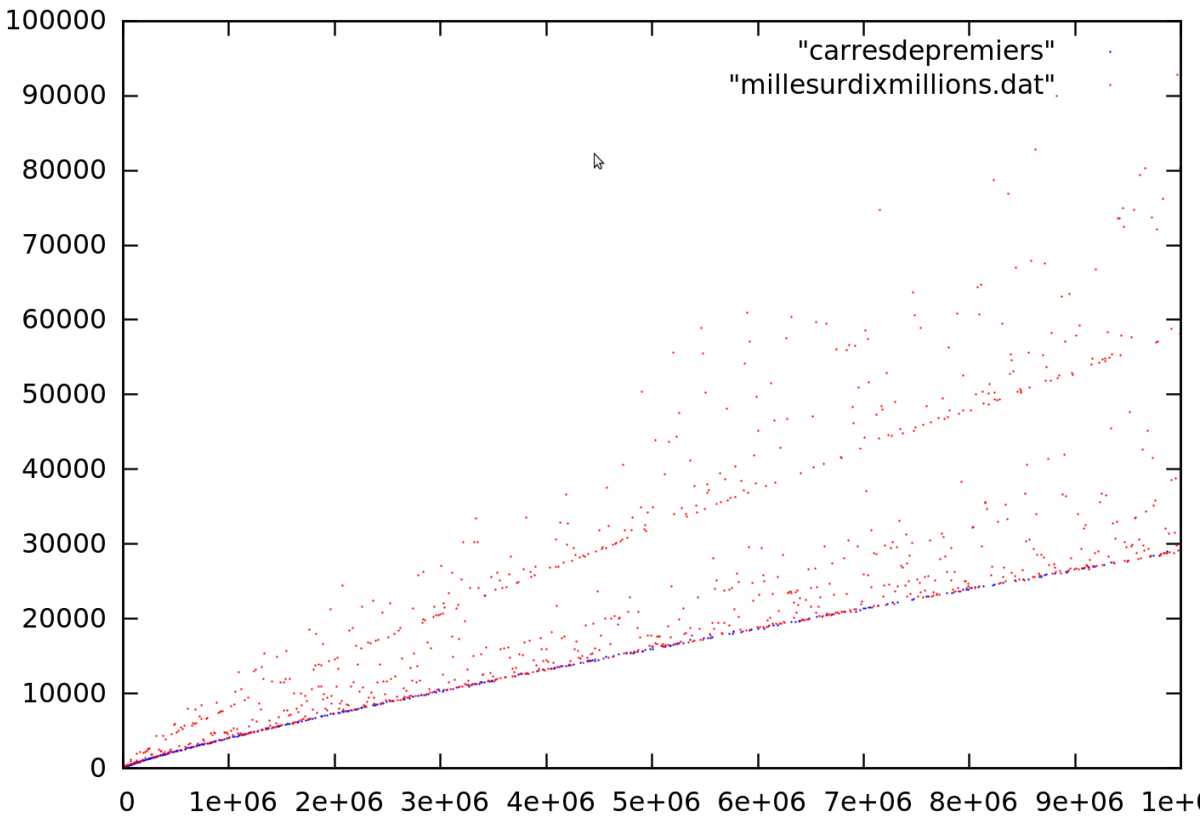


Fig. 12 : Les nombres de décompositions de Goldbach des doubles de carrés de premiers sont sur la première tige de concentration de points.

[H]

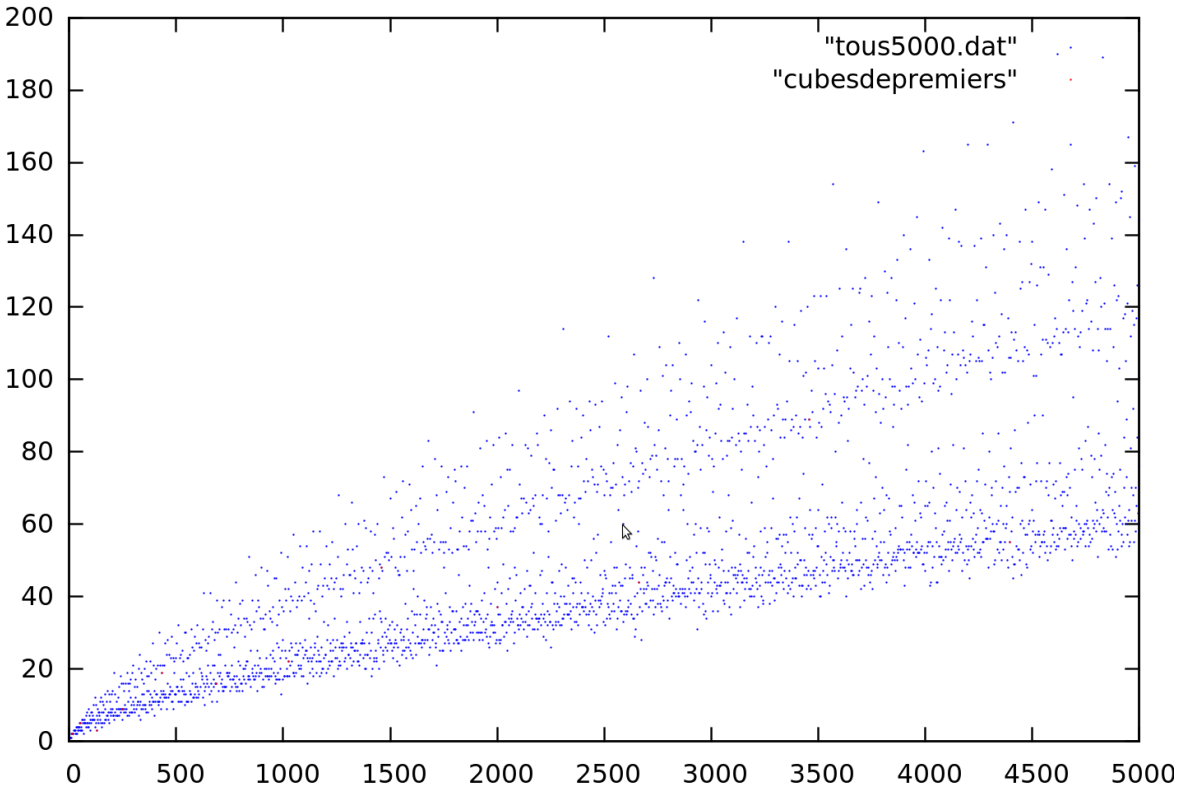


Fig. 13 : Les doubles de cubes de premiers sont sur la deuxième tige de concentration de points.

[H]

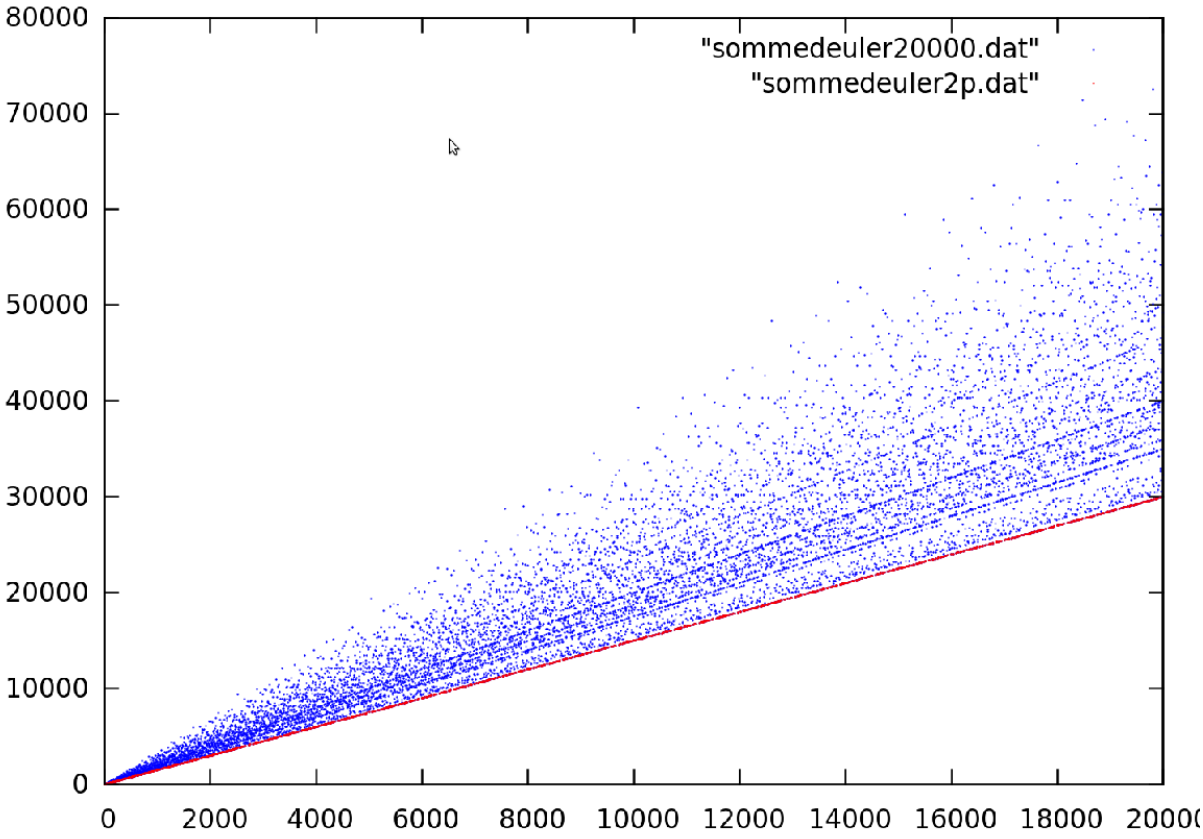


Fig. 14 : σ appliquée aux nombres de la forme $2p$ (doubles de premiers)

[H]

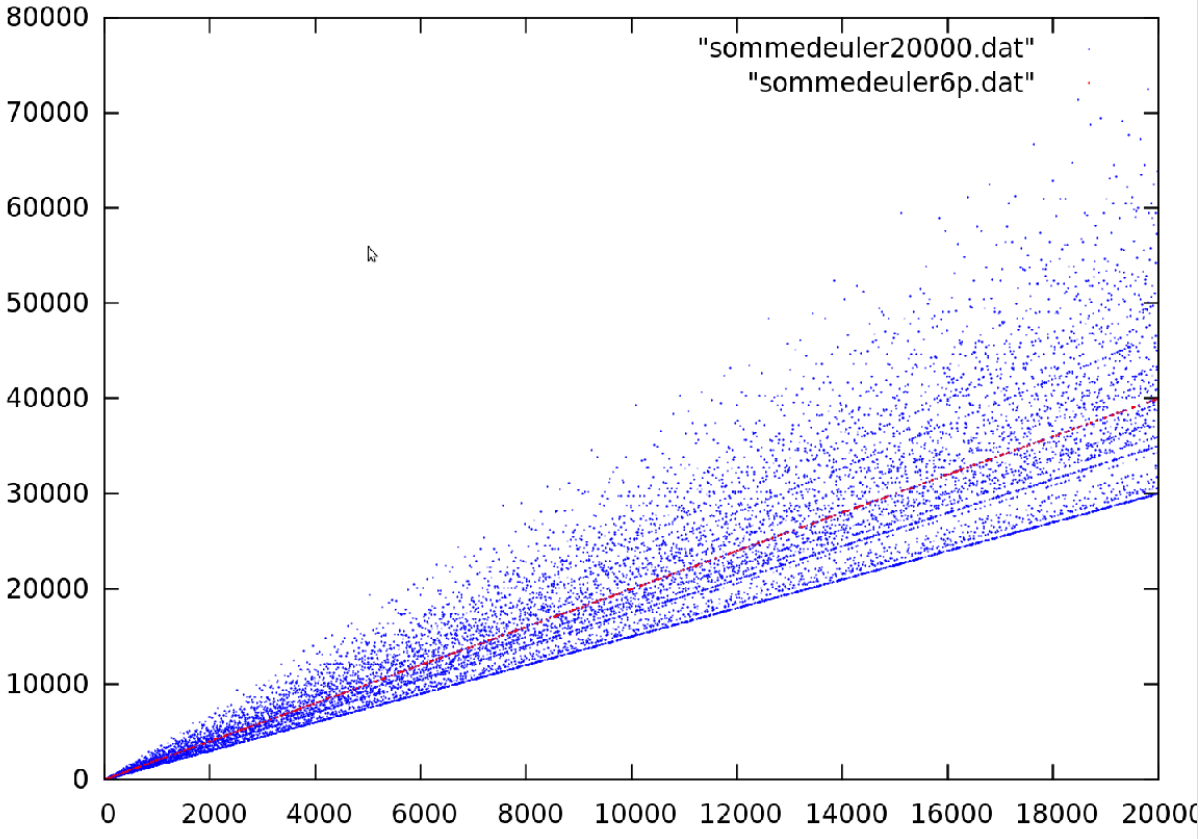


Fig. 15 : σ appliquée aux nombres de la forme $6p$

[H]

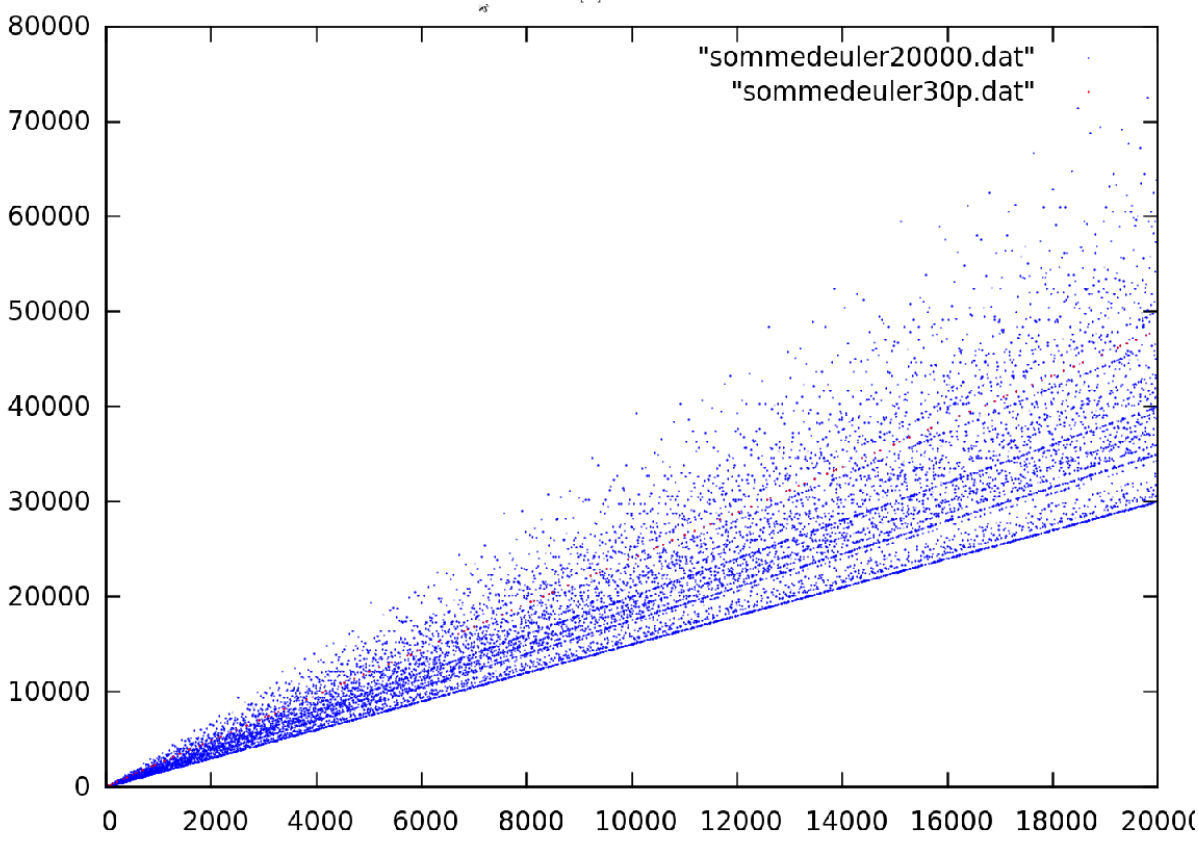


Fig. 16 : σ appliqué aux nombres de la forme $30p$

[H]

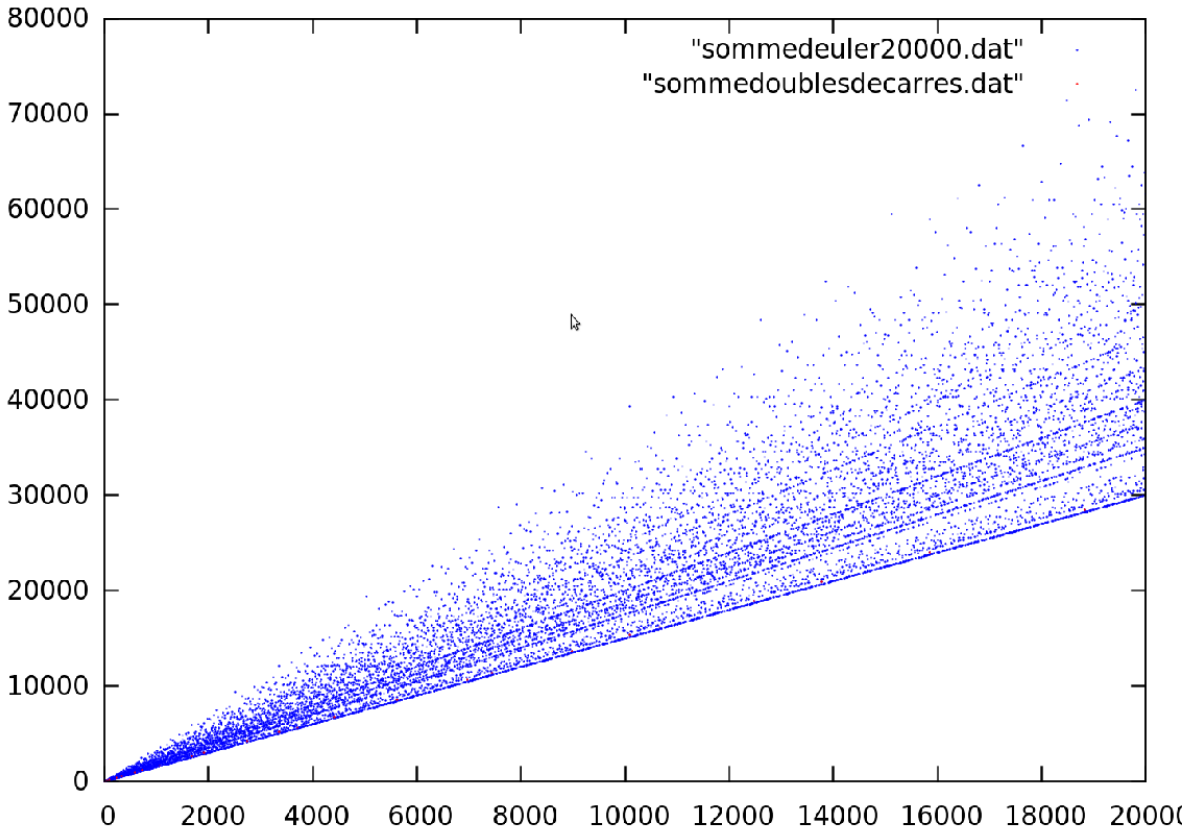


Fig. 17 : σ appliquée aux doubles de carrés de premiers

[H]

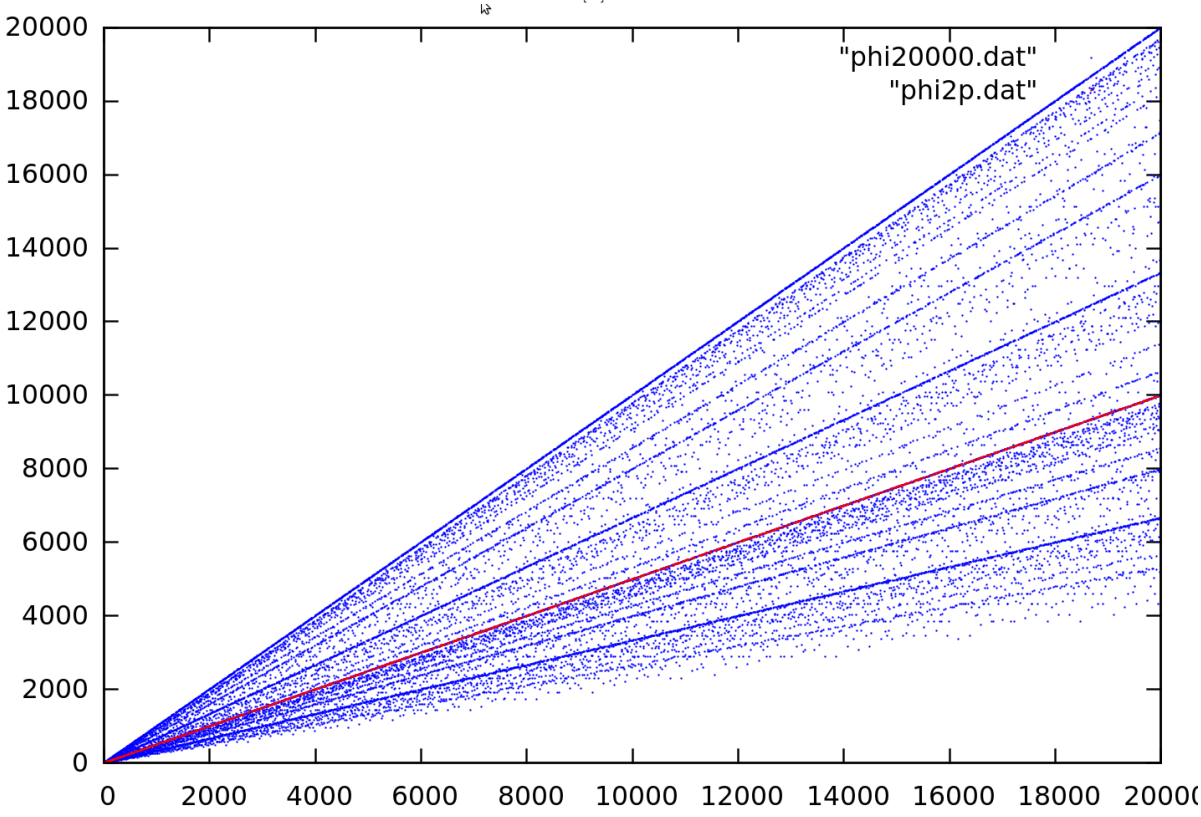


Fig. 18 : Indicateur d'Euler appliqué aux nombres de la forme $2p$ (doubles de premiers)

[H]

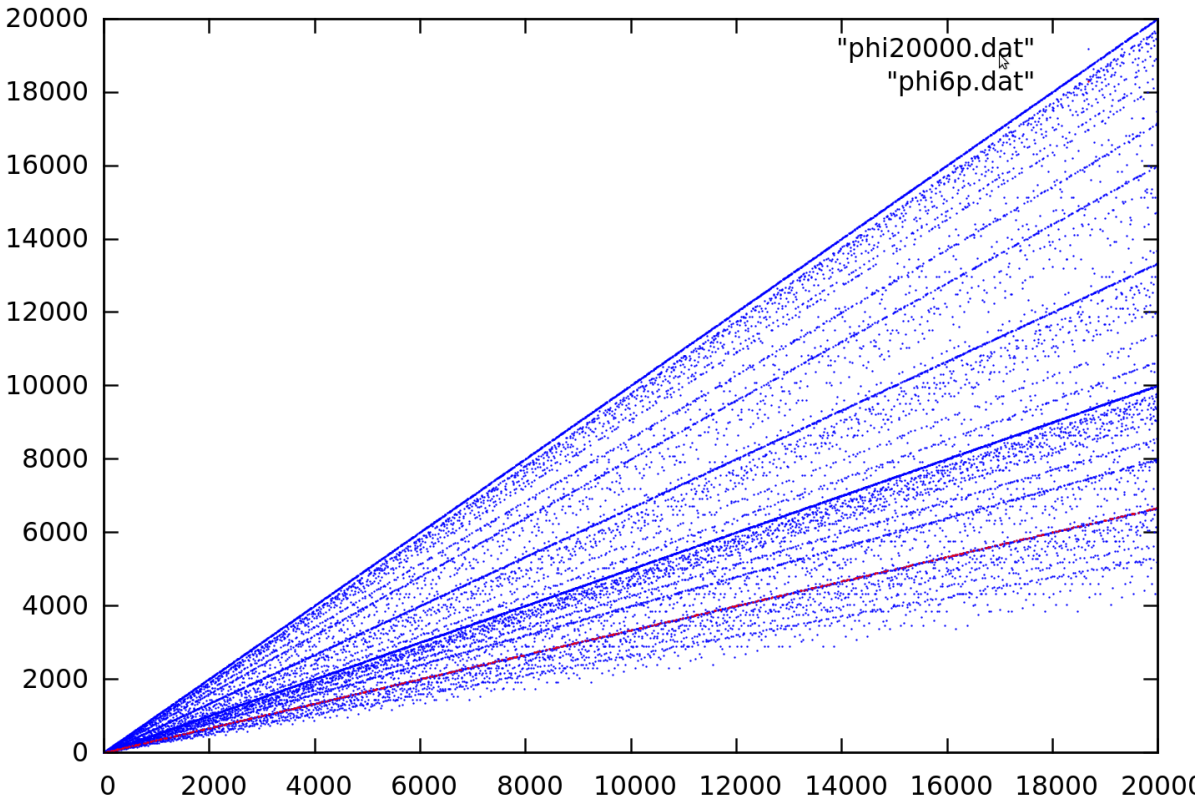


Fig. 19 : Indicateur d'Euler appliqué aux nombres de la forme $6p$

[H]

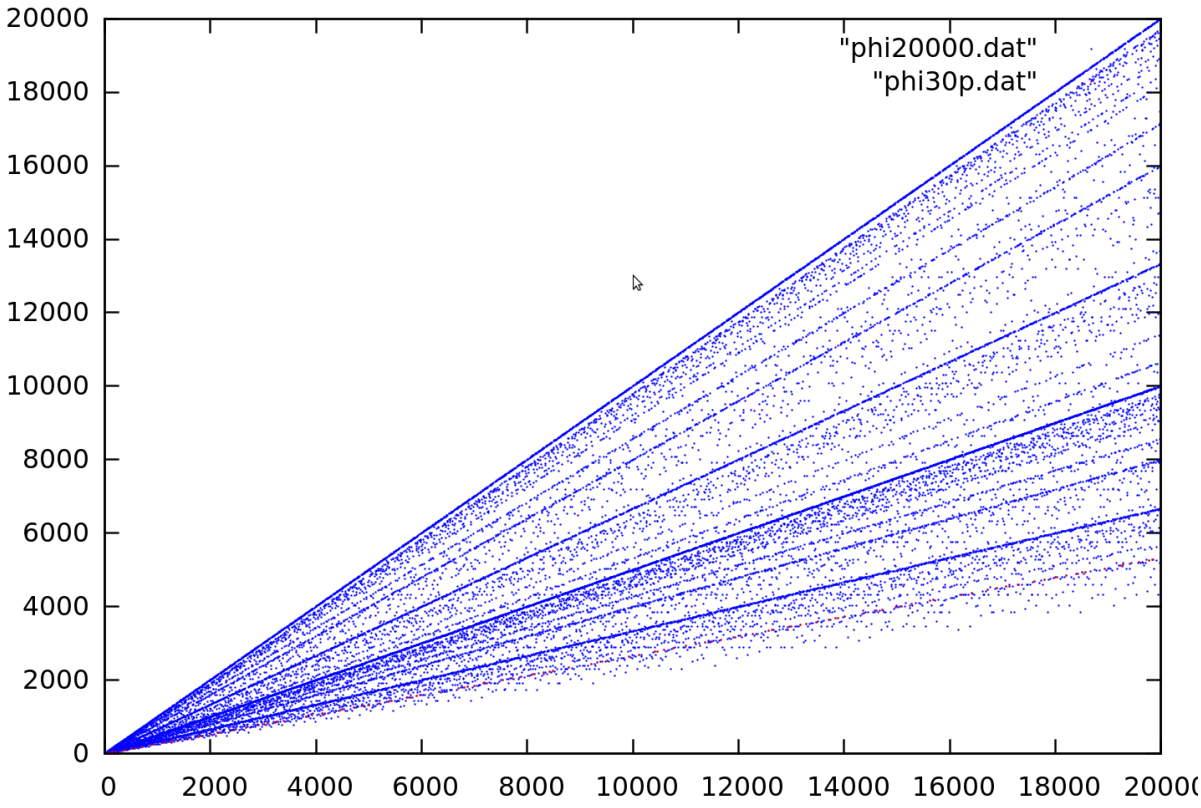


Fig. 20 : Indicateur d'Euler appliqué aux nombres de la forme $30p$

[H]

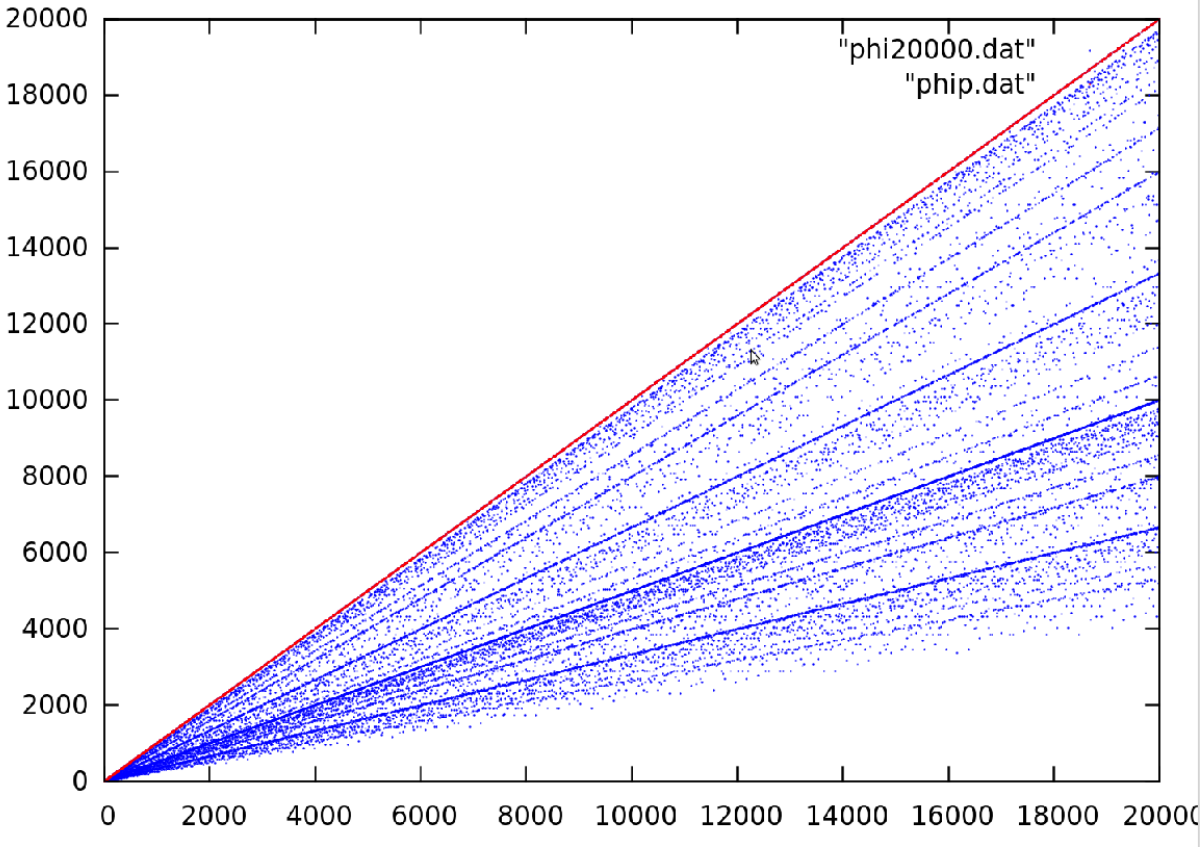


Fig. 21 : Indicateur d'Euler appliqué aux nombres premiers

[H]

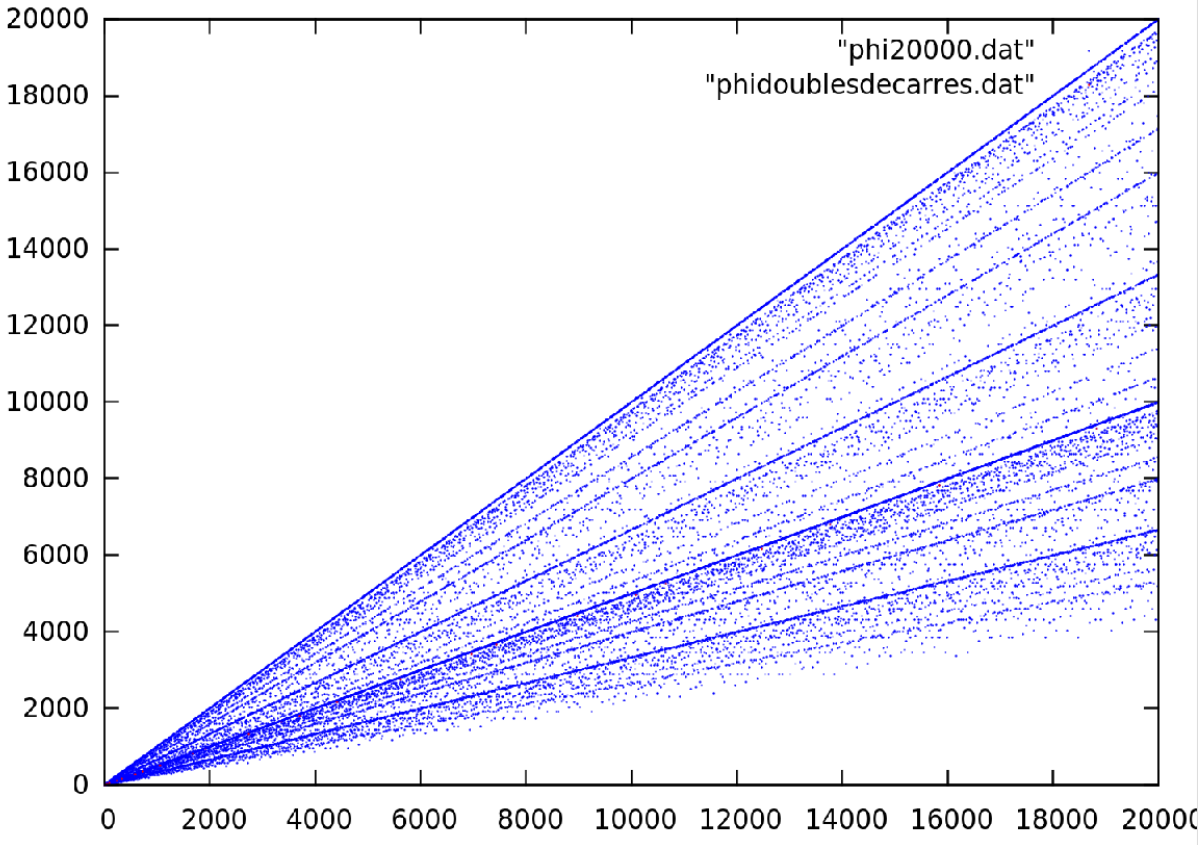


Fig. 22 : φ des doubles de carrés de premiers

[H]

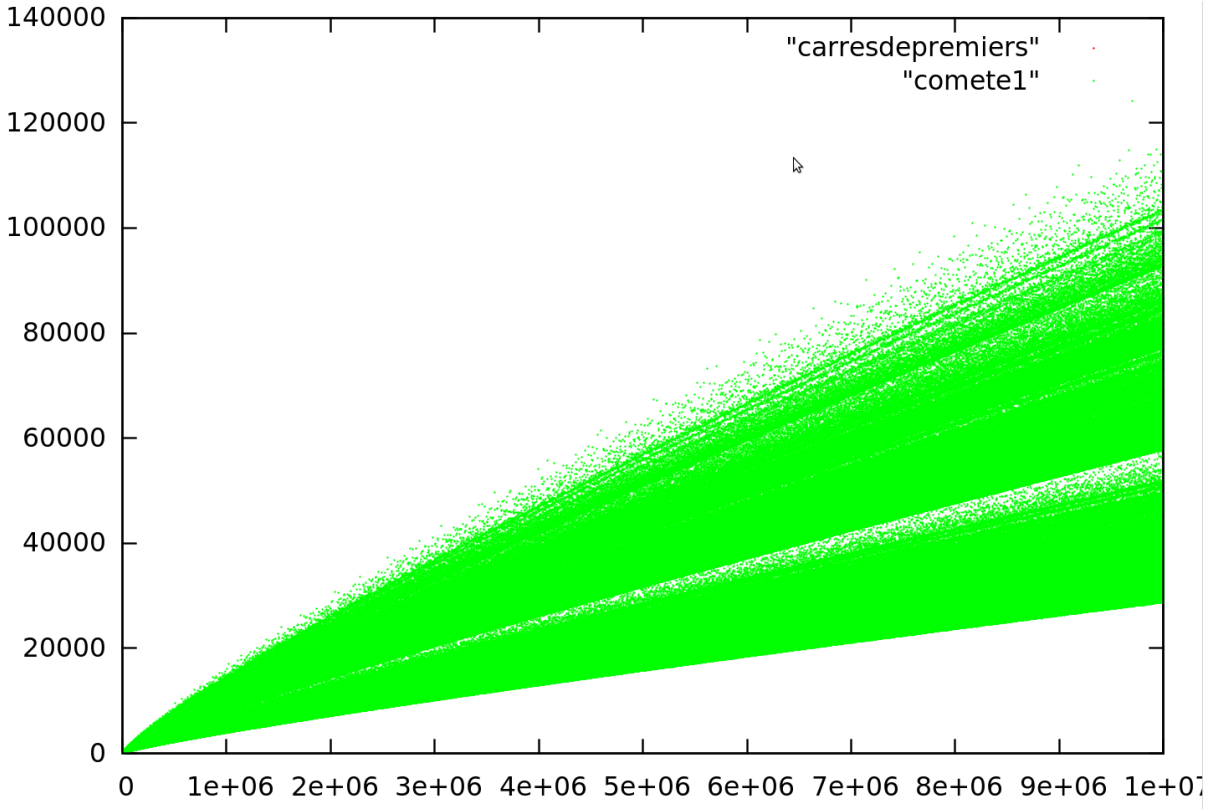


Fig. 23 : Nombres de décompositions de Goldbach sans tirages aléatoires

[H]

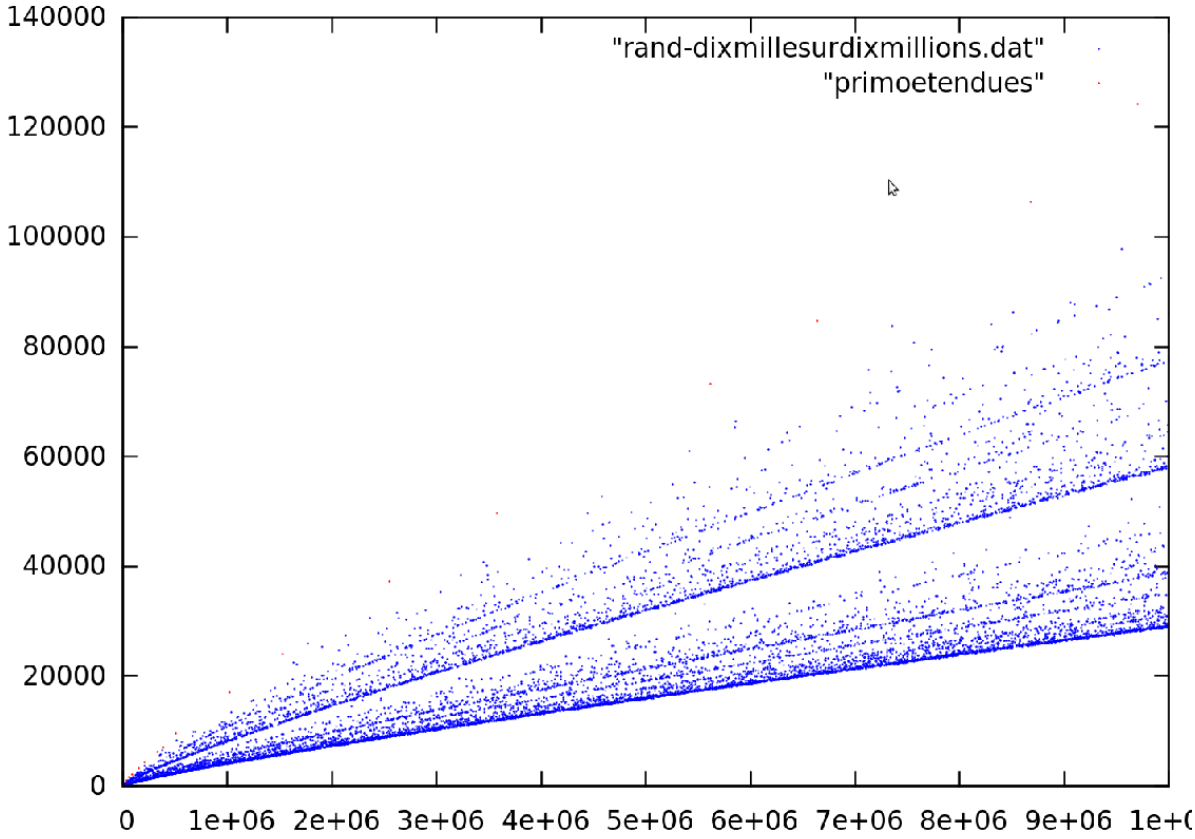


Fig. 24 : Nombres de décompositions de Goldbach des multiples de primorielles

[H]

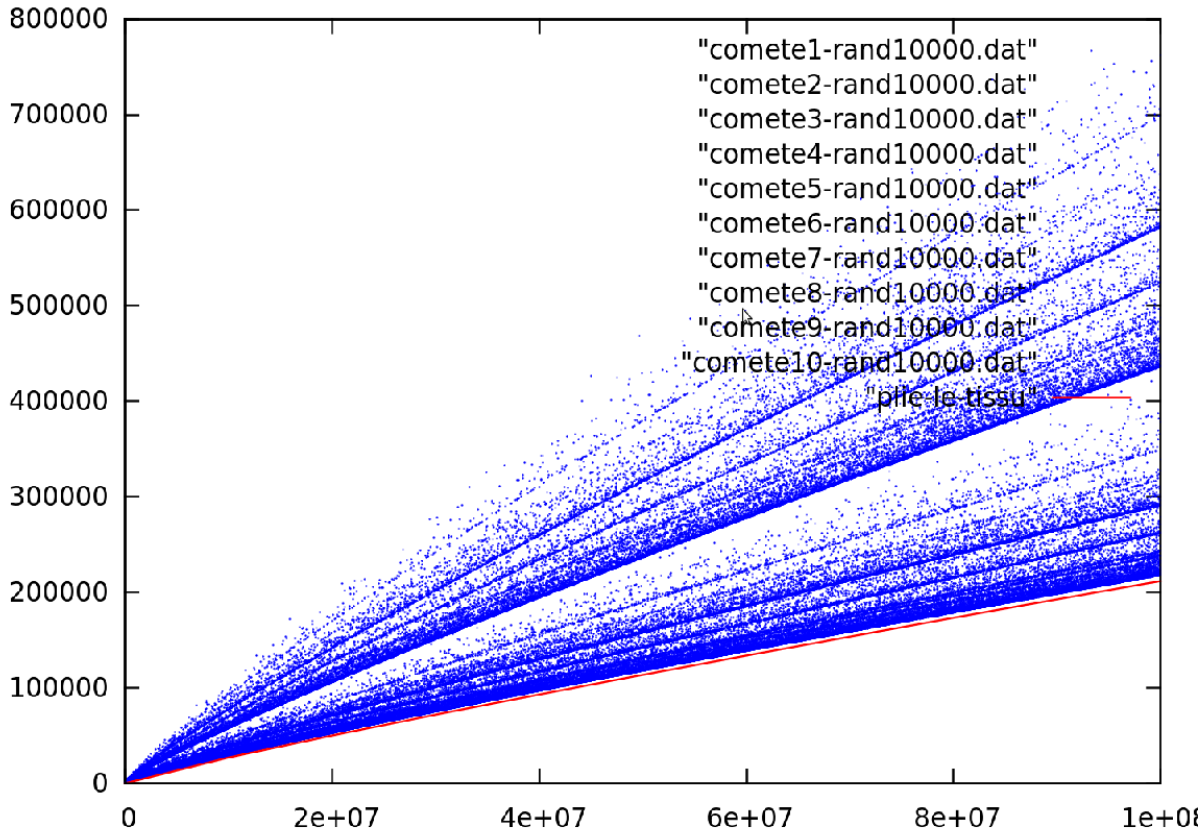


Fig. 25 : Minoration du nombre de décompositions de Goldbach

Quelques comètes : indicatrice d'Euler, somme des diviseurs, nombre de décompositions de Goldbach...

Denise Vella-Chemla

25 décembre 2010

1 Cinq comètes

Les cinq graphiques ci-dessous, obtenus avec gnuplot, présentent les fonctions :

- indicatrice d'Euler (φ),
- somme des diviseurs d'Euler (σ). Une formule de calcul par récurrence de cette somme est fournie dans l'article "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs". Nous avons utilisé pour la calculer une autre formule de récurrence, fournie par Dominique Giard sur la toile dans la séquence A000203 de l'Encyclopédie en ligne des séquences d'entiers (OEIS),
- nombre de diviseurs,
- nombre de décompositions de Goldbach, i.e. nombre de façons différentes d'écrire un nombre pair $2n$ comme somme de deux nombres premiers.
- plus petit décomposant de Goldbach, i.e. associe à $2n$ le plus petit nombre premier p tel que $2n = p+q$ avec p et q premiers,
- et enfin, plus grand décomposant de Goldbach, i.e. associe à $2n$ le plus grand nombre premier inférieur ou égal à n p tel que $2n = p + q$ avec p et q premiers,

Toutes ces visualisations ont pu être réalisées grâce à des outils spécifiques fournis par Daniel Diaz, concepteur de Gnu-Prolog, que l'on remercie vivement.

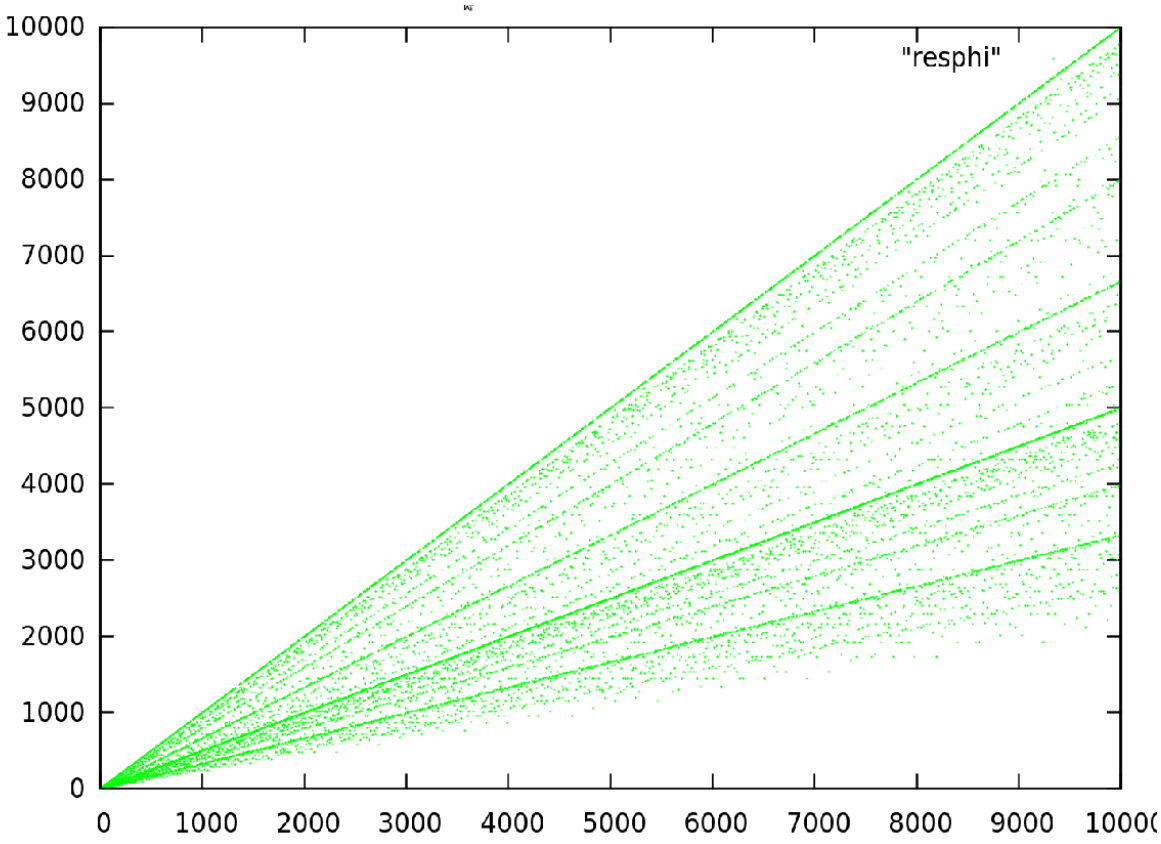


Fig. 1 : Indicateur d'Euler

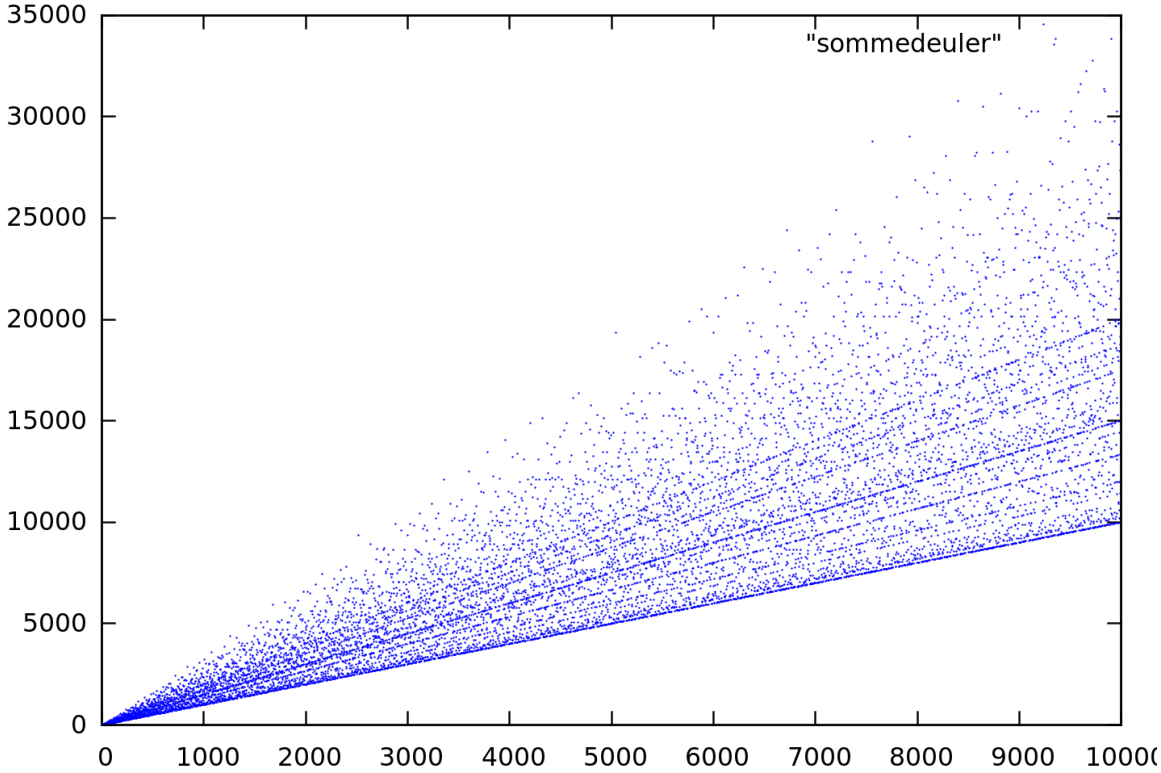


Fig. 2 : Somme des diviseurs

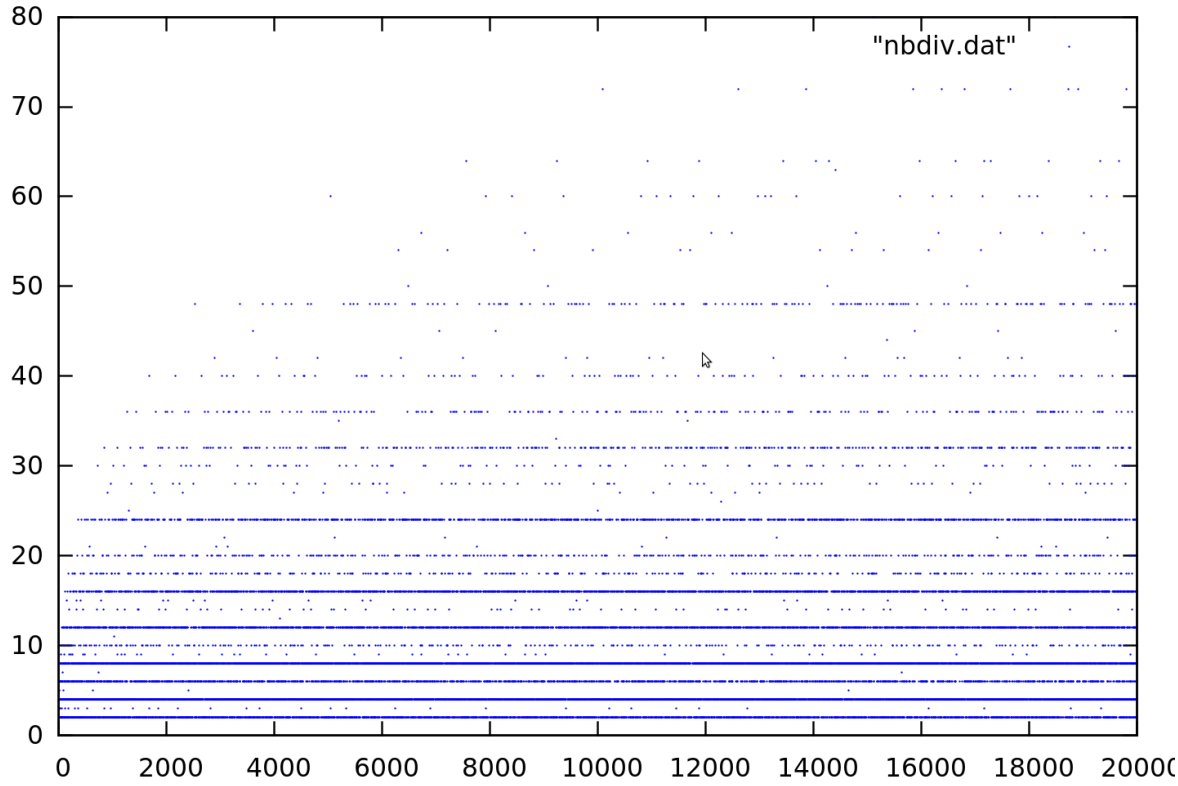


Fig. 3 : Nombre de diviseurs

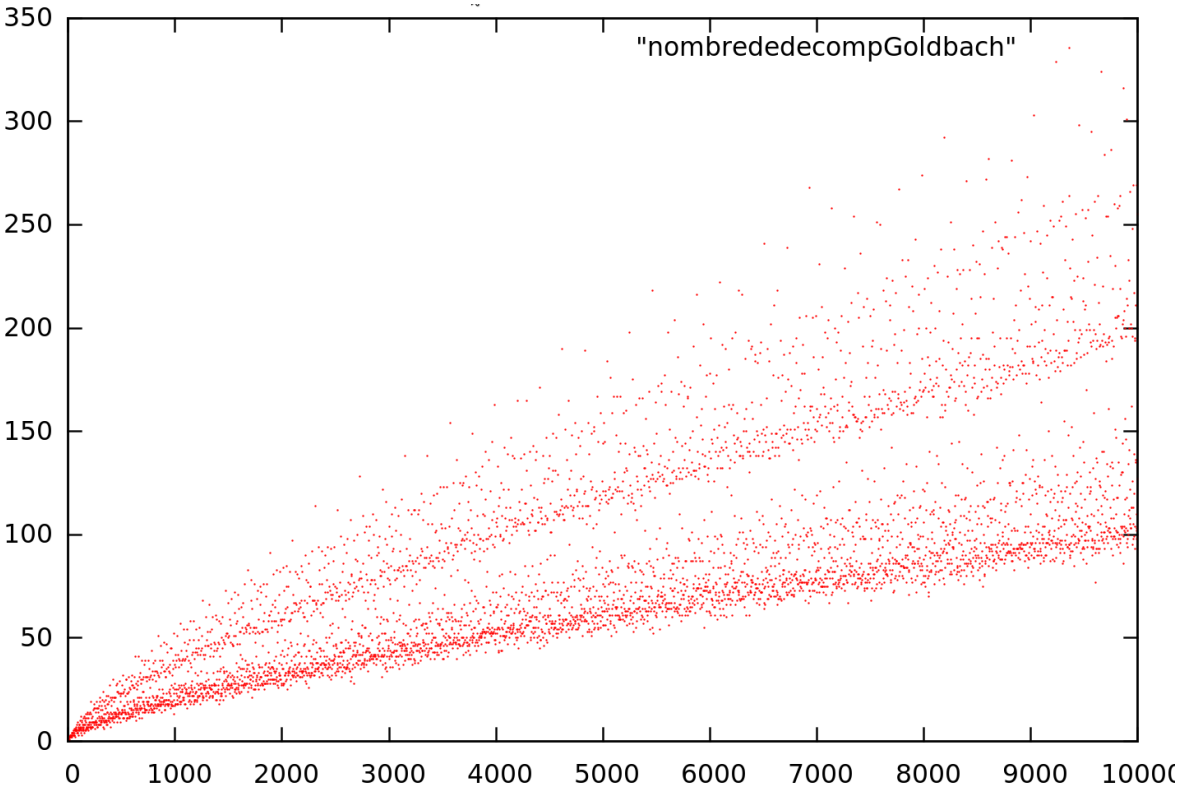


Fig. 4 : Nombre de décompositions de Goldbach

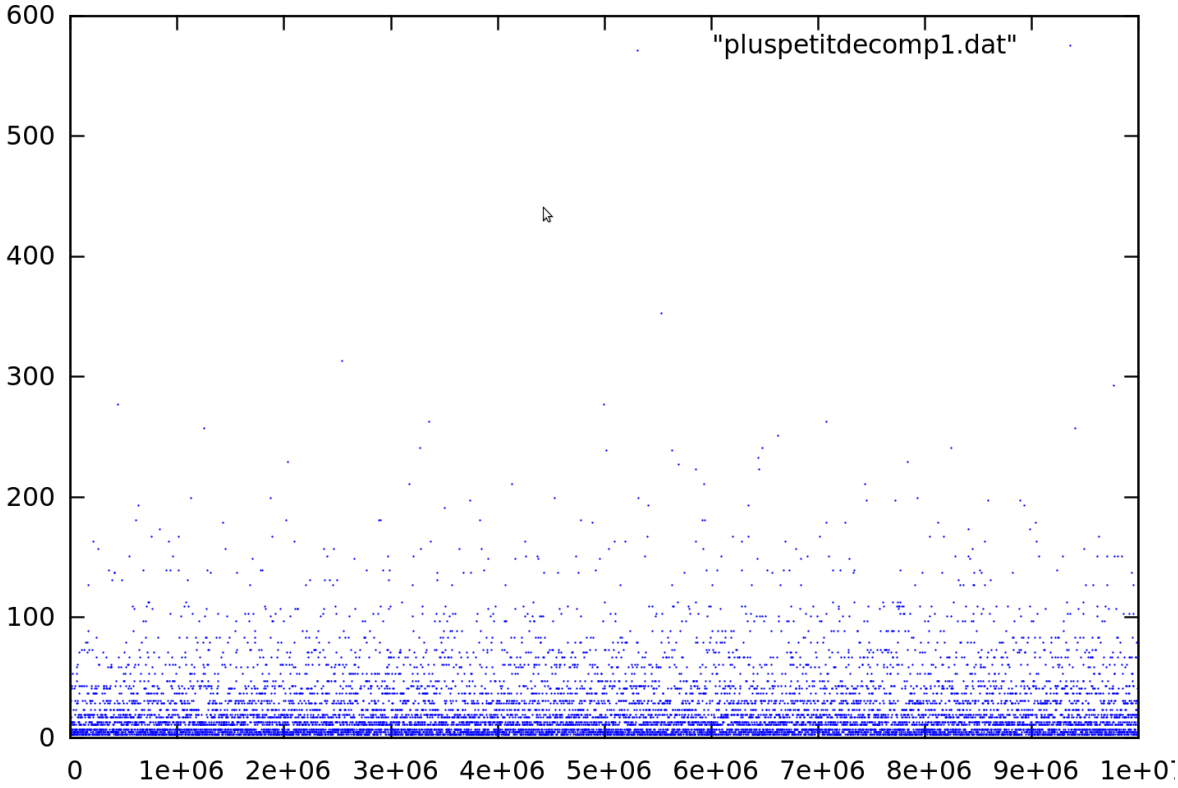


Fig. 5 : Plus petit nombre premier intervenant dans une décomposition de Goldbach

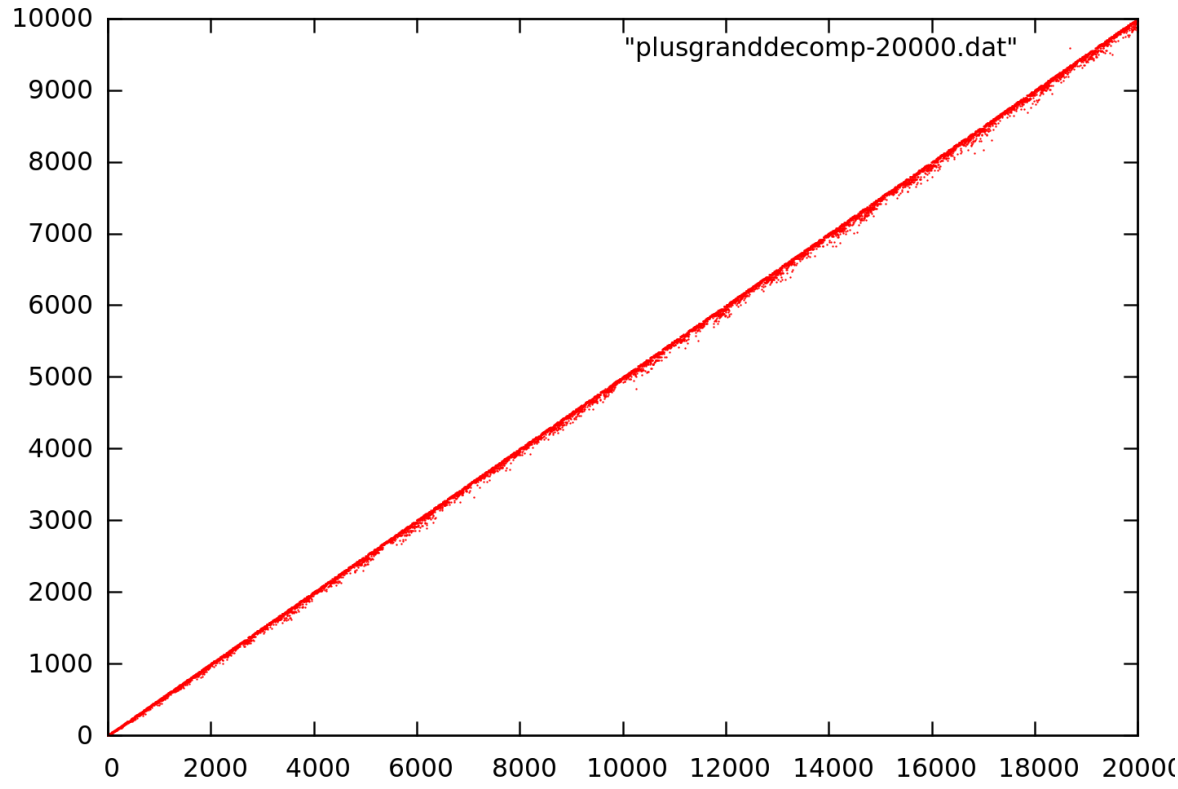


Fig. 6 : Plus grand nombre premier intervenant dans une décomposition de Goldbach

On constate que la comète de la fonction φ semble comme inversée par rapport aux comètes de σ ou *Goldbach*, des bandes de points plus concentrés apparaissant “à l’intérieur” de la comète, la “première” d’entre elles se trouvant “tout en haut” de la comète.

Les deux comètes de σ et *Nombre_de_décompositions_de_Goldbach* semblent présenter une structure similaire, même si l'apparence de celle de la somme des diviseurs est plus linéaire que celle du nombre des décompositions de Goldbach. Si on ramène les trois premières comètes sur un même graphique, la comète des nombres de décompositions de Goldbach se retrouve tout en bas, comme écrasée, car ses valeurs sont bien moindres que celles des deux autres comètes.

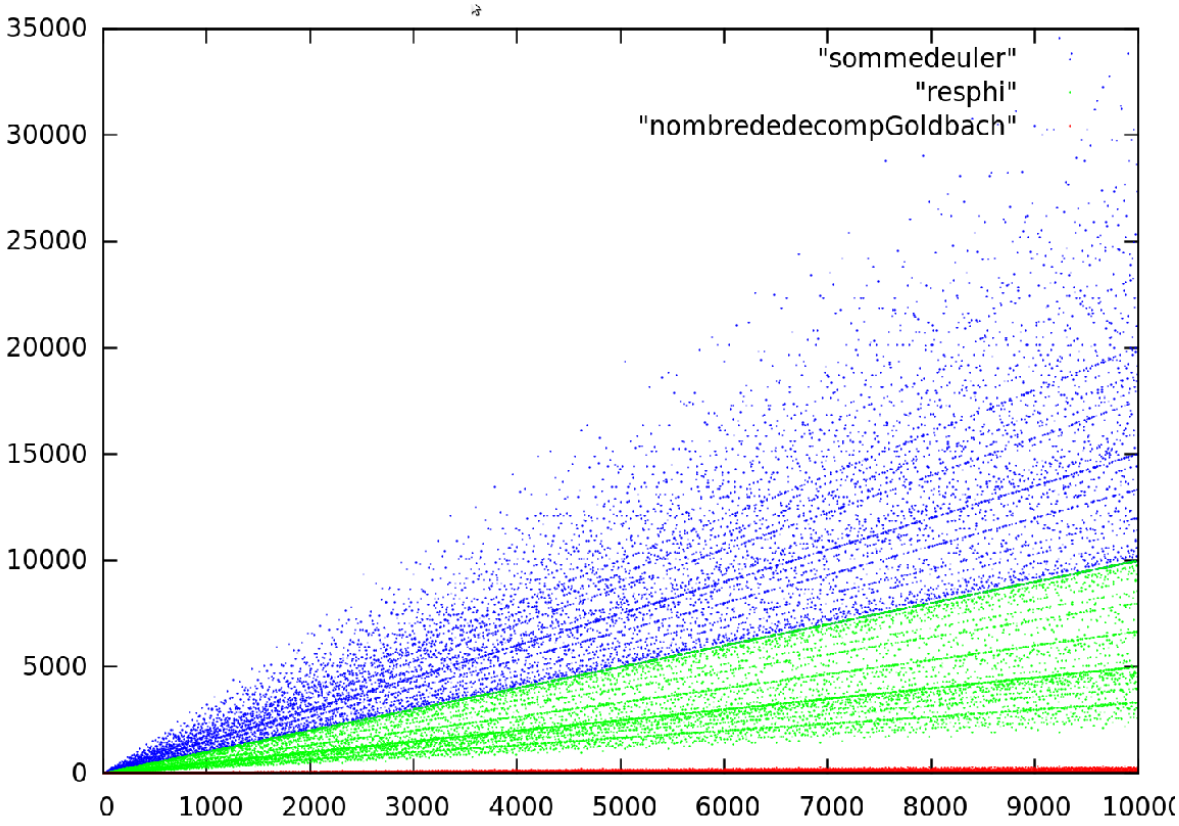


Fig. 7 : σ, φ et Nombre de décompositions de Goldbach

On constate que les comètes associées au nombre de diviseurs et au plus petit décomposant de Goldbach se “ressemblent”. Visualisons-les sur un même graphique, la figure 8 :

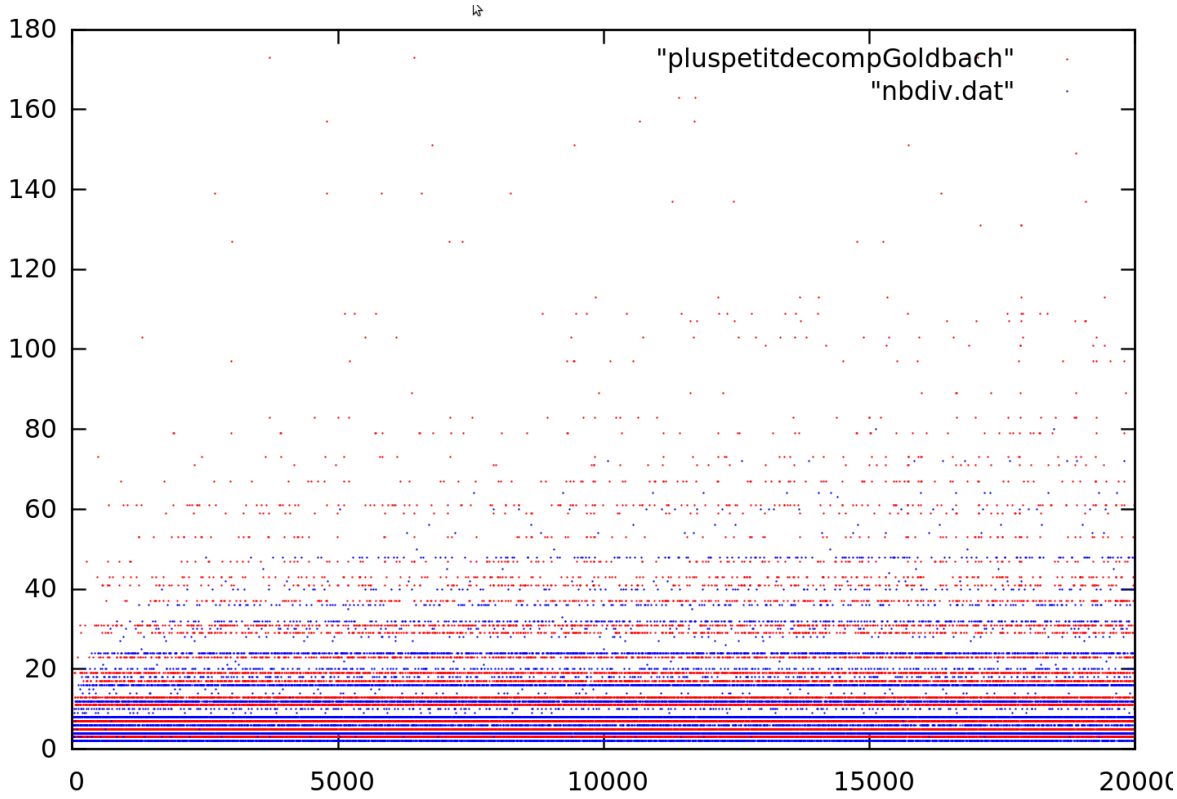


Fig. 8 : Plus petit nombre premier intervenant dans une décompositon de Goldbach et nombre de diviseurs

2 Mathématiques expérimentales

Dans la comète de Goldbach, on réussit à isoler les lignes de concentration des points qui correspondent aux nombres de décompositions de Goldbach des nombres de la forme $2p$, $6p$, $30p$, soit plus globalement $2kp$ avec p premier.

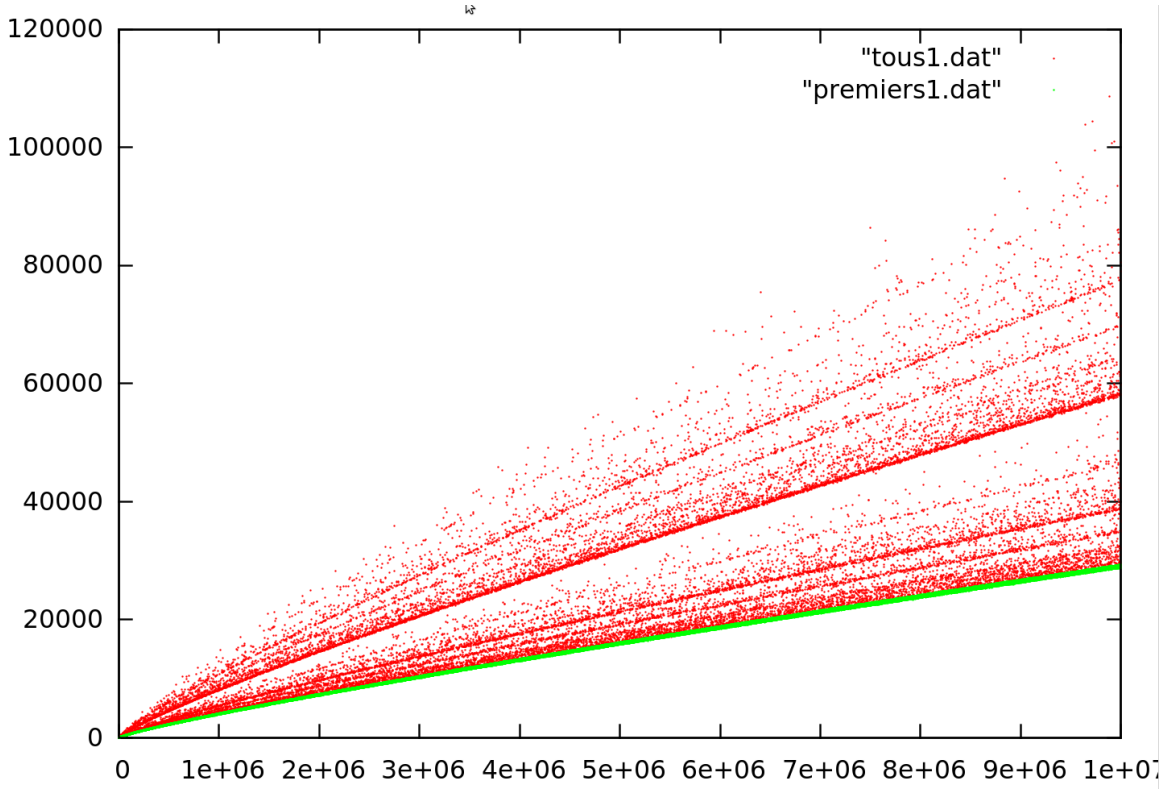


Fig. 9 : Nombre de décompositions de Goldbach des nombres de la forme $2p$ (doubles de premiers)

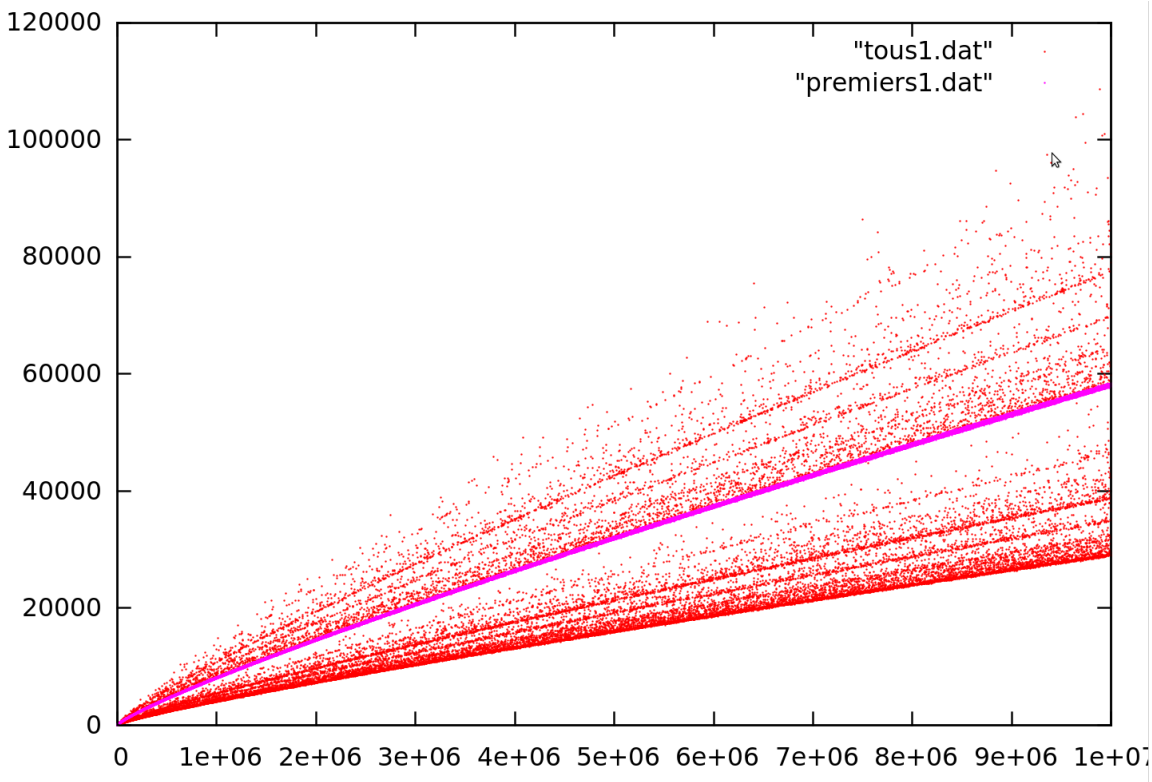


Fig. 10 : Nombre de décompositions de Goldbach des nombres de la forme $6p$

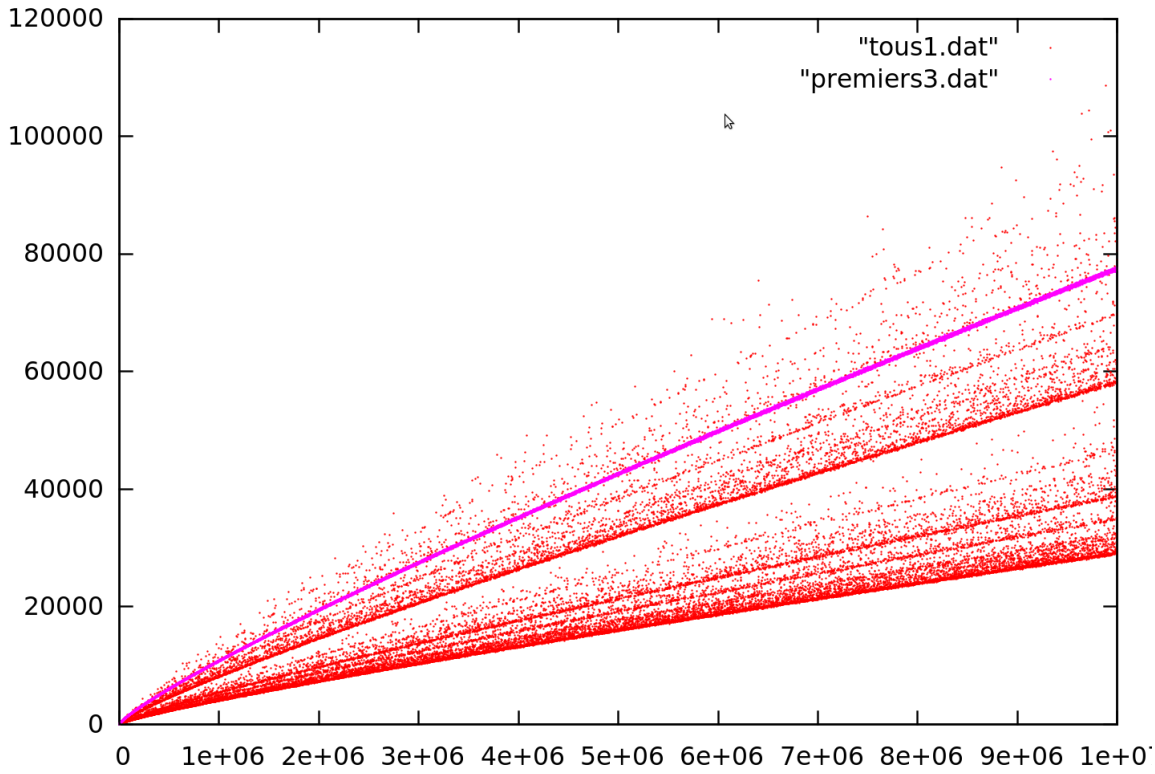


Fig. 11 : Nombre de décompositions de Goldbach des nombres de la forme $30p$

On pense qu'on obtiendra également certaines concentrations de points par l'élévation à la puissance des nombres premiers. C'est ce que l'on constate sur la visualisation ci-après : les décompositions de Goldbach des nombres de la forme $2p^2$ avec p premier par exemple, se trouvent également dans la tige basse de la gerbe.

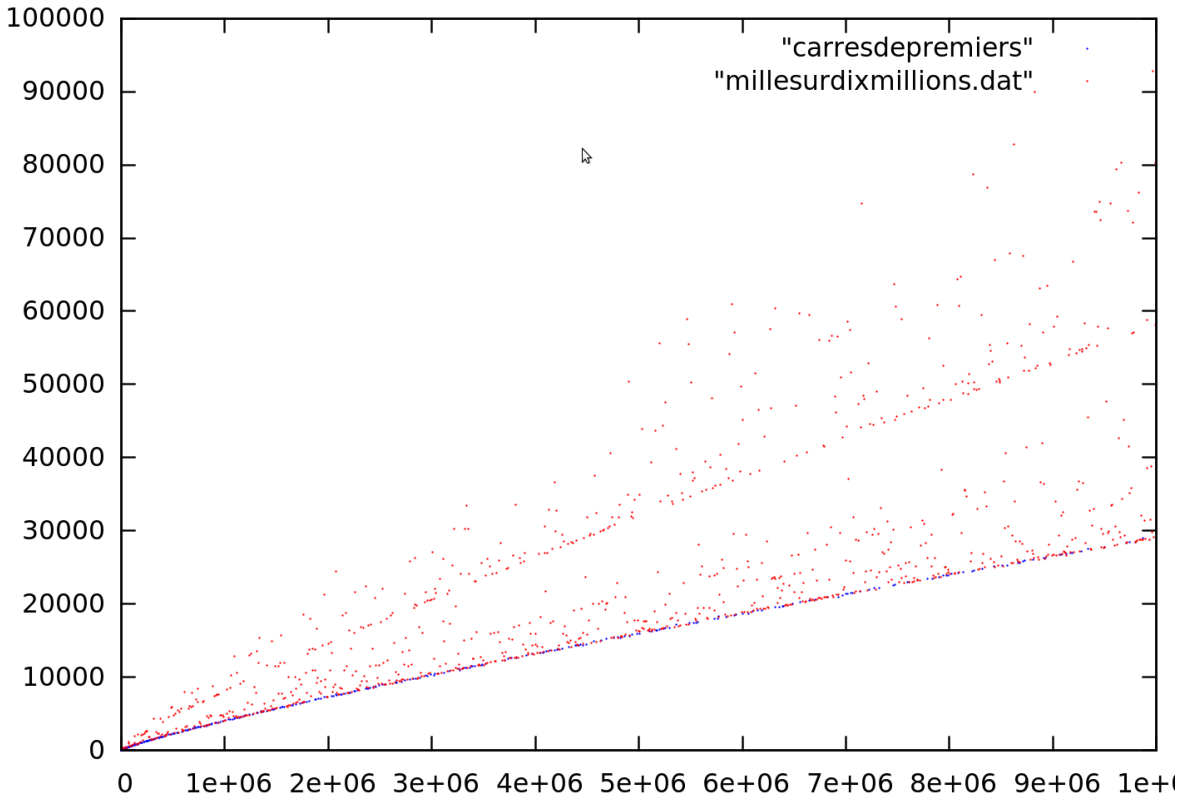


Fig. 12 : Les nombres de décompositions de Goldbach des doubles de carrés de premiers sont sur la première tige de concentration de points.

Quant aux décompositions de Goldbach des nombres de la forme $2p^3$ avec p premier par exemple, ils semblent se trouver sur les mêmes tiges que les nombres de la forme $2p$ ou $6p$ mais il faudrait le confirmer. Sur le graphique en figure 13, on voit les douze points rouges correspondant aux nombres de décompositions des doubles de cubes[1].

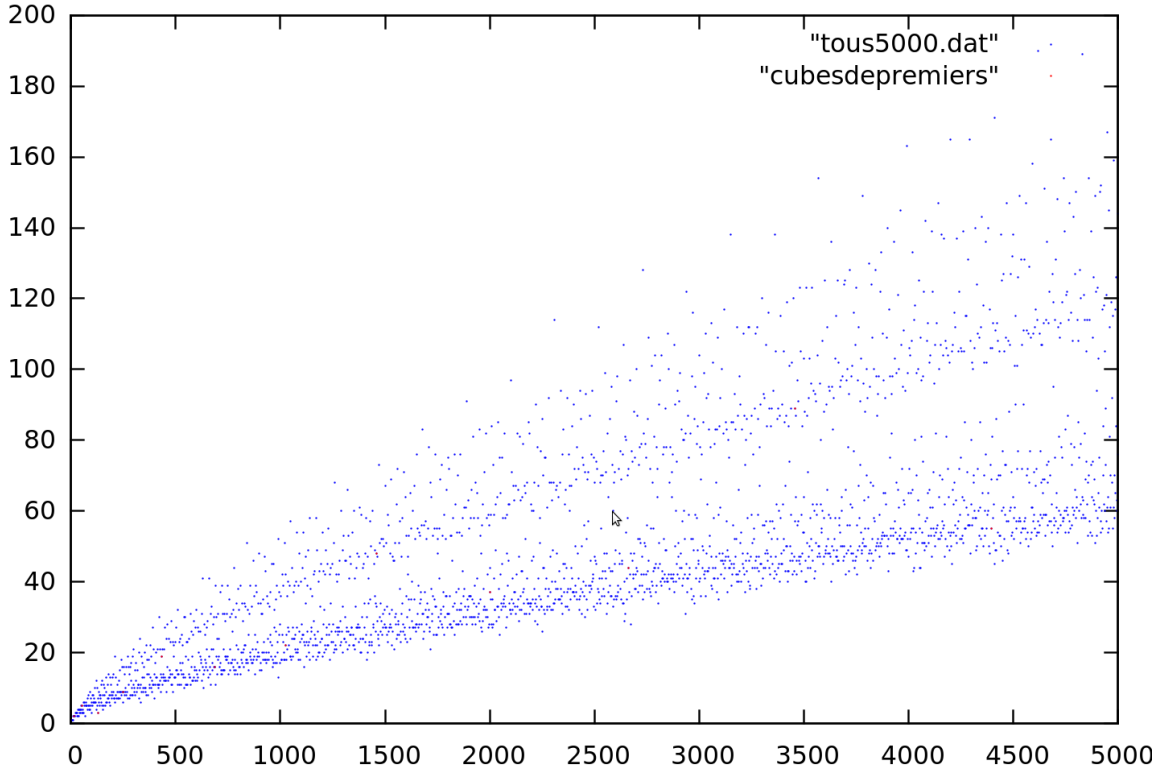


Fig. 13 : Les doubles de cubes de premiers sont sur la deuxième tige de concentration de points.

Dans la comète de la somme des diviseurs d'Euler, on réussit à reproduire les mêmes concentrations de points qui correspondent aux sommes des diviseurs des nombres de la forme $2p$, $6p$, $30p$, soit plus globalement $2kp$ avec p premier.

[1] Il n'y a que 12 petits points rouges à retrouver sur la tige des $2p$ et sur celle des $6p$ en s'arrachant un peu les yeux mais les zooms-écrans permettent de les retrouver aisément.

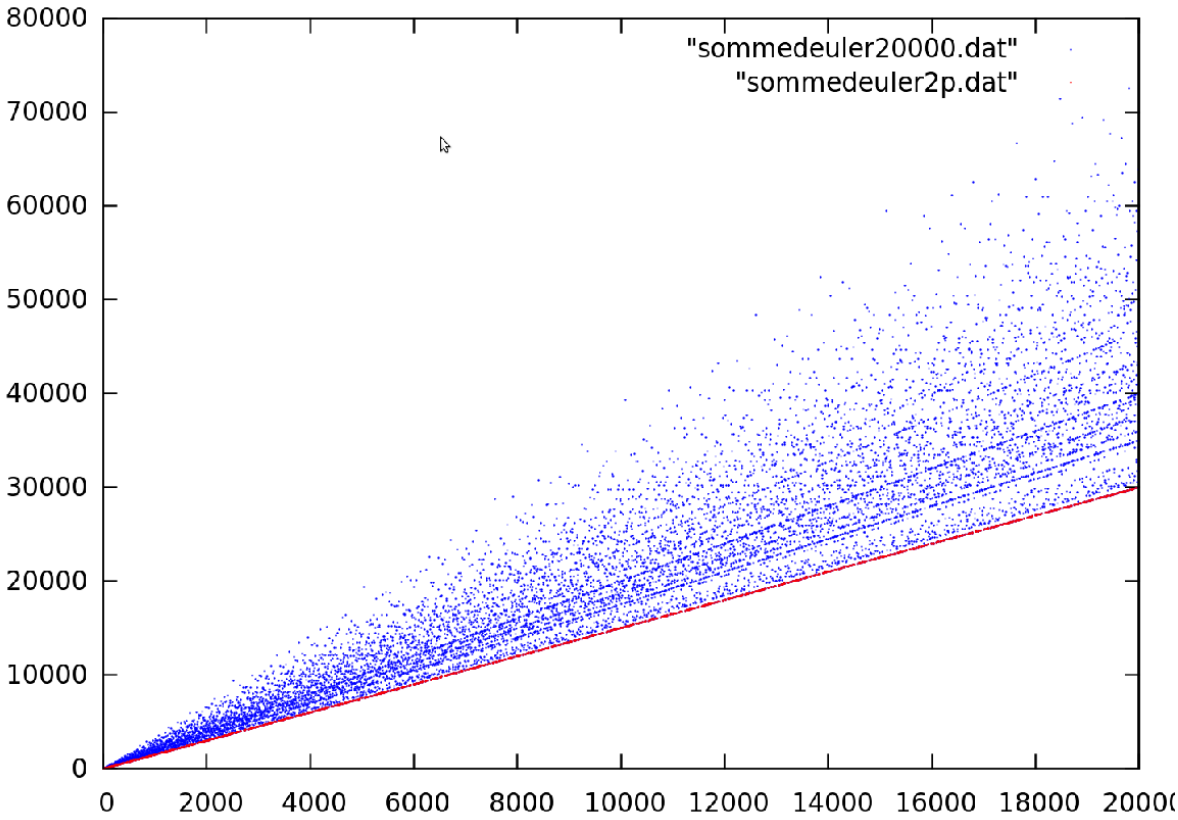


Fig. 14 : σ appliquée aux nombres de la forme $2p$ (doubles de premiers)

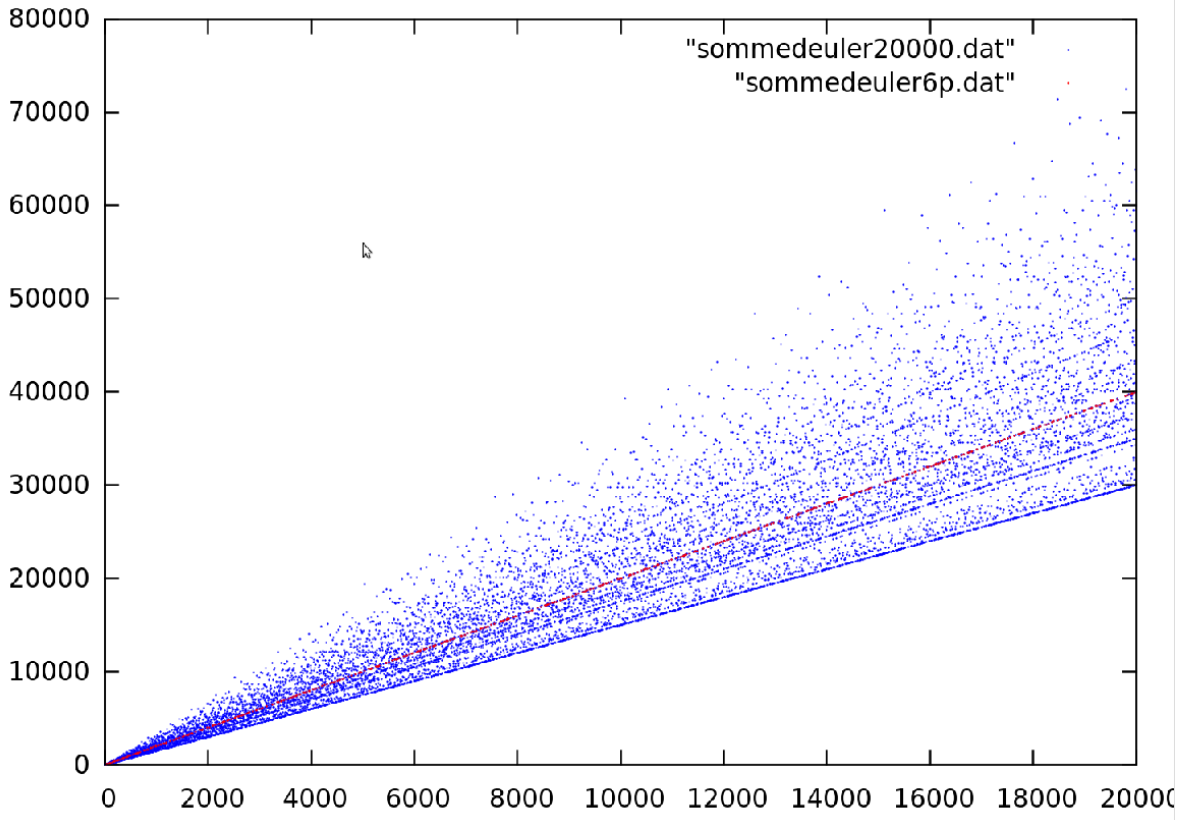


Fig. 15 : σ appliquée aux nombres de la forme $6p$

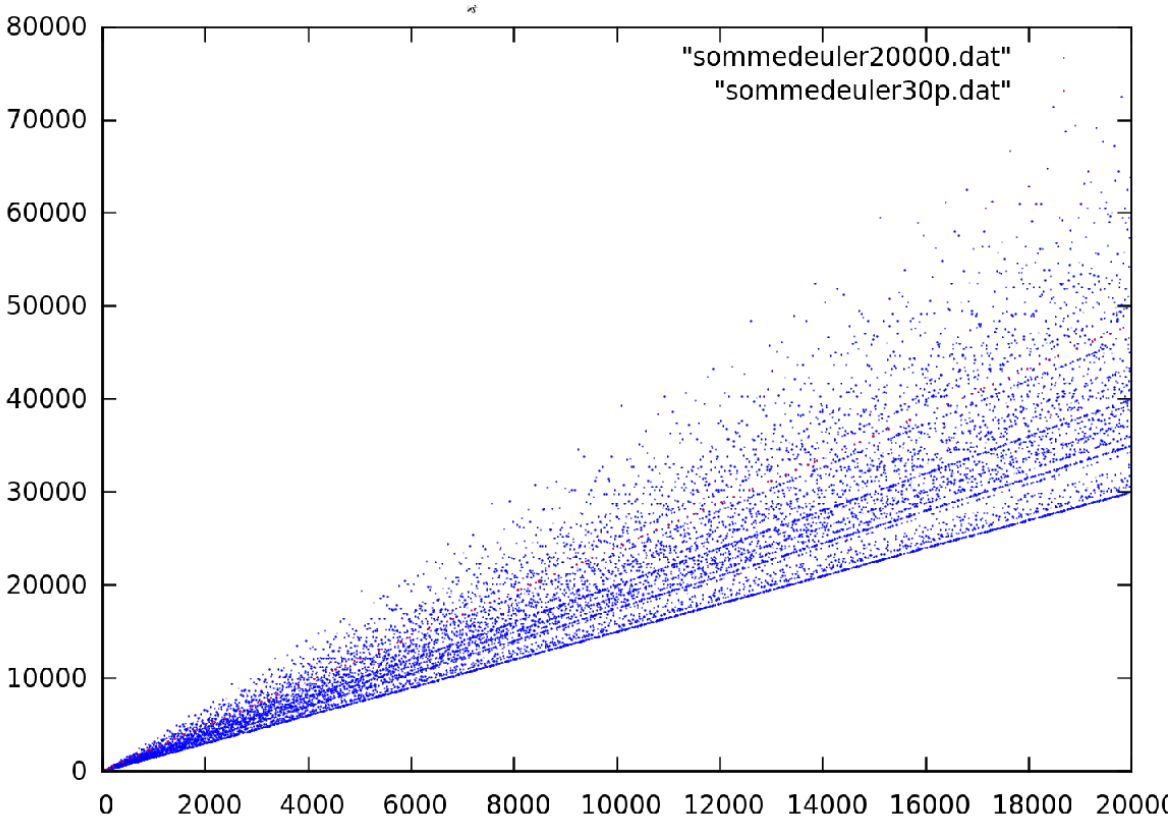


Fig. 16 : σ appliqué aux nombres de la forme $30p$

On reproduit également la concentration de points par l'élévation au carré des nombres premiers. C'est ce que l'on constate sur la visualisation ci-après : les sommes des diviseurs des nombres de la forme $2p^2$ avec p premier par exemple, se trouvent également dans la tige basse de la gerbe[2].

[2]Il n'y a que 25 petits points rouges à retrouver sur la tige basse ; à nouveau, les zoom-écrans ne laissent pas de place au doute...

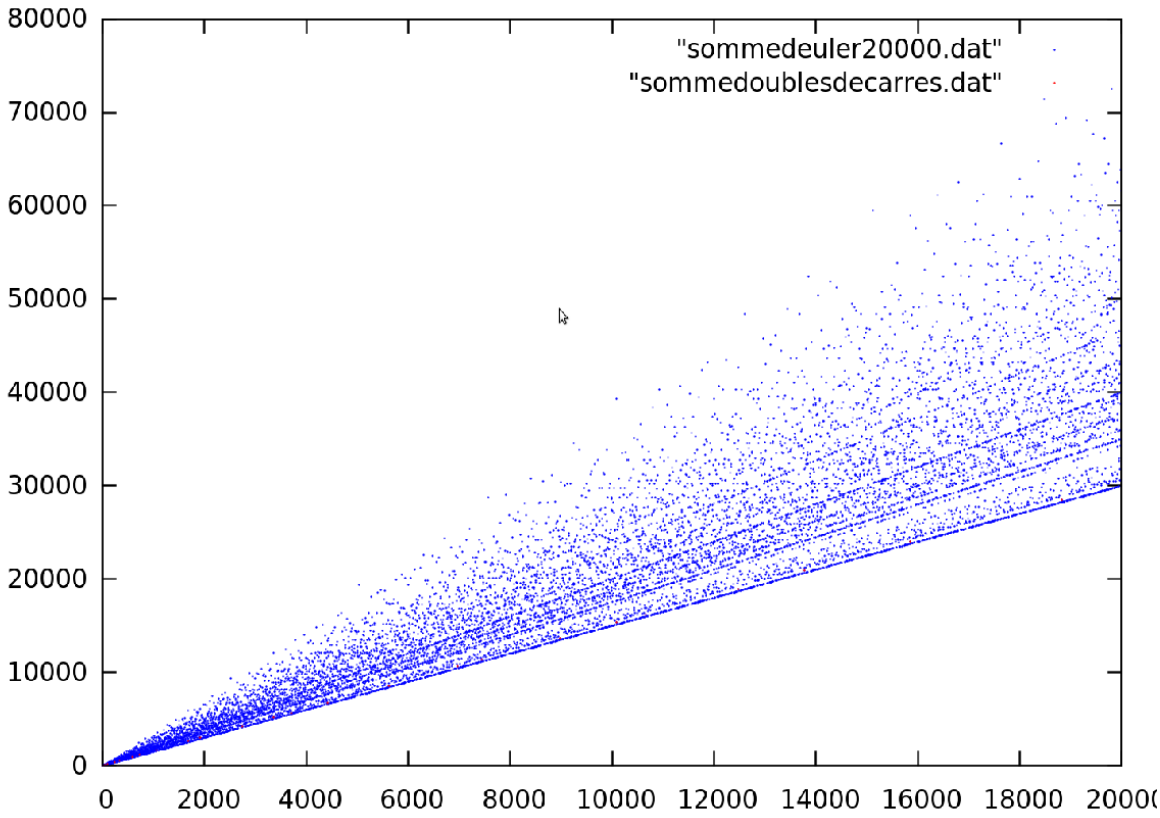


Fig. 17 : σ appliquée aux doubles de carrés de premiers

Dans la comète de l'indicatrice d'Euler, on réussit à produire des concentrations de points qui correspondent aux sommes des diviseurs des nombres de la forme $2p$, $6p$, $30p$, soit plus globalement $2kp$ avec p premier (les $2p$ sont à peu près au milieu de la comète, les $6p$ plus bas et les $30p$ encore plus bas).

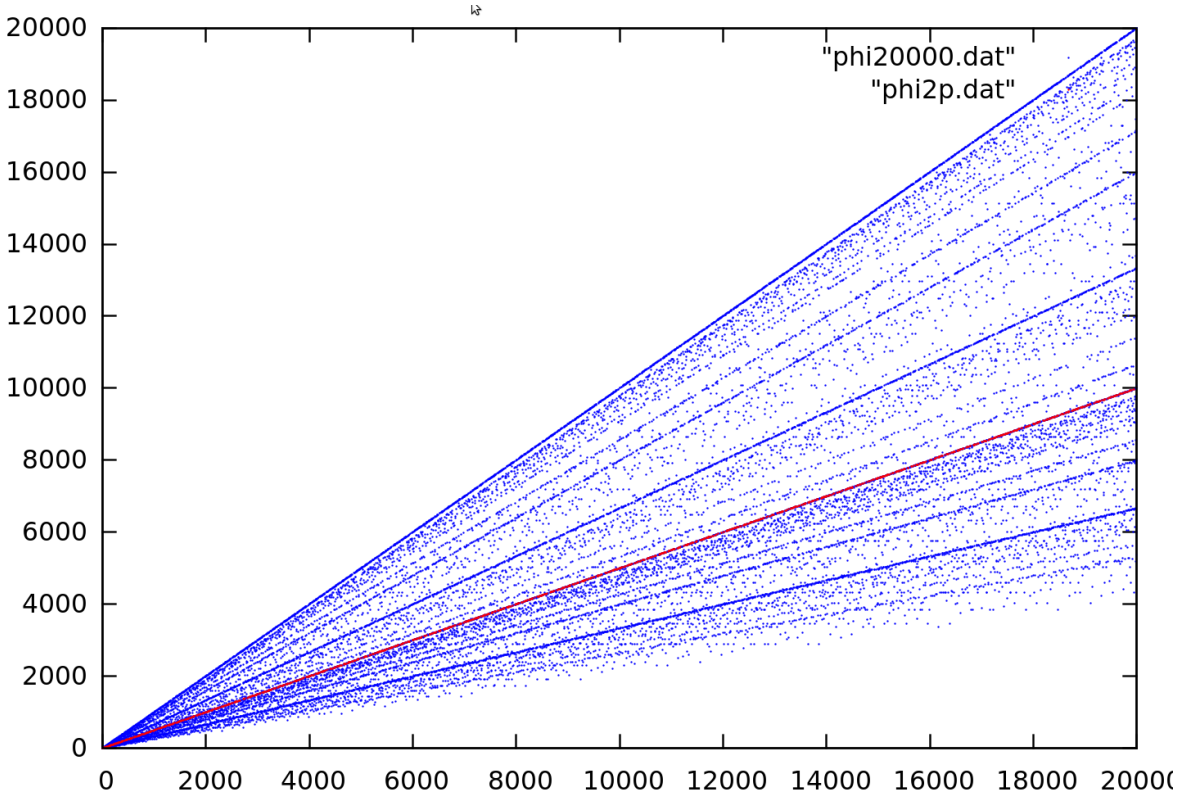


Fig. 18 : Indicateur d'Euler appliqué aux nombres de la forme $2p$ (doubles de premiers)

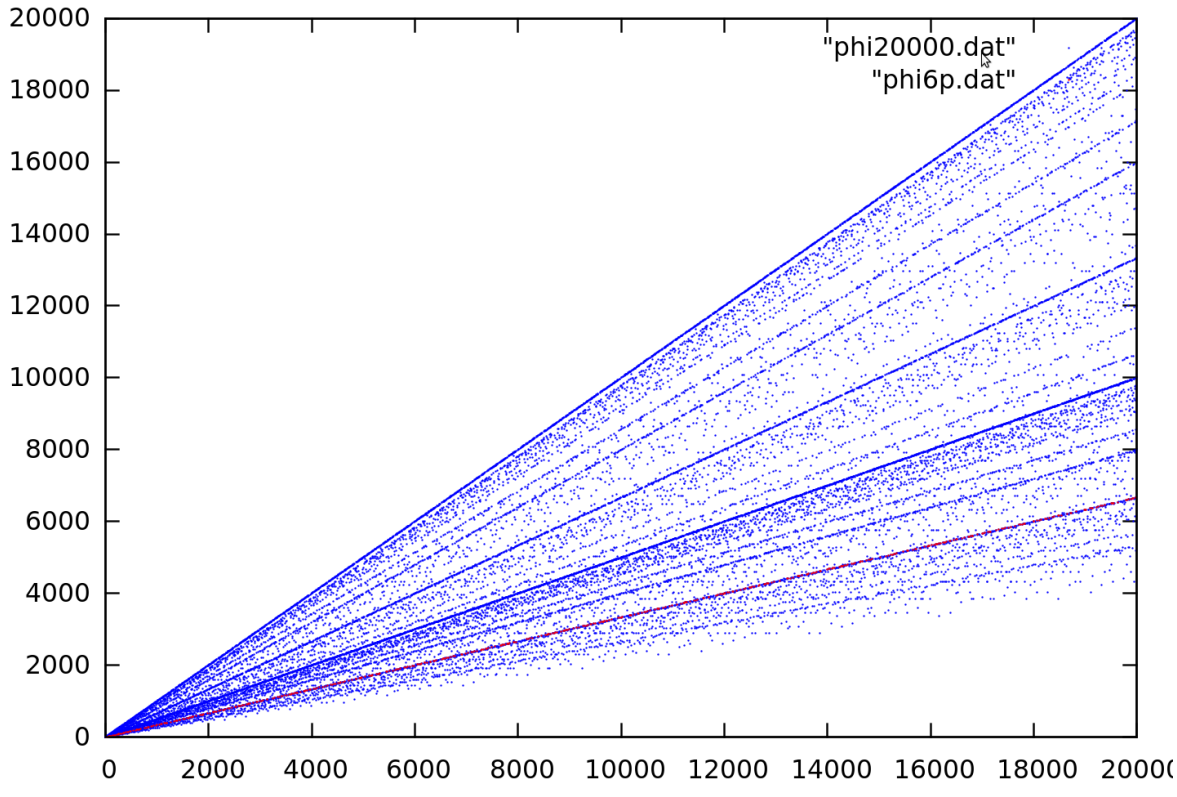


Fig. 19 : Indicateur d'Euler appliqué aux nombres de la forme $6p$

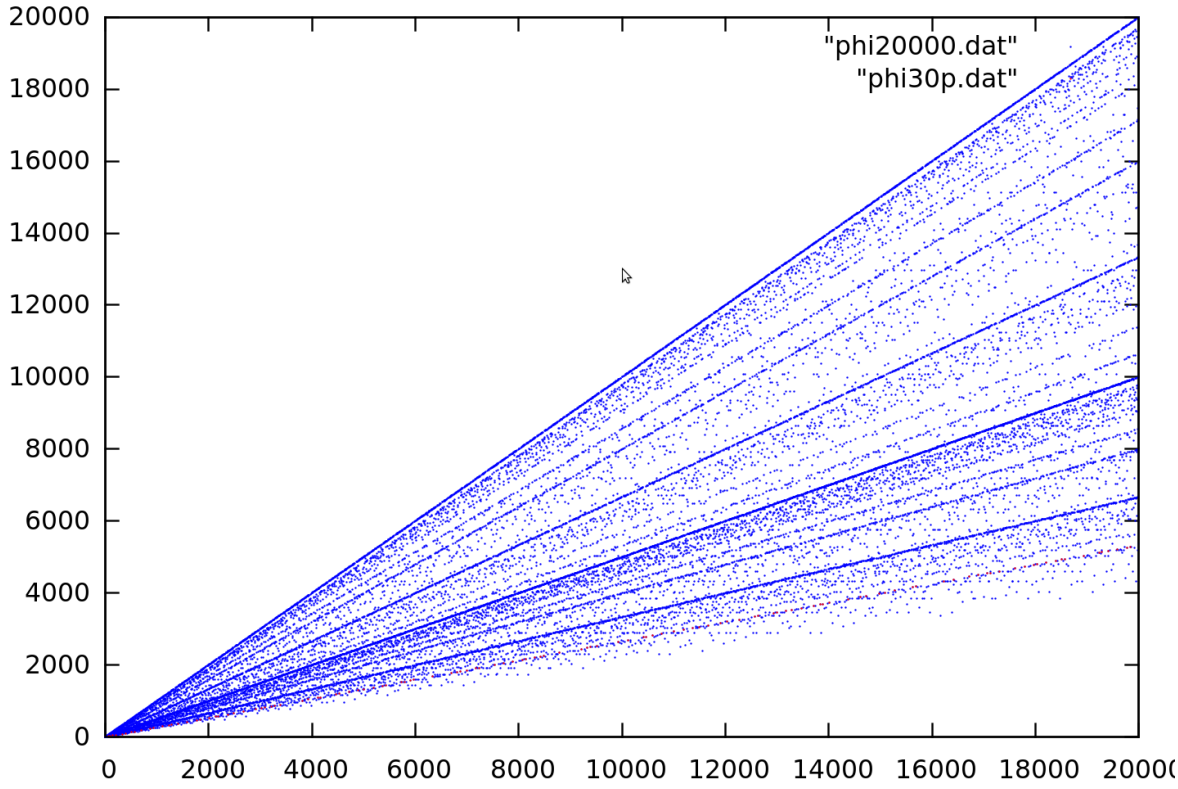


Fig. 20 : Indicateur d'Euler appliqué aux nombres de la forme $30p$

Ce sont les points d'abscisse p qui semblent fournir la limite haute de la comète de φ.

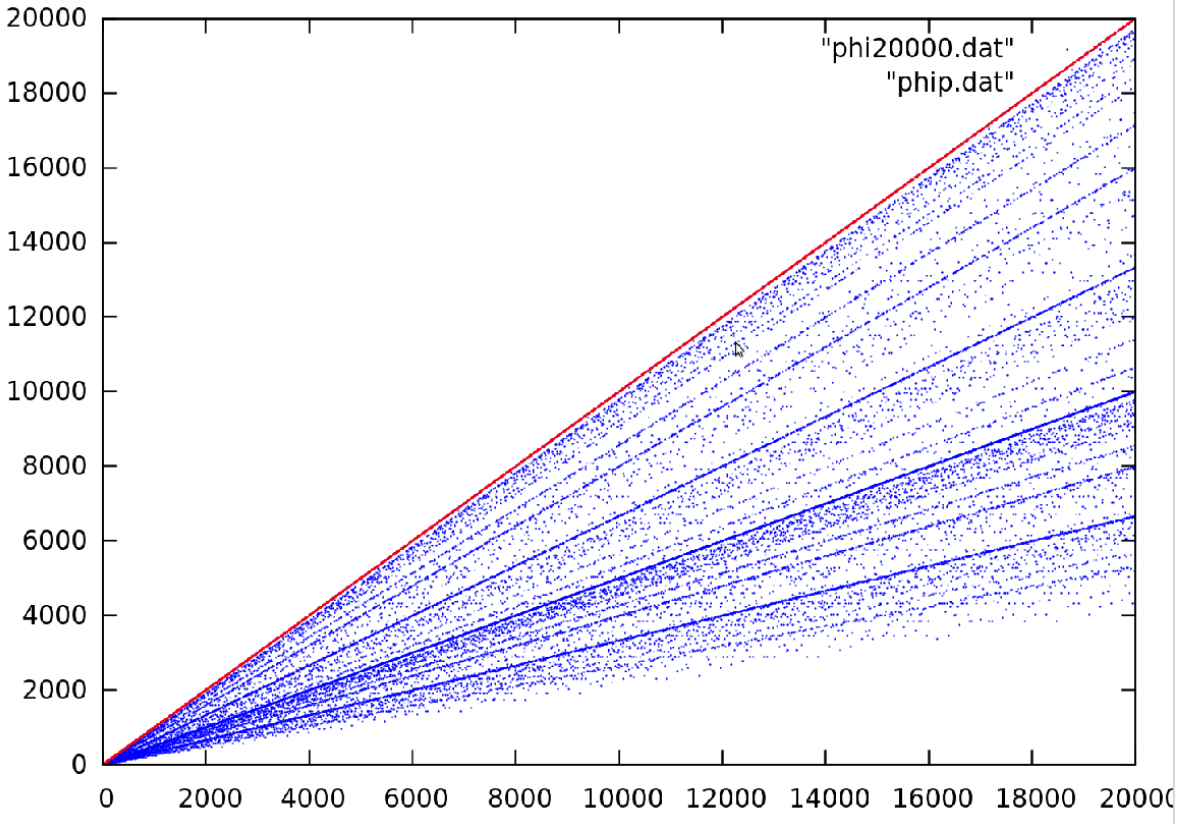


Fig. 21 : Indicateur d'Euler appliqué aux nombres premiers

On reproduit enfin la concentration de points par l'élévation au carré des nombres premiers. C'est ce que l'on

constate sur la visualisation ci-après : les sommes des diviseurs des nombres de la forme $2p^2$ avec p premier par exemple, se trouvent également dans la même tige de la gerbe que les $2p^3$.

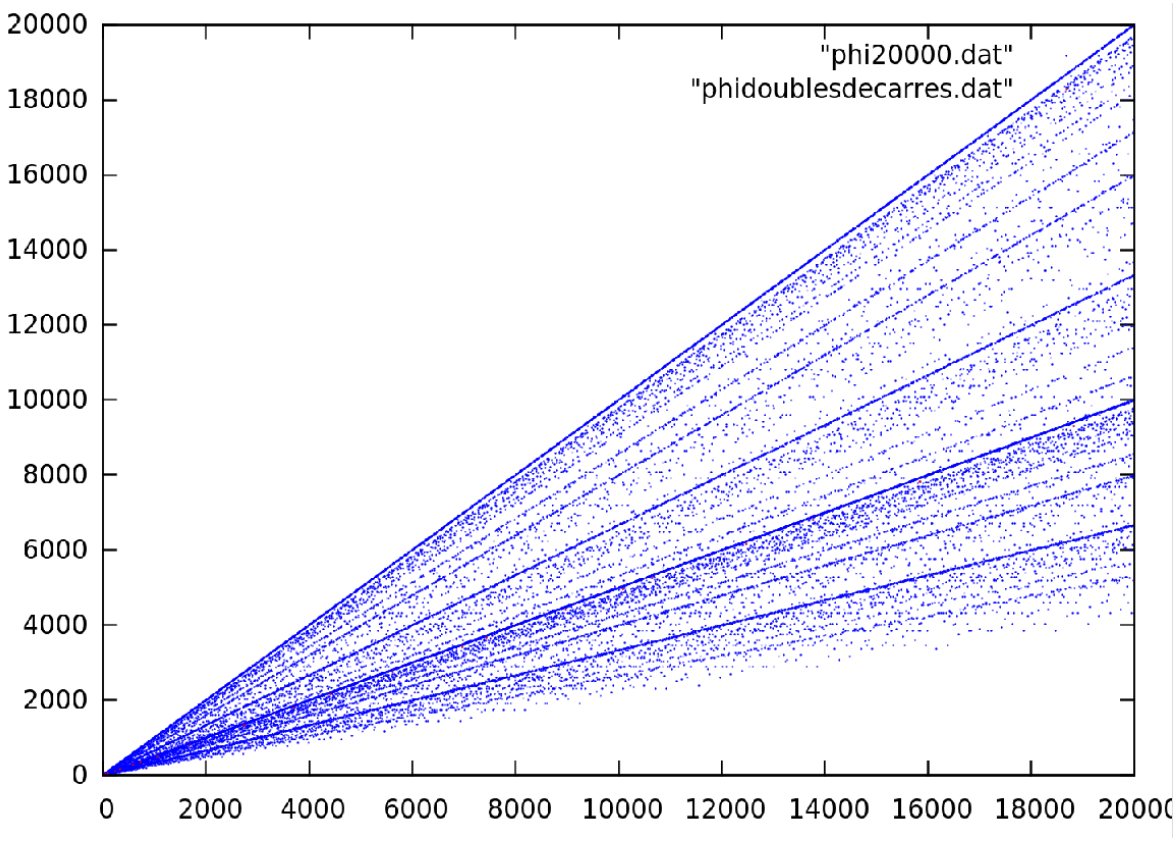


Fig. 22 : φ des doubles de carrés de premiers

Pour que ces visualisations soient lisibles, on doit comprendre que les outils permettent de n'afficher qu'un certain nombre de points pris au hasard dans un fichier de données. Si l'on choisit d'afficher tous les nombres de décompositions, on obtient le graphique de la figure 23 ci-dessous, ininterprétable.

[3]Il y a quelques petits points rouges à retrouver sur la tige des $2p$; à nouveau, les zoom-écrans ne laissent pas de place au doute...

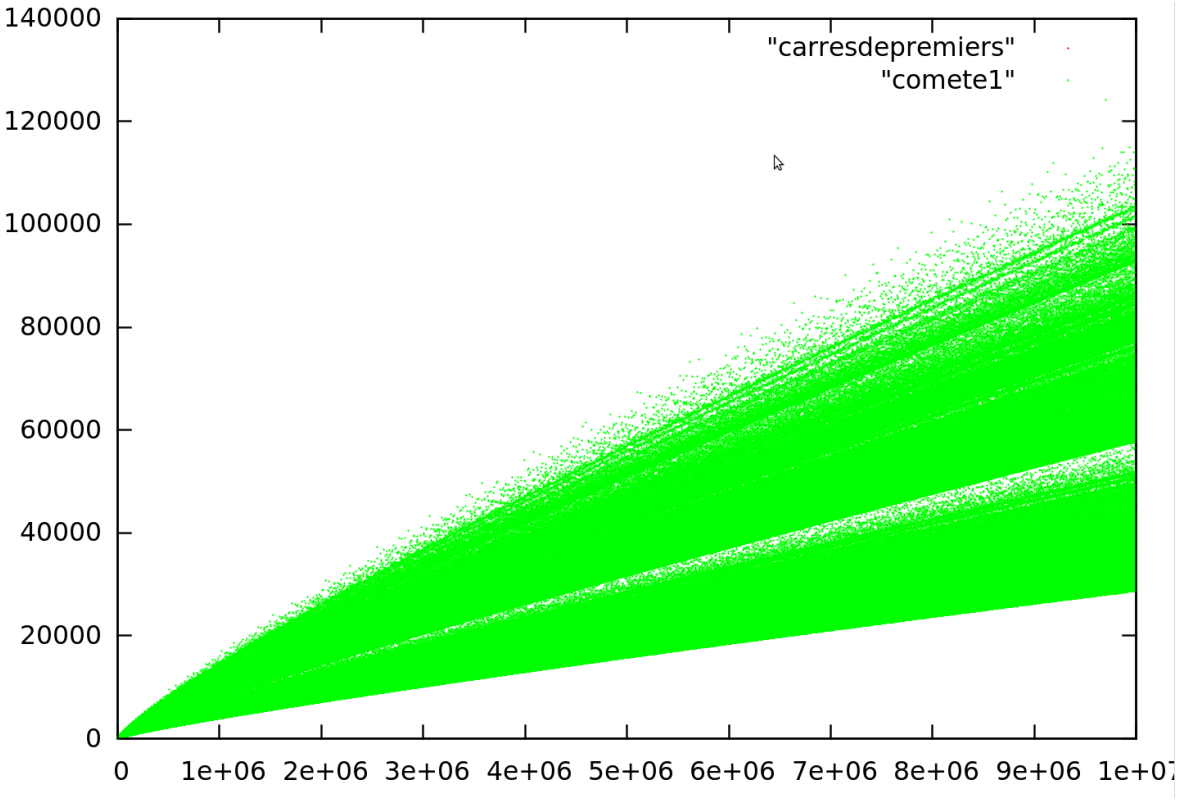


Fig. 23 : Nombres de décompositions de Goldbach sans tirages aléatoires

Fournissons quelques valeurs du nombre de décompositions de Goldbach des doubles de premiers (qui fournissent les valeurs minimales, en bas de la comète).

n	$NbDecompG(n)$	$Log(n)$
$9999998 \sim 10^7$	28983	7
$19999982 \sim 2.10^7$	53364	7.3
$29999962 \sim 3.10^7$	75777	7.47
$39999998 \sim 4.10^7$	97514	7.6
$49999966 \sim 5.10^7$	118760	7.69
$59999998 \sim 6.10^7$	139046	7.77
$69999938 \sim 7.10^7$	159569	7.84
$79999966 \sim 8.10^7$	179764	7.9
$89999942 \sim 9.10^7$	199455	7.95
$99999982 \sim 10^8$	218411	8

On constate que le rapport $\frac{218411}{28983} = 7.53$ semble proche du logarithme[4].

Il semblerait également, au vu de ces seules valeurs, que la fonction $NbDecompG$ est additive mais non pas au sens habituel utilisé en théorie des nombres qui veut que $f(a.b) = f(a) + f(b)$ mais plutôt au sens général qui fait que $f(a + b) = f(a) + f(b)$. On constate non seulement que $f(a + b) \sim f(a) + f(b)$ mais également que $f(\lambda a) \sim \lambda f(a)$.

Testons si la fonction NbDecompG est multiplicative. Pour cela, fournissons-en quelques valeurs :

[4]A noter : les nombres premiers 4 999 999, 19 999 999 et 29 999 999 sont particulièrement rigolos. On peut tester la primalité des nombres en utilisant le logiciel de factorisation par la méthode des courbes elliptiques à l'adresse http://www.alpertron.com.ar/ECM.HTM

n	$NbDecompG(n)$
$2026 = 2.1013$	32
$4054 = 2.2027$	55
$4106702 = 2.1013.2027$	13561
$8213404 = 2.1013.2.2027$	24549
$2053352 = 1013.2027 + 1$	9187

$NbDecompG(a.b)$ a une valeur différente de $NbDecompG(a).NbDecompG(b)$.

Enfin, fournissons les valeurs et la visualisation des nombres de décompositions de Goldbach de certains multiples des primorielles équitablement répartis jusqu'à 10 millions.

n	$NbDecompG(n)$
6	1
30	3
210	19
2310	114
30030	905
60060	1564
90090	2135
150150	3215
210210	4273
330330	6181
390390	7094
510510	9493
1021020	17075
1531530	24044
2552550	37302
3573570	49655
5615610	73205
6636630	84638
8678670	106360
9699690	124180

Comme on peut le constater, ces nombres semblent fournir les valeurs limites hautes de la comète...

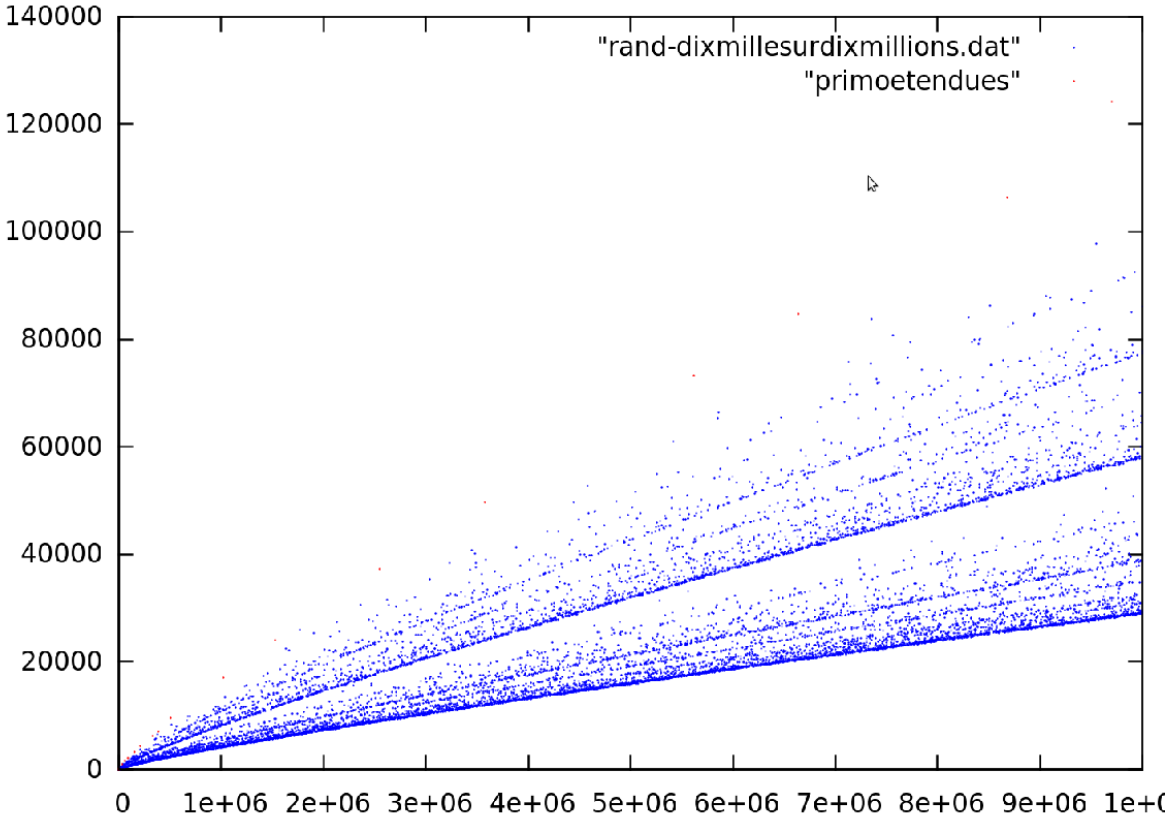


Fig. 24 : Nombres de décompositions de Goldbach des multiples de primorielles

Les outils permettent enfin, et cela n'est pas la moindre des choses, de voir si une fonction définie par l'utilisateur minore ou pas le nombre de décompositions de Goldbach (combien de fois, pour qui, etc).

J'ai choisi la fonction de minoration suivante, découlant de la méthode dite par "pliage du tissu" dans laquelle le produit s'effectue sur les nombres p premiers impairs inférieurs ou égaux à $2\sqrt{x}+1$:

$$MinoreGoldbach(x) = \left\lfloor \frac{x-1}{2} \right\rfloor \prod_{p} \left(1 - \frac{2}{p}\right)$$

Des tests plus poussés montrent que, quoique proche du nombre de décompositions de Goldbach (la différence maximum enregistrée entre le résultat de cette fonction et le nombre de décompositions de Goldbach est de 43 jusqu'à 10^7), elle ne le minore pas.

Par contre, en divisant le résultat de la fonction proposée par $log(x)$ ou bien par $log(log(x))$, on obtient une minoration systématique, mais en obtenant des résultats en moyenne plus éloignés des points de la comète (les outils permettent d'obtenir un rapport moyen de 13.94 dans le premier cas et de 2.5 dans le deuxième cas). La première formule, bien que non minorante, permettait d'obtenir un rapport moyen de 0.92, qui représente le fait que la formule "collait" bien aux points de la comète.

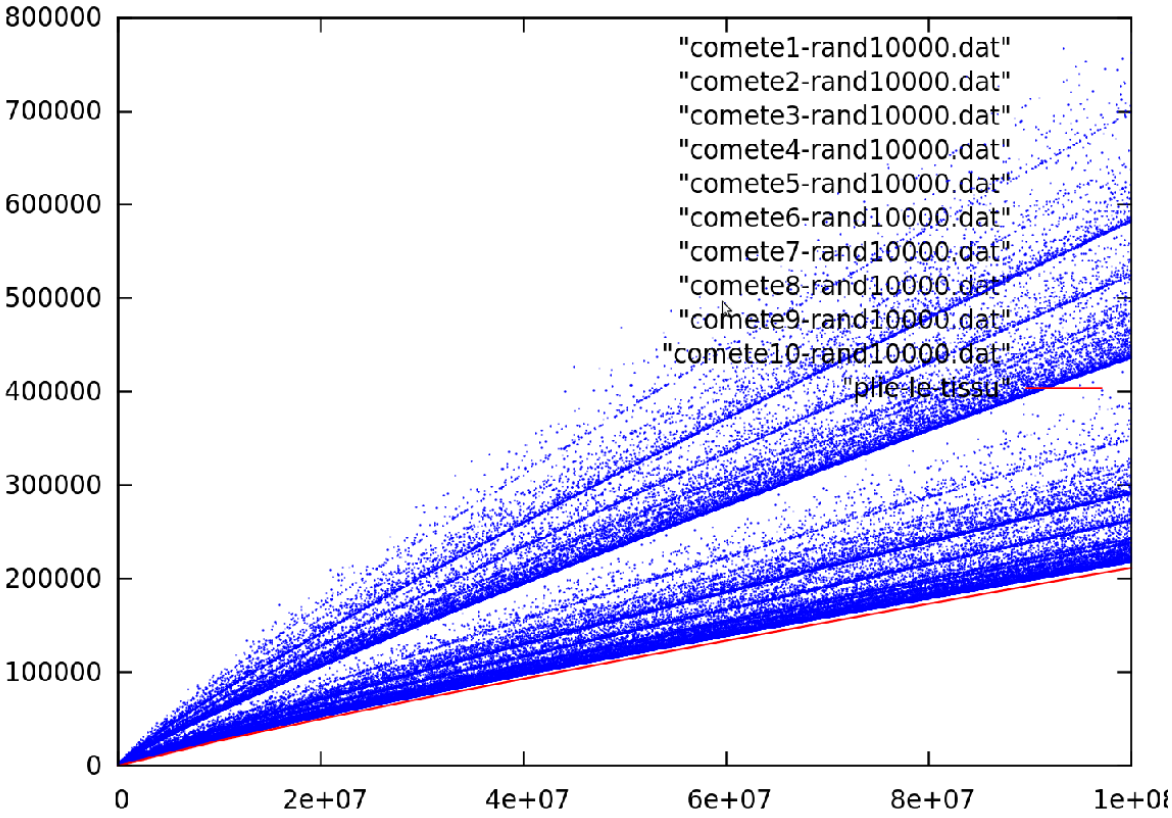
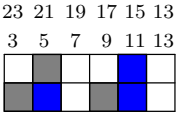


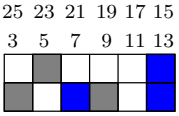
Fig. 25 : Minoration du nombre de décompositions de Goldbach

21 19 17 15 13
3 5 7 9 11

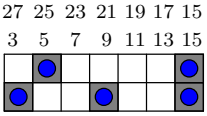
23 21 19 17 15 13
3 5 7 9 11 13



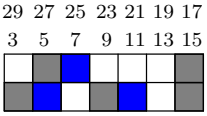
25 23 21 19 17 15
3 5 7 9 11 13



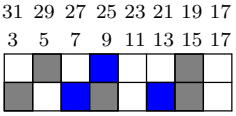
27 25 23 21 19 17 15
3 5 7 9 11 13 15



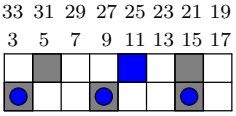
29 27 25 23 21 19 17
3 5 7 9 11 13 15



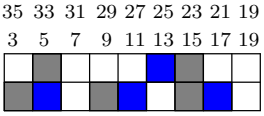
31 29 27 25 23 21 19 17
3 5 7 9 11 13 15 17



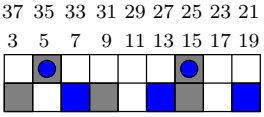
33 31 29 27 25 23 21 19
3 5 7 9 11 13 15 17



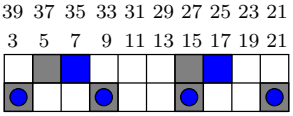
35 33 31 29 27 25 23 21 19
3 5 7 9 11 13 15 17 19



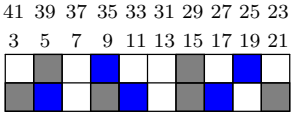
37 35 33 31 29 27 25 23 21
3 5 7 9 11 13 15 17 19



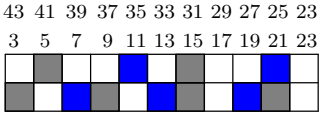
39 37 35 33 31 29 27 25 23 21
3 5 7 9 11 13 15 17 19 21



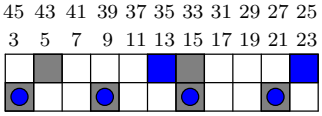
41 39 37 35 33 31 29 27 25 23
3 5 7 9 11 13 15 17 19 21



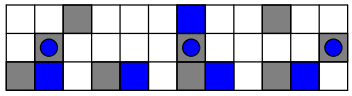
43 41 39 37 35 33 31 29 27 25 23
3 5 7 9 11 13 15 17 19 21 23



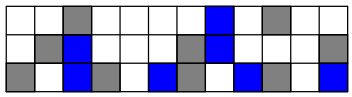
45 43 41 39 37 35 33 31 29 27 25
3 5 7 9 11 13 15 17 19 21 23



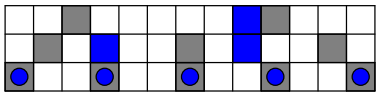
47 45 43 41 39 37 35 33 31 29 27 25
3 5 7 9 11 13 15 17 19 21 23 25



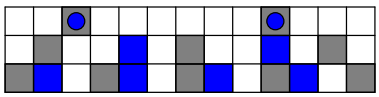
49 47 45 43 41 39 37 35 33 31 29 27
3 5 7 9 11 13 15 17 19 21 23 25



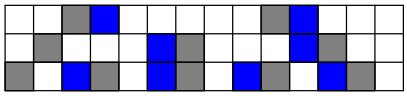
51 49 47 45 43 41 39 37 35 33 31 29 27
3 5 7 9 11 13 15 17 19 21 23 25 27



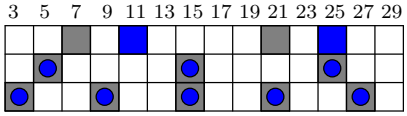
53 51 49 47 45 43 41 39 37 35 33 31 29
3 5 7 9 11 13 15 17 19 21 23 25 27



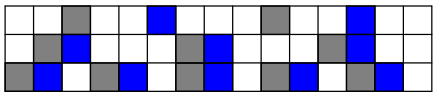
55 53 51 49 47 45 43 41 39 37 35 33 31 29
3 5 7 9 11 13 15 17 19 21 23 25 27 29



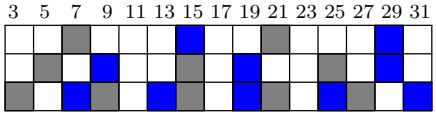
57 55 53 51 49 47 45 43 41 39 37 35 33 31
3 5 7 9 11 13 15 17 19 21 23 25 27 29



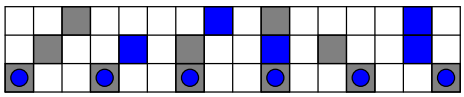
59 57 55 53 51 49 47 45 43 41 39 37 35 33 31
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31



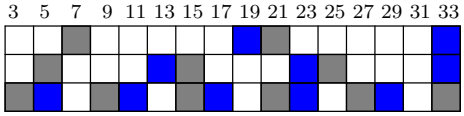
61 59 57 55 53 51 49 47 45 43 41 39 37 35 33
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31



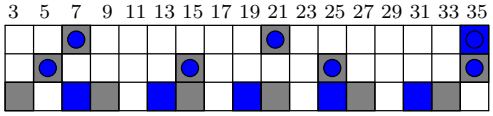
63 61 59 57 55 53 51 49 47 45 43 41 39 37 35 33
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33



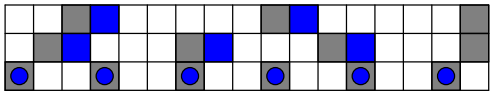
65 63 61 59 57 55 53 51 49 47 45 43 41 39 37 35
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33



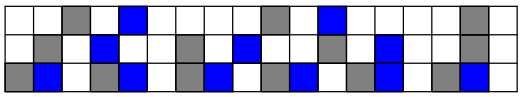
67 65 63 61 59 57 55 53 51 49 47 45 43 41 39 37 35
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35



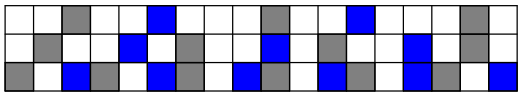
69 67 65 63 61 59 57 55 53 51 49 47 45 43 41 39 37
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35



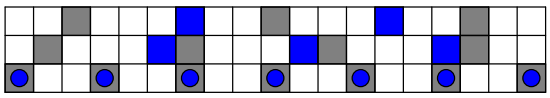
71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41 39 37
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37



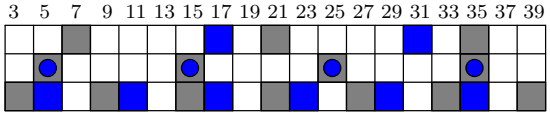
73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41 39
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37



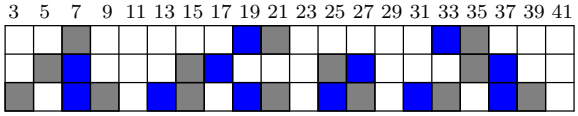
75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41 39
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39



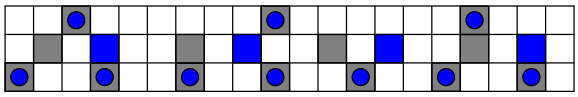
77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39



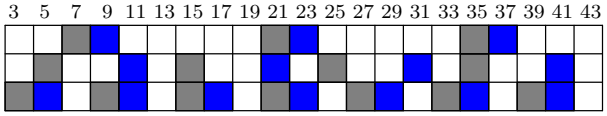
79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41



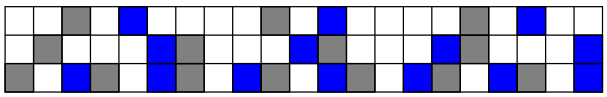
81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41



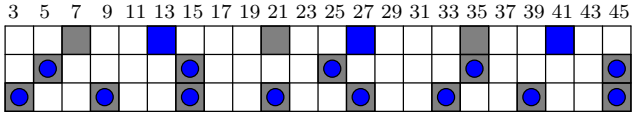
83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43



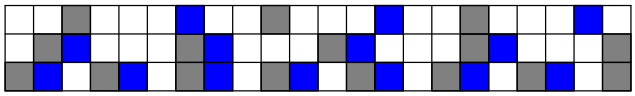
85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43



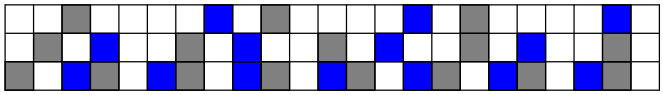
87 85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45



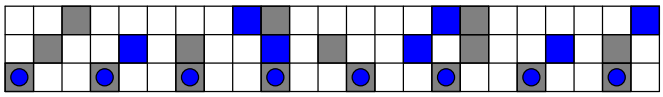
89 87 85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45



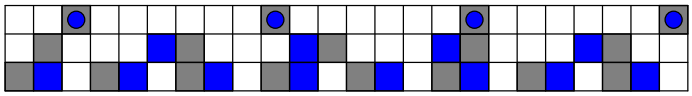
91 89 87 85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47



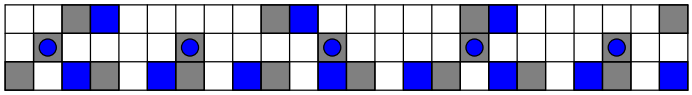
93 91 89 87 85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47



95 93 91 89 87 85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49



97 95 93 91 89 87 85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49



Poursuite des expérimentations

Les tableaux suivants fournissent les nombres de décompositions de Goldbach de certains nombres pairs, inférieurs à 10^7, et respectant certains critères. Dans la suite, on notera $r(n)$ le nombre de décompositions différentes de n comme somme de deux nombres premiers.

n = $2^k.3$	$r(n)$
6	1
12	1
24	3
48	5
96	7
192	11
384	19
768	31
1536	47
3072	79
6144	145
12288	226
24576	397
49152	675
98304	1185
196608	2110
393216	3679
786432	6639
1572864	11952
3145728	21367
6291456	38887

n = $2^k.5$	$r(n)$
10	2
20	2
40	3
80	4
160	8
320	11
640	18
1280	27
2560	48
5120	76
10240	141
20480	234
40960	387
81920	671
163840	1194
327680	2133
655360	3809
1310720	6762
2621440	12226
5242880	22134

n = $2^k.7$	$r(n)$
14	2
28	2
56	3
112	7
224	7
448	13
896	20
1792	36
3584	55
7168	94
14336	152
28672	276
57344	467
114688	818
229376	1424
458752	2516
917504	4503
1835008	8102
3670016	14633
7340032	26662
n = $2^k.11$	$r(n)$
22	3
44	3
88	4
176	7
352	10
704	18
1408	25
2816	40
5632	74
11264	124
22528	206
45056	346
90112	638
180224	1066
360448	1938
720896	3385
1441792	6151
2883584	11147
5767168	20027

n = $2^k.13$	$r(n)$
26	3
52	3
104	5
208	7
416	10
832	22
1664	28
3328	46
6656	80
13312	139
26624	230
53248	404
106496	688
212992	1222
425984	2146
851968	3874
1703936	6972
3407872	12558
6815744	22769
n = 2.3^k	$r(n)$
6	1
18	2
54	5
162	10
486	23
1458	48
4374	102
13122	245
39366	561
118098	1369
354294	3418
1062882	8599
3188646	21650
9565938	55711
n = 2.5^k	$r(n)$
10	2
50	4
250	9
1250	28
6250	95
31250	326
156250	1179
781250	4359
3906250	17187

n = 2.7^k	$r(n)$
14	2
98	3
686	16
4802	64
33614	309
235298	1442
1647086	7407
n = 2.11^k	$r(n)$
22	3
242	8
2662	44
29282	251
322102	1756
3543122	13202

Pour les nombres dans la factorisation desquels interviennent plusieurs nombres premiers impairs, il semblerait que :

$$Si\ a \mid b\ alors\ r(a)\ \leq\ r(b).$$

C.P.Bruter me fait remarquer que $r(n)$ est souvent la somme de plusieurs nombres $r(a_i)$ avec $a_i\ <\ n$.

Effectivement, dans le tableau des $2^k.13$, on relève les partitions suivantes :
$r(5) = 10 = r(4) + r(2) = 7 + 3$
$22 = 10 + 7 + 5$
$28 = 10 + 7 + 5 + 3 + 3$
$46 = 28 + 10 + 5 + 3$
$80 = 46 + 28 + 3 + 3$
$139 = 80 + 46 + 10 + 3$
$230 = 139 + 46 + 28 + 10 + 7$
$404 = 230 + 139 + 28 + 7$
$688 = 404 + 230 + 46 + 5 + 3$
$1222 = 688 + 404 + 80 + 28 + 22$
$2146 = 1222 + 688 + 230 + 3 + 3$
$3874 = 2146 + 1222 + 404 + 80 + 22$
$6972 = 3874 + 2146 + 688 + 230 + 28 + 3 + 3$
$12558 = 6972 + 3874 + 1222 + 404 + 80 + 3 + 3$
$22769 = 12558 + 6972 + 2146 + 688 + 230 + 139 + 28 + 5 + 3$

Dans le tableau des $2^k.5$, on peut trouver une partition du dernier nombre de décompositions :
$22134 = 12226 + 6762 + 2133 + 671 + 234 + 76 + 18 + 8 + 4 + 2$

Les partitions des $r(n)$ des 4 premiers tableaux seront ajoutés en annexe.

Un élément important est le suivant : on pourrait croire que ces partitions ne sont possibles que parce que les ensembles de nombres premiers dont on additionne les cardinaux sont disjoints deux à deux, ce qui n'est absolument pas le cas : 71 et 91 par exemple sont tous deux décomposants des nombres 13312

et 3328 qui appartiennent à des ensembles dont on va ajouter les cardinaux pour obtenir le cardinal de l'ensemble de décompositions de 26624. C'est donc bien la relation qu'entretiennent les décomposants de Goldbach au pair qu'ils décomposent et non leurs qualités intrinsèques qui intervient vraisemblablement ici.

Les partitions utilisées dans le tableau des $2^k.3$, celui des $2^k.5$ ou celui des $2^k.13$ ne présentent pas de similarité entre elles (les lignes utilisées pour en trouver une autre ne sont pas les mêmes dans l'un et l'autre cas).

Quand on essaie de trouver similairement des partitions des $r(n)$ faisant intervenir des "$r(m)$ plus petits" dans les tableaux des nombres de la forme $2.p^k$, on ne peut y parvenir car les $r(n)$ croissent trop rapidement.

On essaie de comparer plutôt de façon transversale les $r(n)$ des nombres de la forme $2p^k$ à ceux de leur correspondant de la forme $2kp$. C'est ce qui est présenté dans le tableau suivant :

Il semble qu'on ait toujours la relation suivante : $r(2p^k) > r(2kp)$.

n = 2p^k	$r(n)$	$n' = 2kp$	$r(n')$
$18 = 2.3^2$	2	2.2.3	1
$50 = 2.5^2$	4	2.2.5	2
$98 = 2.7^2$	3	2.2.7	2
$242 = 2.11^2$	8	2.2.11	3
$54 = 2.3^3$	5	2.3.3	2
$250 = 2.5^3$	9	2.3.5	3
$686 = 2.7^3$	16	2.3.7	4
$2662 = 2.11^3$	44	2.3.11	6
$162 = 2.3^4$	10	2.4.3	3
$1250 = 2.5^4$	28	2.4.5	3
$4802 = 2.7^4$	64	2.4.7	3
$29282 = 2.11^4$	251	2.4.11	4
$486 = 2.3^5$	23	2.5.3	3
$6250 = 2.5^5$	95	2.5.5	4
$33614 = 2.7^5$	309	2.5.7	5
$322102 = 2.11^5$	1756	2.5.11	6
$1458 = 2.3^6$	48	2.6.3	4
$31250 = 2.5^6$	326	2.6.5	6
$235298 = 2.7^6$	1442	2.6.7	8
$3543122 = 2.11^6$	13202	2.6.11	9
$4374 = 2.3^7$	102	2.7.3	4
$156250 = 2.5^7$	1179	2.7.5	5
$1647086 = 2.7^7$	7407	2.7.11	3

Enfin, on essaie d'établir des relations en utilisant le tableau des $r(n)$ pour les n de la forme $2^k.7.11$ en le mettant en regard des tableaux fournissant l'un les $r(n)$ des nombres de la forme $2^k.7$ et l'autre les $r(n)$ des nombres de la forme $2^k.11$ (cf. page 2).

n = 2^k.7.11	$r(n)$
154	8
308	8
616	19
1232	28
2464	52
4928	70
9856	130
19712	219
39424	371
78848	654
157696	1179
315392	2037
630784	3689
1261568	6520
2523136	11918
5046272	21503

On n'arrive absolument pas à trouver quoi que ce soit.

Fournissons maintenant les valeurs de $\sigma(n)$ et de $r(n)$ pour les nombres de 3 à 100. Nous aimerions atteindre l'objectif suivant : trouver une relation de récurrence qui fournisse le nombre de décompositions de Goldbach d'un nombre pair en fonction des nombres de décompositions de Goldbach de nombres plus petits que lui.

Note : je remercie très vivement Daniel Diaz qui, en programmant des outils performants, me permet de mener à bien ces expérimentations.

n	$\sigma(n)$	r(n)	n	$\sigma(n)$	r(n)	n	$\sigma(n)$	r(n)	n	$\sigma(n)$	r(n)
3	4	1	28	56	3	53	54	6	78	168	11
4	7	1	29	30	4	54	120	8	79	80	5
5	6	2	30	72	6	55	72	6	80	186	8
6	12	1	31	32	3	56	120	7	81	121	10
7	8	2	32	63	5	57	80	10	82	126	5
8	15	2	33	48	6	58	90	6	83	84	6
9	13	2	34	54	2	59	60	6	84	224	13
10	18	2	35	48	5	60	168	12	85	108	9
11	12	3	36	91	6	61	62	4	86	132	6
12	28	3	37	38	5	62	96	5	87	120	11
13	14	3	38	60	5	63	104	10	88	180	7
14	24	2	39	56	7	64	127	3	89	90	7
15	24	3	40	90	4	65	84	7	90	234	14
16	31	2	41	42	5	66	144	9	91	112	6
17	18	4	42	96	8	67	68	6	92	168	8
18	39	4	43	44	5	68	126	5	93	128	13
19	20	2	44	84	4	69	96	8	94	144	5
20	42	3	45	78	9	70	144	7	95	120	8
21	32	4	46	72	4	71	72	8	96	252	11
22	36	3	47	48	5	72	195	11	97	98	7
23	24	4	48	124	7	73	74	6	98	171	9
24	60	5	49	57	3	74	114	5	99	156	13
25	31	4	50	93	6	75	124	12	100	217	8
26	42	3	51	72	8	76	140	4			
27	40	5	52	98	5	77	96	8			

La conjecture de Goldbach est trivialement vérifiée pour les nombres pairs doubles de premiers. Il faudrait dans un premier temps la prouver pour les nombres de la forme $2.p^2$ qui semblent fournir les valeurs minimales de la comète. Ensuite, les nombres d'une autre forme seront ramenés aux nombres de la forme $2p$ par le théorème des restes chinois. Je crois par exemple que 2.3^6 a 48 décomposants, comme toute une série de nombres tels que $900, 1092, 1368, 1404, 1458, 1524, 1750, 1960, 2080, 2320, 2420, 2548, 2560, 2620$ $2674, 2690, 2912, 3034, 3098, 3110, 3208, 3232, etc$ parmi lesquels il doit sûrement y avoir un $2p$ notamment en vertu du théorème de Dirichlet. En quelque sorte, on fait une projection d'un point de la comète sur un point d'abscisse plus élevée et de même ordonnée, à cause de certaines propriétés. Et cette manière de voir est contraire à la notion même de récurrence qui veut qu'on puisse calculer $r(n)$ en fonction de $r(m)$ plus petits ; là, il s'agirait plutôt de trouver $r(n)$ comme étant égal au $r(n')$ d'un nombre n' plus grand que n.

On rappelle que l'on cherche, pour un nombre pair $2n$ donné, l'ensemble des nombres premiers q, non congrus à $2n$ selon tout p' premier inférieur ou égal à $\sqrt{2n}$.

Quelques expérimentations autour de la Conjecture de Goldbach

Denise Vella-Chemla

20 février 2011

1 Introduction

Dans cette note, on étudie les nombres de décompositions de Goldbach de nombres pairs de formes particulières, dans le but de mettre à jour certaines propriétés (qui amèneraient peut-être à une idée de démonstration).
Ce travail fait suite à des expérimentations menées autour de ce que l'on a coutume d'appeler la "comète de Goldbach"[1].
Il a été réalisé en utilisant des outils logiciels spécifiques dédiés à la Conjecture de Goldbach et programmés par Daniel Diaz, que l'on remercie vivement.

2 Doubles de premiers, puissances de 2

Les doubles de nombres premiers vérifient trivialement la Conjecture de Goldbach qui stipule que tout nombre pair supérieur ou égal à 4 est la somme de deux nombres premiers.

Le tableau suivant fournit les nombres de décompositions de Goldbach des puissances de 2 inférieures à 10^7. Dans la suite, on notera $r(n)$ le nombre de décompositions différentes de n comme somme de deux nombres premiers.

[1] Les résultats de ces expérimentations sont consignés à l'adresse http://denise.vella.chemla.free.fr/cometes1111landscape.pdf.

n = 2^k	$r(n)$
4	1
8	1
16	2
32	2
64	5
128	3
256	8
512	11
1024	22
2048	25
4096	53
8192	76
16384	151
32768	244
65536	435
131072	749
262144	1314
524288	2367
1048576	4239
2097152	7471
4194304	13705
8388608	24928

3 Les $2^k.p$

Le tableau suivant fournit les nombres de décompositions de Goldbach de certains nombres pairs, inférieurs à 10^7, de la forme $2^k.p$, avec p premier impair.

n = $2^k.3$	$r(n)$	n = $2^k.5$	$r(n)$	n = $2^k.7$	$r(n)$	n = $2^k.11$	$r(n)$	n = $2^k.13$	$r(n)$
6	1	10	2	14	2	22	3	26	3
12	1	20	2	28	2	44	3	52	3
24	3	40	3	56	3	88	4	104	5
48	5	80	4	112	7	176	7	208	7
96	7	160	8	224	7	352	10	416	10
192	11	320	11	448	13	704	18	832	22
384	19	640	18	896	20	1408	25	1664	28
768	31	1280	27	1792	36	2816	40	3328	46
1536	47	2560	48	3584	55	5632	74	6656	80
3072	79	5120	76	7168	94	11264	124	13312	139
6144	145	10240	141	14336	152	22528	206	26624	230
12288	226	20480	234	28672	276	45056	346	53248	404
24576	397	40960	387	57344	467	90112	638	106496	688
49152	675	81920	671	114688	818	180224	1066	212992	1222
98304	1185	163840	1194	229376	1424	360448	1938	425984	2146
196608	2110	327680	2133	458752	2516	720896	3385	851968	3874
393216	3679	655360	3809	917504	4503	1441792	6151	1703936	6972
786432	6639	1310720	6762	1835008	8102	2883584	11147	3407872	12558
1572864	11952	2621440	12226	3670016	14633	5767168	20027	6815744	22769
3145728	21367	5242880	22134	7340032	26662				
6291456	38887								

4 Les 2.p^k

Le tableau suivant fournit les nombres de décompositions de Goldbach de certains nombres pairs, inférieurs à 10^7, de la forme $2.p^k$ avec p premier impair.

n = 2.3^k	$r(n)$	n = 2.5^k	$r(n)$	n = 2.7^k	$r(n)$	n = 2.11^k	$r(n)$	n = 2.13^k	$r(n)$
6	1	10	2	14	2	22	3	26	3
18	2	50	4	98	3	242	8	338	9
54	5	250	9	686	16	2662	44	4394	55
162	10	1250	28	4802	64	29282	251	57122	406
486	23	6250	95	33614	309	322102	1756	742586	3431
1458	48	31250	326	235298	1442	3543122	13202	9653618	30833
4374	102	156250	1179	1647086	7407				
13122	245	781250	4359						
39366	561	3906250	17187						
118098	1369								
354294	3418								
1062882	8599								
3188646	21650								
9565938	55711								

5 Nombre de décompositions de Goldbach de quelques nombres pairs n'ayant que 7 et 11 comme facteurs premiers impairs

Sont fournies ci-dessous les nombres de décompositions de Goldbach de nombres pairs qui ont soit seulement 7, soit seulement 11, soit seulement 7 et 11 comme facteurs premiers impairs dans leur décomposition.

n=$2^k.7^2$	$r(n)$	n=$2^k.7^3$	$r(n)$	n=$2^k.11^2$	$r(n)$	n=$2^k.11^3$	$r(n)$	n=$2^k.7^k.11^k$	$r(n)$
98	3	686	16	242	8	2662	44	154	8
196	9	1372	27	484	14	5324	69	23716	254
392	11	2744	50	968	17	10648	116	3652264	16256
784	18	5488	80	1936	33	21296	199		
1568	25	10976	125	3872	52	42592	337		
3136	49	21952	229	7744	94	85184	600		
6272	78	43904	373	15488	153	170368	1075		
12544	147	87808	645	30976	265	340736	1823		
25088	236	175616	1130	61952	439	681472	3276		
50176	429	351232	2007	123904	809	1362944	5839		
100352	718	702464	3688	247808	1413	2725888	10563		
200704	1246	1404928	6446	495616	2533	5451776	19198		
401408	2234	2809856	11654	991232	4497				
802816	4032	5619712	21212	1982464	8056				
1605632	7224			3964928	14377				
3211264	13194			7929856	26463				
6422528	23805								

On constate que, en général, si $a < b < c$ alors $r(a) < r(b) < r(c)$, mais ça n'est pas toujours le cas.
Par exemple, 23716 ($9^{ème}$ colonne) est compris entre 12544 et 25088 ($1^{ère}$ colonne), entre 21952 et 43904 ($3^{ème}$ colonne), entre 15488 et 30976 ($5^{ème}$ colonne) et entre 21296 et 42592 ($7^{ème}$ colonne).
r(23716)=254 est bien compris entre r(21952)=229 et r(43904)=373 ($4^{ème}$ colonne) ou bien entre r(15488)=153 et r(30976)=265 ($6^{ème}$ colonne) ou encore entre r(21296)=199 et r(42592)=337 ($8^{ème}$ colonne).
r(23716)=254 n'est cependant pas compris entre r(12544)=147 et r(25088)=236 ($2^{ème}$ colonne).
On peut de la même façon intercaler un $2^k.7.11$ entre un $2^k.7.7$ et un $2^k.11.11$ et constater que les images par la fonction r respectent l'ordre des antécédents. De même, on peut intercaler un $2.p^k$ entre deux éléments $2^{k_1}.p$ et $2^{k_2}.p$ convenablement choisis et constater que l'ordre se transmet des antécédents aux images.

Pour les nombres dans la factorisation desquels interviennent plusieurs nombres premiers impairs, il semblerait que *si* $a|b$ *alors* $r(a) \leq r(b)$.

6 Quelques constats

C.P.Bruter me fait remarquer que, pour les nombres de la forme $2^k.p$, $r(n)$ est souvent la somme de plusieurs nombres $r(a_i)$ de la même forme avec $a_i < n$.

Effectivement, dans le tableau des $2^k.13$, on relève les partitions suivantes :
$r(2^5.13) = 10 = r(2^4.13) + r(2^2.13) = 7 + 3$
$22 = 10 + 7 + 5$
$28 = 10 + 7 + 5 + 3 + 3$
$46 = 28 + 10 + 5 + 3$
$80 = 46 + 28 + 3 + 3$
$139 = 80 + 46 + 10 + 3$
$230 = 139 + 46 + 28 + 10 + 7$
$404 = 230 + 139 + 28 + 7$
$688 = 404 + 230 + 46 + 5 + 3$
$1222 = 688 + 404 + 80 + 28 + 22$
$2146 = 1222 + 688 + 230 + 3 + 3$
$3874 = 2146 + 1222 + 404 + 80 + 22$
$6972 = 3874 + 2146 + 688 + 230 + 28 + 3 + 3$
$12558 = 6972 + 3874 + 1222 + 404 + 80 + 3 + 3$
$22769 = 12558 + 6972 + 2146 + 688 + 230 + 139 + 28 + 5 + 3$

Dans le tableau des $2^k.5$, on peut trouver une partition du nombre de décompositions $r(2^{20}.5) = r(5242880) = 22134$:
$22134 = 12226 + 6762 + 2133 + 671 + 234 + 76 + 18 + 8 + 4 + 2$

Il semblerait que l'on puisse toujours, pour les nombres de décompositions des nombres pairs de la forme $2^k.p$ avec p premier impair, obtenir le nombre de décompositions d'un certain d'entre eux par addition de certains nombres de décompositions de nombres pairs de la même forme et plus petits.

Un élément important est le suivant : on pourrait croire que ces partitions ne sont possibles que parce que les ensembles de nombres premiers dont on additionne les cardinaux sont disjoints deux à deux, ce qui n'est pas le cas : 71 et 91 par exemple sont tous deux décomposants des nombres 13312 et 3328 et appartiennent à des ensembles dont on va ajouter les cardinaux pour obtenir le cardinal de l'ensemble de décompositions de 26624. C'est donc bien la relation qu'entretiennent les décomposants de Goldbach au pair qu'ils décomposent et non leurs qualités intrinsèques qui intervient vraisemblablement ici.

Les partitions utilisées dans le tableau des $2^k.3$, celui des $2^k.5$ ou celui des $2^k.13$ ne présentent pas de similarité entre elles (les lignes utilisées pour en trouver une autre ne sont pas les mêmes dans l'un et l'autre cas).

Quand on essaie de trouver similairement des partitions des $r(n)$ faisant intervenir des "$r(m)$ plus petits" dans les tableaux des nombres de la forme $2.p^k$, on ne peut y parvenir car les $r(n)$ croissent trop rapidement.

On essaie de comparer plutôt de façon transversale les $r(n)$ des nombres de la forme $2p^k$ à ceux de leur correspondant de la forme $2kp$. C'est ce qui est présenté dans le

tableau suivant :

Il semble qu'on ait toujours la relation suivante : $r(2p^k) > r(2kp)$.

n = 2p^k	$r(n)$	$n' = 2kp$	$r(n')$
$18 = 2.3^2$	2	2.2.3	1
$50 = 2.5^2$	4	2.2.5	2
$98 = 2.7^2$	3	2.2.7	2
$242 = 2.11^2$	8	2.2.11	3
$54 = 2.3^3$	5	2.3.3	2
$250 = 2.5^3$	9	2.3.5	3
$686 = 2.7^3$	16	2.3.7	4
$2662 = 2.11^3$	44	2.3.11	6
$162 = 2.3^4$	10	2.4.3	3
$1250 = 2.5^4$	28	2.4.5	3
$4802 = 2.7^4$	64	2.4.7	3
$29282 = 2.11^4$	251	2.4.11	4
$486 = 2.3^5$	23	2.5.3	3
$6250 = 2.5^5$	95	2.5.5	4
$33614 = 2.7^5$	309	2.5.7	5
$322102 = 2.11^5$	1756	2.5.11	6
$1458 = 2.3^6$	48	2.6.3	4
$31250 = 2.5^6$	326	2.6.5	6
$235298 = 2.7^6$	1442	2.6.7	8
$3543122 = 2.11^6$	13202	2.6.11	9
$4374 = 2.3^7$	102	2.7.3	4
$156250 = 2.5^7$	1179	2.7.5	5
$1647086 = 2.7^7$	7407	2.7.11	3

Enfin, on essaie d'établir des relations en utilisant le tableau des $r(n)$ pour les n de la forme $2^k.7.11$ en le mettant en regard des tableaux fournissant l'un les $r(n)$ des nombres de la forme $2^k.7$ et l'autre les $r(n)$ des nombres de la forme $2^k.11$.

n = $2^k.7$	$r(n)$	n = $2^k.11$	$r(n)$	n = $2^k.7.11$	$r(n)$
14	2	22	3	154	8
28	2	44	3	308	8
56	3	88	4	616	19
112	7	176	7	1232	28
224	7	352	10	2464	5
448	13	704	18	4928	70
896	20	1408	25	9856	130
1792	36	2816	40	19712	219
3584	55	5632	74	39424	371
7168	94	11264	124	78848	654
14336	152	22528	206	157696	1179
28672	276	45056	346	315392	2037
57344	467	90112	638	630784	3689
114688	818	180224	1066	1261568	6520
229376	1424	360448	1938	2523136	11918
458752	2516	720896	3385	5046272	21503
917504	4503	1441792	6151		
1835008	8102	2883584	11147		
3670016	14633	5767168	20027		
7340032	26662				

Il semblerait que l'on ait $r(2^k ab) > r(2^k a) + r(2^k b)$ ou encore $r(2^k ab) > 2r(2^{k-2} ab)$.

7 Rappel de l'objectif initial

Fournissons maintenant les valeurs de $\sigma(n)$ et de $r(n)$ pour les nombres de 3 à 100. En suivant l'exemple de l'article d'Euler "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs", nous aurions aimé atteindre l'objectif suivant : trouver une relation de récurrence qui fournisse le nombre de décompositions de Goldbach d'un nombre pair en fonction des nombres de décompositions de Goldbach de nombres plus petits que lui. Mais force est de constater que cette tâche semble insurmontable.

n	$\sigma(n)$	r(n)	n	$\sigma(n)$	r(n)	n	$\sigma(n)$	r(n)	n	$\sigma(n)$	r(n)
3	4	1	28	56	3	53	54	6	78	168	11
4	7	1	29	30	4	54	120	8	79	80	5
5	6	2	30	72	6	55	72	6	80	186	8
6	12	1	31	32	3	56	120	7	81	121	10
7	8	2	32	63	5	57	80	10	82	126	5
8	15	2	33	48	6	58	90	6	83	84	6
9	13	2	34	54	2	59	60	6	84	224	13
10	18	2	35	48	5	60	168	12	85	108	9
11	12	3	36	91	6	61	62	4	86	132	6
12	28	3	37	38	5	62	96	5	87	120	11
13	14	3	38	60	5	63	104	10	88	180	7
14	24	2	39	56	7	64	127	3	89	90	7
15	24	3	40	90	4	65	84	7	90	234	14
16	31	2	41	42	5	66	144	9	91	112	6
17	18	4	42	96	8	67	68	6	92	168	8
18	39	4	43	44	5	68	126	5	93	128	13
19	20	2	44	84	4	69	96	8	94	144	5
20	42	3	45	78	9	70	144	7	95	120	8
21	32	4	46	72	4	71	72	8	96	252	11
22	36	3	47	48	5	72	195	11	97	98	7
23	24	4	48	124	7	73	74	6	98	171	9
24	60	5	49	57	3	74	114	5	99	156	13
25	31	4	50	93	6	75	124	12	100	217	8
26	42	3	51	72	8	76	140	4			
27	40	5	52	98	5	77	96	8			

Il serait intéressant de comprendre ne-serait-ce que pourquoi la conjecture est vraie (car peu en doutent) pour des nombres de la forme $2.p^2$, ou bien de la forme $2^k.p$ parce qu'ils semblent fournir les valeurs minimales de la comète.
2.3^6, par exemple, a 48 décomposants, comme toute une série de nombres tels que $900, 1092, 1368, 1404, 1458, 1524, 1750, 1960, 2080, 2320, 2420, 2548, 2560, 2620$
$2674, 2690, 2912, 3034, 3098, 3110, 3208, 3232, etc$ parmi lesquels il doit sûrement y avoir un $2p$ notamment en vertu du théorème de Dirichlet. En quelque sorte, on fait une projection d'un point de la comète sur un point d'abscisse plus élevée et de même ordonnée, à cause de certaines propriétés. Mais cette manière de voir est contraire à la notion même de récurrence que l'on cherchait à obtenir et qui veut qu'on puisse calculer $r(n)$ en fonction de $r(n_i)$ plus petits ; pour les nombres qui ne sont pas dans la ligne basse de la comète, il s'agirait plutôt de trouver $r(n)$ comme étant égal au $r(n')$ d'un nombre n' plus grand que n.

8 Tentative d'explication des propriétés de partitions découvertes sur les $2^k.p$

On rappelle que l'on cherche, pour un nombre pair $2n$ donné, l'ensemble des nombres premiers p non congrus à $2n$ selon tout p' premier inférieur ou égal à $\sqrt{2n}$. Ces nombres sont des unités du groupe multiplicatif : ils sont premiers à $2n$.
On cherche à trouver une explication à la propriété de "somme des cardinaux" qui fait

que $r(i) = r(i_1) + r(i_2) + ... + r(i_n)$ avec $i_k < i$ pour tout k.
Admettons que l'on ait réussi à répondre à la question *Quels i_k doivent être choisis comme sommants* ?, il subsiste une interrogation quant au fait que tous les décomposants ne se transmettent pas toujours directement au produit. On comprend à quelle condition un décomposant se transmet à un produit : on a vu qu'un décomposant de Goldbach de $2x$ est une unité qui est non-congrue à $2x$ selon tout module inférieur à $\sqrt{2x}$. Dans la suite, on utilisera la notation $a \not\equiv b$ $(mod$?$)$ pour exprimer que a est non-congru à b selon tout module *adéquat* (i.e. inférieur à la racine du pair considéré) alors que la notation $a \equiv b$ $(mod$?$)$ exprimera que a est congru à b selon un module (la première proposition étant la négation logique de la deuxième).

Si $p \not\equiv x$ $(mod$?$)$ et si $p.\frac{1}{y} \not\equiv x$ $(mod$?$)$ alors $p \not\equiv xy$ $(mod$?$)$ et p est un décomposant du produit xy. Il faut ici mettre des conditions sur l'implication pour respecter le paragraphe 23 de la section Seconde des Recherches Arithmétiques de Gauss qui stipule que *Si a est premier avec m, que e et f soient des nombres incongrus suivant le module m, ae et af seront aussi incongrus.*

Tandis que si $p \not\equiv x$ $(mod$?$)$ et si $p.\frac{1}{y} \equiv x$ $(mod$?$)$ alors $p \equiv xy$ $(mod$?$)$ et p n'est pas un décomposant du produit xy mais alors puisque les cardinaux sont égaux, il doit y avoir la possibilité de trouver *un autre* p qui remplace p dans l'ensemble des décomposants du produit puisque, finalement, on en trouve autant.

9 Une autre piste utilisant les résidus quadratiques

La loi de réciprocité quadratique a reçu de si nombreuses démonstrations (notamment par Gauss) qu'elle doit être un théorème *puissant*, dont doivent découler de nombreux autres théorèmes.
On cherche p tel que $p \not\equiv 2a$ $(mod$?$)$. Cela équivaut à $p.\frac{1}{a} \not\equiv 2$ $(mod$?$)$[2].
Si l'on prend l'ensemble des modules dont 2 n'est pas résidu quadratique, et que parmi eux, on considère ceux dont $p.\frac{1}{a}$ est résidu quadratique, alors ces modules seront tels que $p.\frac{1}{a} \not\equiv 2$ $(mod$?$)$.
De telles hyothèses peuvent avoir pour conséquence les partitions sur les cardinaux que l'on a constatées, c'est à dire le fait que les décompositions de Goldbach des grands nombres découlent des décompositions de Goldbach de nombres plus petits.

[2]Se référer aux sections 112 à 116 des Recherches Arithmétiques de Gauss.

Conjecture de Goldbach
et systèmes de congruences du second degré

Denise Vella-Chemla

14/8/11

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Cette conjecture est trivialement vérifiée par les nombres pairs doubles de nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru[1] à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\, n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\, q \leq \sqrt{n},\quad p \not\equiv n\ (q)$$

Posons $n\ =\ x^2 b$ avec x^2 le plus grand carré divisant n.

b est le produit des nombres premiers de valuation p-adique impaire (i.e. élevés à une puissance impaire) dans la factorisation de n (ce faisant, on obéit en quelque sorte à la préconisation de Gauss dans l'article 146 page 109 point III de la section Quatrième des Recherches Arithmétiques : *"Au reste, on voit facilement que si parmi les facteurs p, p′, p″, etc., il y en a un nombre pair d'égaux entre eux, on peut les rejeter, puisqu'ils n'influent en rien sur la relation de p à n."*).

Résoudre un système d'incongruences quadratiques de la forme $\frac{1}{b}.p \not\equiv x^2\ (q)$ selon tous les modules premiers q inférieurs à $\sqrt{n}$ en utilisant la loi de réciprocité quadratique, le théorème d'or selon Gauss, permet-il de trouver un décomposant de Goldbach de n au moins ?

2 Méthode inductive à la recherche de *la raison qui fait que...*

Si l'on parvient à démontrer qu'un nombre premier p au moins vérifie les incongruences $\frac{1}{b}.p \not\equiv x^2\ (q)$ selon tous les modules premiers q inférieurs à $\sqrt{n}$, notre problème sera résolu. Si l'on appelle A le produit $\frac{1}{b}.p$, p est un diviseur de A. Il s'agit alors de résoudre l'incongruence $x^2 - A \not\equiv 0\ (q)$. Nous verrons que dans les articles 147 à 149 des Recherches Arithmétiques, Gauss fournit les formules qui contiennent tous les nombres premiers à A dont A est résidu, ou tous ceux qui sont diviseurs des nombres de la forme $x^2 - A$, x^2 étant un carré indéterminé.

2.1 Exemples 1 et 2

Commençons par le nombre pair $98\ =\ 2.7^2$.
Les 3 modules premiers impairs à considérer inférieurs à la racine de 98 sont 3, 5 et 7.
L'incongruence $p \not\equiv 2.7^2 (mod\ 3,\ 5\ et\ 7)$ devient $\frac{1}{2}.p \not\equiv 7^2 (mod\ 3,\ 5\ et\ 7)$.
L'écriture de 3 modules entre parenthèses est non-conventionnelle mais nous permet de gagner de la place,

[1] On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

elle indique une conjonction de faits[2].
L'inverse de 2 est 2 (mod 3), l'inverse de 2 est 3 (mod 5) et l'inverse de 2 est 4 (mod 7). 2 est non-résidu de 3. 3 est non-résidu de 5. 4 est résidu de 7.
Ici, on rappelle que tout nombre premier p est résidu de lui-même. D'autre part, bien qu'un nombre premier p ne soit pas inversible dans $(\mathbb{Z}/p\mathbb{Z}, \times)$, Gauss fournit à l'article 109, section Quatrième des Recherches Arithmétiques la convention selon laquelle si r est résidu de p, l'inverse de r noté $\frac{1}{r}$ est lui-aussi résidu de p pour p un nombre premier (ceci est en particulier vrai de p un nombre premier qui est toujours résidu de lui-même).
Le nombre premier recherché doit donc être :

- résidu de 3 pour que, en le multipliant par l'inverse de 2, on n'obtienne pas un carré ;
- résidu de 5 (pour la même raison) ;
- non-résidu de 7 (pour la raison opposée).

19 et 31 vérifient les 3 conditions exigées et sont des décomposants de Goldbach de 98. Si on dresse une petite table "est résidu de" des nombres premiers inférieurs à 49, la moitié de 98, selon les modules 3, 5 et 7, voici ce que l'on obtient :

	3	5	7
19	×	×	
31	×	×	
37	×		×
3	×		
5		×	
7	×		×
11		×	×
13	×		
17			
23			×
29		×	×
41		×	
43	×		×
47			

Les deux solutions que sont 19 et 31 sont "semblables du point de vue de leur relation quadratique" aux modules 3, 5 et 7.

19 est aussi décomposant de Goldbach de $242 = 2.11^2$ mais ne l'est plus de $238 = 2.13^2$. Le raisonnement est similaire mais il faut alors tenir compte de toute une série d'autres modules qui se sont ajoutés à l'ensemble des modules inférieurs à la racine du nombre pair que l'on considère.

2.2 Exemple 3

$100 = 2^2.5^2$ est un carré. En appliquant le même raisonnement que précédem-ment, on cherche un nombre qui soit à la fois non-résidu de 3, 5 et 7. C'est le cas de 17 et de 47 qui sont tous deux des décomposants de Goldbach de 100.

2.3 Autres exemples

A partir de là, on décide de suivre l'exemple d'Euler : dans l'article *"Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs"*, il fournit des résultats exhaustifs jusqu'à 100.

[2]Elle correspond à l'écriture suivante utilisée par Gauss dans l'article 105 de la section Quatrième des Recherches Arithmétiques *"selon les modules a, b, c, etc."*.

Peut-être que l'étude des nombres pairs factorisés jusqu'à 100 (on laisse de côté les doubles de premiers qui vérifient trivialement la conjecture) va petit à petit nous faire comprendre comment il faut généraliser...

$8 = 2^3$.
Le raisonnement habituel amène à chercher un résidu de 3 or 3 est bien un décomposant de Goldbach de 8.

$12 = 2^2.3$.
L'inverse de 3 est résidu de 3. 5, qui est non résidu du seul diviseur impair de 12 de valuation p-adique impaire, est un décomposant de Goldbach de 12.

$16 = 2^4$.
5 non résidu de 3 est décomposant de Goldbach de 16.

$18 = 2.3^2$.
On cherche un résidu de 3 (selon le raisonnement habituel uniquement selon le module 3) et 7 fournit bien une décomposition de Goldbach de 18.

$20 = 2^2.5$.
On cherche un résidu de 3. 3 ou bien 7 fournissent tous deux des décompositions de Godlbach de 20.

$24 = 2^3.3$.
3 apparaît avec une valuation p-adique impaire dans la factorisation de 24. L'inverse de 3 est résidu de 3. Il s'avère que 5 et 11, tous deux non-résidus de 3, fournissent des décompositions de Goldbach de 24 ainsi que 7 qui quant à lui est non-résidu de 5.

$28 = 2^2.7$.
Modulo 3, l'inverse de 7 est 1 qui est résidu de 3. Modulo 5, l'inverse de 7 est 3 qui est non-résidu de 5. On cherche donc un nombre qui soit non-résidu de 3 et résidu de 5. 5 et 11 sont dans ce cas et fournissent tous les deux des décompositions de Goldbach de 28.

$30 = 2.3.5$.
Ici, faisons un petit aparté : 30 a "beaucoup" de petits décomposants, de même que 60, 90, 120, 150 ou 900, par exemple. L'étude des points de la comète de Goldbach, en février 2011, nous a montré que ces nombres pairs ont un nombre de décompositions de Goldbach "bien supérieurs" à leurs voisins. On le constate en utilisant l'article de Cantor qui avait vérifié la conjecture jusqu'à 1000 et qui avait émis quelques conjectures que l'on retrouve notamment dans le chapitre *Cantor et la Conjecture de Goldbach* de l'excellent livre d'Anne-Marie Décaillot *"Cantor et la France"*.
L'inverse de 3 est résidu de 3, l'inverse de 5 l'est de 5. On constate que *tous* les premiers autres que 2, 3 et 5 (les diviseurs de 30) fournissent des décompositions de Goldbach : 7, 11 et 13.
Pour le nombre pair $60 = 2^2.3.5$, même chose : *tous* les nombres premiers de 7 à 29 sans exception fournissent des décompositions de Goldbach de 60.
Pour $120 = 2^3.3.5$, tous les premiers compris entre 7 et 59 fournissent une décomposition de Goldbach de 120 sauf 29 et 43 (ce qui représente 12 décomposi-tions et 2 "ratages").
Pour $150 = 2.3.5^2$, les résidus de 19 que sont 11, 19 et 23 fournissent 3 décompo-sants, tandis que les résidus de 17 que sont 43, 47, 53 et 67 en fournissent 4 autres.
Pour $90 = 2.3^3.5$, 48 nombres premiers sur les 81 nombres premiers compris entre 13 et 443 permettent d'obtenir une décomposition de Goldbach [3].
Parmi ces nombres, $270 = 2.3^3.5$ a un nombre de décomposants de Goldbach (il en a 20) qui vaut environ le double de celui de ses voisins immédiats (268 et 272 en ont respectivement 9 et 8). On s'est intéressé à lui car la conjecture de Goldbach aura 270 ans en 2012...

L'étude de ces nombres qui ont beaucoup de petits facteurs premiers nous amène à croire qu'il suffit peut-être parfois que la relation "non-résidu de" soit vérifiée pour l'un des diviseurs seulement pour permettre

[3] On peut carrément (!) parler de rentabilité...

l'obtention d'un décomposant de Goldbach. Cela nous fait vivement souhaiter comprendre la page 112 des Recherches Arithmétiques dans laquelle Gauss utilise un raisonnement combinatoire[4].

Poursuivons notre liste des nombres pairs inférieurs à 100 non doubles de premiers.

$32 = 2^5$
On cherche un résidu de 3 et 5 à la fois. 19 fournit une décomposition de 32.

$36 = 2^2.3^2$
C'est un carré. 5 qui est non-résidu de 3 fournit une décomposition mais 7 résidu de 3 en fournit une également.

$40 = 2^3.5$
Les résidus de 11 que sont 3 et 11 fournissent chacun une décomposition. 17 non-résidu de 3 en fournit une également.

$42 = 2.3.7$
Les résidus de 5 que sont 5, 11, 19, 29 et 31 fournissent chacun une décomposition.

$44 = 2^2.11$
Les résidus de 3 que sont 3, 7 et 13 fournissent chacun une décomposition.

$48 = 2^4.3$
Les résidus de 5 que sont 5, 11, 19, 29, 31 et 41 fournissent une décomposition.

$50 = 2.5^2$
Les résidus de 3 que sont 3, 7, 13 et 19 fournissent chacun une décomposition.

$52 = 2^2.13$
Les non-résidus de 3 que sont 5, 11 et 23 fournissent chacun une décomposition.

$54 = 2.3^3$
Les non-résidus de 3 que sont 7 et 13 fournissent une décomposition.

$56 = 2^3.7$
Les résidus de 3 que sont 3, 13 et 19 (7 étant un diviseur de 56 ne peut fournir de décomposition) fournissent chacun une décomposition.

$64 = 2^6$
Les non-résidus de 3 que sont 5, 11, 17 et 23 fournissent une décomposition.

$66 = 2.3.11$
Les résidus de 29 que sont 5, 7, 13, 23 et 29 fournissent chacun une décomposition.

$68 = 2^2.17$
Observons la table : pour ne conserver que 7 et 31, il faut qu'il y ait une croix en colonne 3 et que les colonnes 5 et 7 soient l'inverse l'une de l'autre. Cependant alors 19 et 43 vérifient cette condition bien que ne fournissant pas de décompositions de Goldbach. On constate que leur complémentaire à n est à chaque fois un carré (49 et 25).

[4]Malheureusement, on trouve à la fin de cette page un *"Mais pour abréger, nous sommes forcés de ne pas donner plus de développement à la démonstration."* qui rappelle furieusement le *"La marge est trop petite."* de Fermat...

$70 = 2.5.7$
Les non-résidus de 3 que sont 11, 17, 23 et 29 fournissent une décomposition.

$72 = 2^3.3^2$
Les résidus de 5 que sont 5, 11, 19, 29 et 31 fournissent chacun une décomposition.

$76 = 2^2.19$
Les non-résidus de 3 que sont 5, 17, 23 et 29 fournissent chacun une décomposition.

$78 = 2.3.13$
Les résidus de 19 que sont 5, 7, 11, 17 et 19 fournissent chacun une décomposition.

$80 = 2^4.5$
Les résidus de 3 que sont 7, 13, 19 et 37 fournissent chacun une décomposition.

$84 = 2^2.3.7$
Les résidus de 5 que sont 5, 11, 31 et 41 fournissent chacun une décomposition, ainsi que les résidus de 13 que sont 13, 17 et 23 et enfin le résidu de 7 qu'est 37.

$88 = 2^3.11$
Les résidus de 5 que sont 5 et 41 fournissent chacun une décomposition, ainsi que les résidus de 13 que sont 17 et 29.

$90 = 2.3^2.5$
Les résidus de 19 que sont 7, 11, 17, 19 et 23 fournissent chacun une décomposition ainsi que les résidus de 7 que sont 29, 37 et 43.

$92 = 2^2.23$
Tous les résidus de 3 inférieurs à 36 que sont 3, 13, 19 et 31 fournissent chacun une décomposition.

$96 = 2^5.3$
Les résidus de 29 que sont 7, 13, 23 et 29 fournissent chacun une décomposition ainsi que les résidus de 3 que sont 37 et 43.

2.4 Pour résumer et tenter d'aller plus avant

Dans les listes de nombres suivantes, on fournit entre parenthèses après chaque nombre les modules p dont les résidus (R *suivi de* p) ou non-résidu (N *suivi de* p)[5] permettent d'en trouver le plus de décompositions de Goldbach.
On a trouvé des décomposants de Goldbach de n :

- qui étaient non-résidus du plus petit non-résidu de n pour les nombres pairs suivants : 16 ($N3$), 24 ($N5$), 28 ($N3$), 40 ($N3$), 52 ($N3$), 54 ($N3$), 64 ($N3$), 70 ($N3$), 76 ($N3$), 100 ($N3N5N7$), 242 ($N7$) ;
- qui étaient résidus d'un non-diviseur de n pour les nombres pairs suivants : 8 ($R3$), 20 ($R3$), 28 ($R5$), 30 ($R7$), 32 ($R3$), 40 ($R11$), 42 ($R5$), 44 ($R3$), 48 ($R5$), 50 ($R3$), 56 ($R3$), 60 ($R7$), 66 ($R29$), 68 ($R3$), 72 ($R5$), 78 ($R19$), 80 ($R3$), 84 ($R5$), 88 ($R5$), 90 ($R7$), 92 ($R3$), 96 ($R3$), 98 ($R3$), 120 ($R7$), 150 ($R17$), 242 ($R3$), 270 ($R7$), 900 ($R7$) ;
- qui étaient non-résidus d'un diviseur de valuation p-adique impaire pour les nombres pairs suivants : 12 ($N3$), 24 ($N3$) ;

[5] On reprend la notation de Gauss.

- qui étaient non-résidus d'un diviseur de valuation p-adique paire pour le nombre pair suivant : 36 ($N3$) ;
- qui étaient résidus d'un diviseur de valuation p-adique paire pour les nombres pairs suivants : 18 ($R3$), 36 ($R3$).

Les nombres des trois dernières catégories peuvent aisément être intégrés aux deux premières catégories. On a bien en tête la règle *"moins par moins donne plus, moins par plus donne moins"* pour les caractères résidu/non-résidu démontrée par Gauss dans l'article 98 de la section Quatrième des Recherches Arithmétiques.

Concernant la première catégorie, on fournit pour mémoire en annexe 1 les résidus quadratiques des nombres inférieurs à 100 pour vérification de ce que l'on a constaté.

Concernant la deuxième catégorie, même si la condition *résidu d'un non-diviseur* semble toujours permettre l'obtention d'un décomposant de Goldbach, on remarque également qu'on peut toujours trouver un nombre premier décomposant de Goldbach de n parmi les nombres premiers qui sont non-résidus de tous les diviseurs impairs de n et cette condition semble plus satisfaisante dans la mesure où Gauss fournit dans les articles 129 et 130 de la section Quatrième des Recherches Arithmétiques la démonstration d'un théorème selon lequel tout nombre premier de la forme $4n+1$ est toujours non-résidu d'un nombre premier au moins plus petit que lui. L'annexe 4 donne le détail de ce constat pour les nombres de la deuxième catégorie.

On a cependant beau essayer d'induire certaines formes des résultats ci-dessus, on ne trouve pas grand chose : il semblerait que les nombres pairs qui sont des puissances paires de 2 appartiennent toujours à la première classe identifiée alors que les nombres pairs puissances impaires de 2 appartiennent à la seconde, ou bien que les nombres premiers de la forme $4n+3$ apparaissent à une puissance impaire dans les nombres de la première classe mais on peut difficilement envisager de généraliser à partir de quelques nombres par ci, par là.

Il y a cependant une phrase de Gauss qui attire particulièrement notre attention : dans l'article 105, le module est composé, produit de premiers ou de puissances de premiers (ça pourrait être n dans notre cas) et Gauss écrit dans le deuxième paragraphe de cet article *que les différentes combinaisons donneront des valeurs différentes, et* ***qu'elles les donneront toutes***. Est-ce à dire qu'on peut toujours trouver un nombre premier satisfaisant les relations *"non-résidu"* qu'on cherche à satisfaire quel que soit n ?

On a vu qu'on doit étudier si les nombres premiers de valuation p-adique impaire sont résidus ou pas des modules premiers inférieurs à la racine du nombre pair considéré. Gauss conseille d'affecter les nombres premiers de la forme $4n+1$ du signe + et les nombres premiers de la forme $4n+3$ du signe $-$[6] et compter s'ils se présentent en nombre pair ou pas. Il faudrait peut-être mettre en oeuvre un raisonnement combinatoire tel que celui de l'article 148 page 111 pour montrer qu'un tel nombre premier existe toujours, qui fournit une décomposition de Goldbach de n. Dans l'article 148 en question, Gauss établit un classement des nombres plus petits que n et premiers à n selon qu'ils sont dans le premier cas non-résidus d'aucun diviseur de n ou bien non-résidu d'un nombre pair de diviseurs de n et dans le second cas non-résidus d'un nombre impair de diviseurs de n. Un tel classement serait-il pertinent pour le problème qui nous intéresse ?

3 *"Est résidu quadratique de"*, une relation *"presque-symétrique"*

3.1 Illustration de la loi de réciprocité quadratique pour les modules premiers

On rappelle que p est résidu quadratique de q s'il existe un carré auquel p est congru selon le module q. Par exemple, 3 est résidu quadratique de 37 et réciproquement car $3 \equiv 15^2 (mod\ 37)$ et $37 \equiv 1^2 (mod\ 3)$.

[6] Gauss les appelle les $4n-1$.

Selon un module premier, il y a autant de résidus que de non-résidus. Deux nombres complémentaires à p sont soit tous deux résidus ou bien tous deux non-résidus lorsque p est un $4n+1$, soit l'un résidu et l'autre non-résidu lorsque p est un $4n+3$.

Illustrons cela dans deux tableaux, l'un pour le module 13 de la forme $4n+1$, l'autre pour le module 19, de la forme $4n+3$: comme q et $n-q$ ont même carré selon le module p, on va les mettre dans une même colonne du tableau (les plus grands dans la première ligne, les plus petits dans la deuxième). On va indiquer pour mémoire le résidu minimum absolu de leur carré selon le module considéré dans la troisième ligne. On va utiliser la couleur bleue pour les résidus seulement et constater la relation de symétrie ou d'anti-symétrie du caractère *"résidu de"* qui lie les deux nombres d'une même colonne.

Selon le module 13, de la forme $4n+1$:

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

Selon le module 19, de la forme $4n+3$:

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

Gauss fournit une application simple de la loi de réciprocité quadratique aux nombres premiers selon leur forme à la page 116 des Recherches Arithmétiques, article 151 : *"il s'ensuit que la relation de p à q est la même que celle de q à p, quand p ou q est de la forme $4n+1$, et qu'elle est inverse quand p et q sont de la forme $4n+3$"*.

Rappelons la table de la relation qui en découle (c'est la table II des annexes des Recherches Arithmétiques). Cette table présente une *"presque-symétrie"* selon sa diagonale. On a noté par une croix noire la relation lorsqu'elle est symétrique (entre deux nombres premiers impairs dont l'un au moins est un $4n+1$) et par une croix bleue la relation lorsqu'elle est anti-symétrique (lorsque les deux nombres premiers impairs sont des $4n+3$).

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
2	×			×			×		×		×		×		×
3	×	×			×	×			×			×			×
5	×		×		×			×		×	×		×		
7	×	×		×				×		×	×	×			×
11	×		×	×	×			×				×		×	
13	×	×				×	×		×	×				×	
17	×					×	×	×						×	×
19	×	×	×				×	×			×				
23	×			×	×	×		×	×	×			×	×	
29	×		×	×		×			×	×					
31	×	×	×		×			×	×		×		×	×	
37	×	×		×	×							×	×		×
41	×		×						×		×	×	×	×	
43	×	×		×		×	×		×				×	×	
47	×				×		×	×	×		×	×		×	×

En annexe 5, on illustre par les tables que les symétrie ou anti-symétrie du caractère résidu sont bien moins évidentes selon les modules impairs mais elles existent.

3.2 Illustrations du théorème fondamental dans le cas des modules pairs[7]

Au tout début de ces recherches, j'avais la conviction que la section Quatrième des Recherches Arithmétiques fournirait la solution au problème de Goldbach. J'avais étudié les résidus quadratiques mais mon problème était que, pour aller plus vite, je ne considérais dans mes tables que les seuls nombres impairs, et je perdais ainsi des informations précieuses qui permettent de faire apparaître une propriété de symétrie ou anti-symétrie verticale qui va être présentée maintenant.

3.2.1 Nombres pairs doubles de nombres premiers

On va maintenant s'intéresser aux nombres pairs $2p$ qui sont doubles de nombres premiers. Bien que vérifiant trivialement la conjecture, ils vont s'avérer présenter la propriété qu'on a découverte, et qui lie le caractère résidu de x à celui de $x+p$ parce qu'ils sont tous de la forme $4n+2$[8].
On s'intéresse notamment à ces nombres car l'étude des points de la comète de Goldbach en février 2011 nous a montré que ces nombres semblent *"minimiser"* la comète (avoir peu de décompositions de Goldbach comparativement à tous les autres). On a une explication heuristique de ce phénomène (ils n'ont pas de diviseurs autres qu'eux-mêmes et par ce que j'ai appelé la méthode du *"pliage de tissu"*, leurs colonnes s'éliminent systématiquement deux par deux au lieu de s'éliminer une par une comme elles le font dans le cas des diviseurs, ce qui minimisent le nombre de décompositions).

Si le nombre premier est un $4n+1$, on voit selon $2p$ une symétrie verticale qui fait que $x \ R \ 2p \iff x+p \ R \ 2p.$;
Si c'est un $4n+3$, on voit selon $2p$ une anti-symétrie verticale qui fait également que $x \ R \ 2p \iff x+p \ R \ 2p.$
La différence entre les deux sortes de nombres premiers est que dans un cas, les colonnes (qui contiennent un nombre x et son complémentaire à $2p$ qui est $2p-x$) soit contiennent deux résidus, soit contiennent deux non-résidus, alors que dans l'autre cas, ces deux cas peuvent se produire mais existent également des colonnes dans lesquelles l'un des nombres est un résidu et l'autre un non-résidu.

On omet dorénavant la ligne des restes des carrés dans les tables. On la remplace par une ligne de croix qui indique les décompositions de Goldbach (on suit la convention de Cantor qui consiste à considérer que 1 est un décomposant de Goldbach de $2p$ si $2p-1$ est premier).

On constate selon les modules $10, 26, 34, 58, 74, 82$ une symétrie verticale qui fait que $x \ R \ 2p \iff x+p \ R \ 2p.$

Selon le module 10, de la forme $2(4n+1)$:

10	9	8	7	6	5
0	1	2	3	4	5
			×		×

Selon le module 26, de la forme $2(4n+1)$:

26	25	24	23	22	21	20	19	18	17	16	15	14	13
0	1	2	3	4	5	6	7	8	9	10	11	12	13
			×				×						×

Selon le module 34, de la forme $2(4n+1)$:

34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			×		×						×						×

[7] Ou encore pour paraphraser le titre de l'article d'Euler *"Découverte d'une loi tout extraordinaire des résidus/non-résidus des modules pairs* $4n+2$ *:* $x \ R \ p \iff x+p \ R \ 2p$

[8] Si $2a$ est de la forme $2(4n+1)$, $2a = 8n+2 = 2(4n)+2 = 4(2n)+2 = 4b+2$ tandis que si $2a$ est de la forme $2(4n+3)$, $2a = 2(4n+3) = 8n+6 = 8n+4+2 = 4(2n)+4+2 = 4(2n+1)+2 = 4b+2$.

Selon le module 58, de la forme $2(4n+1)$:

58	57	56	55	54	53	52	51	50	49	48	47	46	45	44
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
					×						×			

43	42	41	40	39	38	37	36	35	34	33	32	31	30	29
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
		×												×

Selon le module 74, de la forme $2(4n+1)$:

74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
	×		×				×						×					

55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
												×						×

Selon le module 82, de la forme $2(4n+1)$:

82	81	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
			×								×									

61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41
		×						×												×

Voyons maintenant les modules doubles de premiers selon lesquels la symétrie devient une anti-symétrie. Selon ces modules $6, 14, 22, 38, 46, 62, 86, 94$, on constate une anti-symétrie verticale qui fait que $x \; R \; 2p \iff x+p \; R \; 2p$.

Selon le module 6, de la forme $2(4n+3)$:

6	5	4	3
0	1	2	3
	×		×

Selon le module 14, de la forme $2(4n+3)$:

14	13	12	11	10	9	8	7
0	1	2	3	4	5	6	7
	×		×				×

Selon le module 22, de la forme $2(4n+3)$:

22	21	20	19	18	17	16	15	14	13	12	11
0	1	2	3	4	5	6	7	8	9	10	11
			×		×						×

Selon le module 38, de la forme $2(4n+3)$:

38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20	19
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
	×						×												×

Selon le module 46, de la forme $2(4n+3)$:

46	45	44	4	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
			×		×												×						×

Selon le module 62, de la forme $2(4n+3)$:

62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	×		×												

46	45	44	43	42	41	40	39	38	37	36	35	34	33	32	31
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
			×												×

Selon le module 86, de la forme $2(4n+3)$:

86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
			×				×						×						×		

64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43
																					×

Selon le module 94, de la forme $2(4n+3)$:

94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
					×						×												×

70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
																	×						

3.2.2 Nombres pairs doubles d'impairs-non premiers

Selon les modules qui sont des nombres pairs doubles d'impairs non-premiers (les $4n+2$ qui ne sont pas doubles d'un nombre premier impair), $x \ R \ 2p \iff x+p \ R \ 2p$.

Selon le module $18 = 2.3^2$, de la forme $2(4n+3)^2$:

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

Selon le module $30 = 2p = 2.3.5$, de la forme $2(4n+3)(4n+1)$:

30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	4	9	16	25	6	19	4	21	13	1	24	19	16	15

Selon le module 30, en ne conservant que les colonnes des nombres premiers à 30, les relations verticales disparaissent :

29	23	19	17
1	7	11	13
1	19	1	19

Selon le module $42 = 2.3.7$, de la forme $2(4n+3)(4n'+3)$:

42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
	×				×						×		×						×		

Selon le module $50 = 2.5^2$, de la forme $2(4n+1)^2$:

50	49	48	47	46	45	44	43	42	41	40	39	38
0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	4	9	16	25	36	49	14	31	0	21	44

37	36	35	34	33	32	31	30	29	28	27	26	25
13	14	15	16	17	18	19	20	21	22	23	24	25
19	46	25	6	39	24	11	0	41	34	29	26	25

Selon le module $54 = 2.3^3$, de la forme $2(4n+3)^3$:

54	53	52	51	50	49	48	47	46	45	44	43	42	41
0	1	2	3	4	5	6	7	8	9	10	11	12	13
	×						×				×		×

40	39	38	37	36	35	34	33	32	31	30	29	28	27
14	15	16	17	18	19	20	21	22	23	24	25	26	27
			×						×				

Selon le module $66 = 2.3.11$, de la forme $2(4n+3)(4n'+3)$:

66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
					×		×						×			

49	48	47	46	45	44	43	42	41	40	39	38	37	36	35	34	33
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
		×				×						×				

Selon le module $70 = 2.5.7$, de la forme $2(4n+1)(4n'+3)$:

70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
			×								×						×

52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36	35
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
					×						×						

Selon le module $78 = 2.3.13$, de la forme $2(4n+3)(4n'+1)$:

78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
					×		×				×						×		×

58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
											×						×		

Selon le module $90 = 2.3^2.5$, de la forme $2(4n+3)^2(4n'+1)$:

90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	×						×				×						×		×			

67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45
23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
×						×		×						×						×		

Selon le module $98 = 2.7^2$, de la forme $2(4n+3)^2$:

98	97	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
	×																		×					

73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49
						×						×												

Il semblerait que si la factorisation de n ne contient aucun nombre premier impair de la forme $4n+3$, on constate une symétrie verticale qui fait que

$$x \; R \; 2p \iff x+p \; R \; 2p.$$

Tandis que si la factorisation de n contient un nombre premier de la forme $4n+3$ au moins, on constate une anti-symétrie verticale qui fait également que

$$x \; R \; 2p \iff x+p \; R \; 2p.$$

.
Cette propriété découle vraisemblablement de la loi de réciprocité quadratique.

3.2.3 Nombres pairs doubles de pairs

Pour les nombres pairs doubles de pairs, on ne constate pas de symétrie ou d'anti-symétrie verticale par rapport à la ligne médiane du tableau symbolisée par deux doubles barres verticales autour de la colonne médiane. On essaiera cependant de comprendre les relations existant entre les caractères *résidu/non-résidu de* $2p$ de x et $x+p$.

Selon le module 8, de la forme 2^3 :

8	7	6	5	4
0	1	2	3	4
	×		×	

Selon le module $12 = 2^2.3$, de la forme $4(4n+3)$:

12	11	10	9	8	7	6
0	1	2	3	4	5	6
	×				×	

Selon le module 16, de la forme 2^4 :

16	15	14	13	12	11	10	9	8
0	1	2	3	4	5	6	7	8
			×		×			

Selon le module $20 = 2^2.5$, de la forme $4(4n+1)$:

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

Selon le module $24 = 2^3.3$, de la forme $2^3(4n+3)$:

24	23	22	21	20	19	18	17	16	15	14	13	12
0	1	2	3	4	5	6	7	8	9	10	11	12
	×				×		×				×	

Selon le module $28 = 2^2.7$, de la forme $4(4n+3)$:

28	27	26	25	24	23	22	21	20	19	18	17	16	15	14
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
					×						×			

Selon le module 32, de la forme 2^5 :

32	31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	×		×										×			

Selon le module $36 = 2^2.3^2$, de la forme $4(4n+3)^2$:

36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	2	20	19	18
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
					×		×						×				×	

Selon le module $40 = 2^4.5$, de la forme $2^4(4n+1)$:

40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22	21	20
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
			×								×						×			

Selon le module $44 = 2^2.11$, de la forme $4(4n+3)$:

44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23	22
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	×		×				×						×									

Selon le module $48 = 2^4.3$, de la forme $2^4(4n+3)$:

48	47	46	45	44	4	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
					×		×				×						×		×					

Selon le module $52 = 2^2.13$, de la forme $4(4n+1)$:

52	51	50	49	48	47	46	45	44	4	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26
0	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	26
					×						×												×			

Selon le module $56 = 2^3.7$, de la forme $2^3(4n+3)$:

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
			×										×	

41	40	39	38	37	36	35	34	33	32	31	30	29	28
15	16	17	18	19	20	21	22	23	24	25	26	27	28
				×									

Selon le module $60 = 2^2.3.5$, de la forme $4(4n+3)(4n'+1)$:

60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	×						×						×		

44	43	42	41	40	39	38	37	36	35	34	33	32	31	30
16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
	×		×				×						×	

Selon le module 64, de la forme 2^6 :

64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
			×		×						×					

47	46	45	44	43	42	41	40	39	38	37	36	35	34	33	32
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
×						×									

Selon le module $68 = 2^2.17$, de la forme $4(4n + 1)$:

68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
	×						×										

50	49	48	47	46	45	44	4	42	41	40	39	38	37	36	35	34
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
													×			

Selon le module $72 = 2^3.3^2$, de la forme $2^3(4n + 3)^2$:

72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54
0	1	2	3	4	5	6	7	8	9	10	11	1	13	14	15	16	17	18
	×				×						×		×					

53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38	37	36
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
×										×		×					

Selon le module $76 = 2^2.19$, de la forme $4(4n + 3)$:

76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
0	1	2	3	4	5	6	7	8	9	10	11	1	13	14	15	16	17	18	19
			×		×												×		

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38
20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38
			×						×									

Selon le module $80 = 2^4.5$, de la forme $2^4(4n+1)$:

80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60
0	1	2	3	4	5	6	7	8	9	10	11	1	13	14	15	16	17	18	19	20
	×						×						×						×	

59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40
2	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
																×			

Selon le module $84 = 2^2.3.7$, de la forme $4(4n+3)(4n'+3)$:

84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66	65	64	63
0	1	2	3	4	5	6	7	8	9	10	11	1	13	14	15	16	17	18	19	20	21
	×				×						×		×				×				

62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44	43	42
22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
	×								×						×				×	

Selon le module $88 = 2^3.11$, de la forme $2^3(4n+3)$:

88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68	67	66
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
					×												×					

65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45	44
23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
						×												×			

Selon le module $92 = 2^2.23$, de la forme $4(4n+3)$:

92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	2	22	23
			×										×						×				

68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
							×															

Selon le module $96 = 2^5.3$, de la forme $2^5(4n+3)$:

96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	2	22	23	24
							×						×				×						×	

71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48
25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
				×								×						×					

Selon le module $100 = 2^2.5^2$, de la forme $4(4n+1)^2$:

100	99	98	97	96	95	94	93	92	91	90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75
0	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
			×								×						×								

74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50
26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
			×												×						×			

3.3 Progressions arithmétiques

Gauss fait mention de nombres appartenant à des progressions arithmétiques dans les articles 104, 147, 148 et 149 de la section Quatrième des Recherches Arithmétiques.

Voyons si les cas étudiés permettent d'obtenir des généralisations.
La première catégorie, pour laquelle un non-résidu du plus petit non-résidu de n fournit systématiquement une décomposition de Goldbach, les nombres sont $16, 24, 28, 40, 52, 54, 64, 70, 100$: à part 3 d'entre eux, (24, 54 et 70), ils sont tous de la forme $12k+4$. Cette notion de *non-résidu d'un non-résidu* est cependant problématique car la relation *résidu* ou la relation *non-résidu* ne sont pas transitives.

Dans la deuxième catégorie, pour lesquels on trouve toujours un non-résidu de tous les diviseurs impairs de n fournissant une décomposition de Goldbach, ils sont tous des formes suivantes : $12k$, $12k+2$, $12k+6$, $12k+8$ ou $12k+10$.

Mais en unifiant les deux catégories en une, dans la mesure où l'on peut toujours pour les nombres de la première catégorie trouver un décomposant de Goldbach qui soit non-résidu de tous les diviseurs de n, il semblerait qu'on puisse pour tous les nombres pairs n trouver un nombre premier non-résidu de tous les diviseurs impairs de n qui fournit une décomposition de Godlbach de n.

Essayons sur un nombre plus grand : $1182666 = 2.3.439.449$. Le nombre premier 157 est non-résidu à la fois de 3, 49 et 449 et il fournit une décomposition de Goldbach de 1182666.

4 Rêves d'un prince

On peut trouver sur la toile le journal mathématique de Gauss. On y lit que Gauss a étudié la conjecture de Goldbach le 14 mai 1796. On peut imaginer que les deux premières lettres mystérieuses du mot GEGAN qui apparaît dans la citation "Vicimus GEGAN" du 11 octobre 1796 sont les initiales respectives de Goldbach et Euler...

Annexe 1 : Résidus quadratiques des nombres inférieurs à 100

2 : 1
3 : 1
4 : 1
5 : 1 4
6 : 1 3 4
7 : 1 2 4
8 : 1 4
9 : 1 4 7
10 : 1 4 5 6 9
11 : 1 3 4 5 9
12 : 1 4 9
13 : 1 3 4 9 10 12
14 : 1 2 4 7 8 9 11
15 : 1 4 6 9 10
16 : 1 4 9
17 : 1 2 4 8 9 13 15 16
18 : 1 4 7 9 10 13 16
19 : 1 4 5 6 7 9 11 16 17
20 : 1 4 5 9 16
21 : 1 4 7 9 15 16 18
22 : 1 3 4 5 9 11 12 14 15 16 20
23 : 1 2 3 4 6 8 9 12 13 16 18
24 : 1 4 9 12 16
25 : 1 4 6 9 11 14 16 19 21 24
26 : 1 3 4 9 10 12 13 14 16 17 22 23 25
27 : 1 4 7 9 10 13 16 19 22 25
28 : 1 4 8 9 16 21 25
29 : 1 4 5 6 7 9 13 16 20 22 23 24 25 28
30 : 1 4 6 9 10 15 16 19 21 24 25
31 : 1 2 4 5 7 8 9 10 14 16 18 19 20 25 28
32 : 1 4 9 16 17 25
33 : 1 3 4 9 12 15 16 22 25 27 31
34 : 1 2 4 8 9 13 15 16 17 18 19 21 25 26 30 32 33
35 : 1 4 9 11 14 15 16 21 25 29 30
36 : 1 4 9 13 16 25 28
37 : 1 3 4 7 9 10 11 12 16 21 25 26 27 28 30 33 34 36
38 : 1 4 5 6 7 9 11 16 17 19 20 23 24 25 26 28 30 35 36
39 : 1 3 4 9 10 12 13 16 22 25 27 30 36
40 : 1 4 9 16 20 24 25 36
41 : 1 2 4 5 8 9 10 16 18 20 21 23 25 31 32 33 36 37 39 40
42 : 1 4 7 9 15 16 18 21 22 25 28 30 36 37 39
43 : 1 4 6 9 10 11 13 14 15 16 17 21 23 24 25 31 35 36 38 40 41
44 : 1 4 5 9 12 16 20 25 33 36 37
45 : 1 4 9 10 16 19 25 31 34 36 40
46 : 1 2 3 4 6 8 9 12 13 16 18 23 24 25 26 27 29 31 32 35 36 39 41
47 : 1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42
48 : 1 4 9 16 25 33 36
49 : 1 2 4 8 9 11 15 16 18 22 23 25 29 30 32 36 37 39 43 44 46
50 : 1 4 6 9 11 14 16 19 21 24 25 26 29 31 34 36 39 41 44 46 49
51 : 1 4 9 13 15 16 18 19 21 25 30 33 34 36 42 43 49
52 : 1 4 9 12 13 16 17 25 29 36 40 48 49
53 : 1 4 6 7 9 10 11 13 15 16 17 24 25 28 29 36 37 38 40 42 43 44 46 47 49 52
54 : 1 4 7 9 10 13 16 19 22 25 27 28 31 34 36 37 40 43 46 49 52
55 : 1 4 5 9 11 14 15 16 20 25 26 31 34 36 44 45 49
56 : 1 4 8 9 16 25 28 32 36 44 49
57 : 1 4 6 7 9 16 19 24 25 28 30 36 39 42 43 45 49 54 55
58 : 1 4 5 6 7 9 13 16 20 22 23 24 25 28 29 30 33 34 35 36 38 42 45 49 51 52 53 54 57

59 : 1 3 4 5 7 9 12 15 16 17 19 20 21 22 25 26 27 28 29 35 36 41 45 46 48 49 51 54 53 57
60 : 1 4 9 16 21 24 25 36 40 45 49
61 : 1 3 4 5 9 12 13 14 15 16 19 20 22 25 27 34 36 39 41 42 45 46 47 48 49 52 54 56 57 58 60
62 : 1 2 4 5 7 8 9 10 14 16 18 19 20 25 28 31 32 33 35 36 38 39 40 41 45 47 49 54 50 51 56 59
63 : 1 4 7 9 16 18 22 25 28 36 37 43 46 49 58
64 : 1 4 9 16 17 25 33 36 41 49 57
65 : 1 4 9 10 14 16 25 26 29 30 35 36 39 40 49 51 55 56 61 64
66 : 1 3 4 9 12 15 16 22 25 27 31 33 34 36 37 42 45 48 49 55 58 60 64
67 : 1 4 6 9 10 14 15 16 17 19 21 22 23 24 25 26 29 33 35 36 37 39 40 47 49 54 55 56 59 60 62 64 65
68 : 1 4 8 9 13 16 17 21 25 32 33 36 49 52 53 60 64
69 : 1 3 4 6 9 12 13 16 18 24 25 27 31 36 39 46 48 49 52 54 55 58 64
70 : 1 4 9 11 14 15 16 21 25 29 30 35 36 39 44 46 49 50 51 56 60 64 65
71 : 1 2 3 4 5 6 8 9 10 12 15 16 18 19 20 24 25 27 29 30 32 36 37 38 40 43 45 48 49 50 54 57 58 60 64
72 : 1 4 9 16 25 28 36 40 49 52 64
73 : 1 2 3 4 6 8 9 12 16 18 19 23 24 25 27 32 35 36 37 38 41 46 48 49 50 54 55 57 61 64 65 67 69 70 71 72
74 : 1 3 4 7 9 10 11 12 16 21 25 26 27 28 30 33 34 36 37 38 40 41 44 46 47 48 49 53 58 62 63 64 65 67 70 71 73
75 : 1 4 6 9 16 19 21 24 25 31 34 36 39 46 49 51 54 61 64 66 69
76 : 1 4 5 9 16 17 20 24 25 28 36 44 45 49 57 61 64 68 73
77 : 1 4 9 11 14 15 16 22 23 25 36 37 42 44 49 53 56 58 60 64 67 70 71
78 : 1 3 4 9 10 12 13 16 22 25 27 30 36 39 40 42 43 48 49 51 52 55 61 64 66 69 75
79 : 1 2 4 5 8 9 10 11 13 16 18 19 20 21 22 23 25 26 31 32 36 38 40 42 44 45 46 49 50 51 52 55 62 64 65 67 72 73 76
80 : 1 4 9 16 20 25 36 41 49 64 65
81 : 1 4 7 9 10 13 16 19 22 25 28 31 34 36 37 40 43 46 49 52 55 58 61 63 64 67 70 73 76 79
82 : 1 2 4 5 8 9 10 16 18 20 21 23 25 31 32 33 36 37 39 40 41 42 43 45 46 49 50 51 57 59 61 62 64 66 72 73 74 77 78 80 81
83 : 1 3 4 7 9 10 11 12 16 17 21 23 25 26 27 28 29 30 31 33 36 37 38 40 41 44 48 49 51 59 61 63 64 65 68 69 70 75 77 78 81
84 : 1 4 9 16 21 25 28 36 37 49 57 60 64 72 81
85 : 1 4 9 15 16 19 21 25 26 30 34 35 36 49 50 51 55 59 60 64 66 69 70 76 81 84
86 : 1 4 6 9 10 11 13 14 15 16 17 21 23 24 25 31 35 36 38 40 41 43 44 47 49 52 53 54 56 57 58 59 60 64 66 67 68 74 78 79 81 83 84
87 : 1 4 6 7 9 13 16 22 24 25 28 30 33 34 36 42 45 49 51 52 54 57 58 63 64 67 78 81 82
88 : 1 4 9 12 16 20 25 33 36 44 48 49 56 60 64 80 81
89 : 1 2 4 5 8 9 10 11 16 17 18 20 21 22 25 32 34 36 39 40 42 44 45 47 49 50 53 55 57 64 67 68 69 71 72 73 78 79 80 81 84 85 87 88
90 : 1 4 9 10 16 19 25 31 34 36 40 45 46 49 54 55 61 64 70 76 79 81 85
91 : 1 4 9 14 16 22 23 25 29 30 35 36 39 42 43 49 51 53 56 64 65 74 77 78 79 81 88
92 : 1 4 8 9 12 13 16 24 25 29 32 36 41 48 49 52 64 69 72 73 77 81 85
93 : 1 4 7 9 10 16 18 19 25 28 31 33 36 39 40 45 49 51 63 64 66 67 69 70 72 76 78 81 82 87 90
94 : 1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42 47 48 49 50 51 53 54 55 56 59 61 63 64 65 68 71 72 74 75 79 81 83 84 89
95 : 1 4 5 6 9 11 16 19 20 24 25 26 30 35 36 39 44 45 49 54 55 61 64 66 74 76 80 81 85
96 : 1 4 9 16 25 33 36 48 49 57 64 73 81
97 : 1 2 3 4 6 8 9 11 12 16 18 22 24 25 27 31 32 33 35 36 43 44 47 48 49 50 53 54 61 62 64 65 66 70 72 73 75 79 81 85 86 88 89 91 93 94 95 96
98 : 1 2 4 8 9 11 15 16 18 22 23 25 29 30 32 36 37 39 43 44 46 49 50 51 53 57 58 60 64 65 67 71 72 74 78 79 81 85 86 88 92 93 95
99 : 1 4 9 16 22 25 27 31 34 36 37 45 49 55 58 64 67 70 81 82 88 91 97
100 : 1 4 9 16 21 24 25 29 36 41 44 49 56 61 64 69 76 81 84 89 96

Annexe 2 : Extraits de la section Quatrième *"Des Congruences du second degré"* des Recherches Arithmétiques

On ne fait ici que recopier des extraits de la section Quatrième des Recherches Arithmétiques qu'il faudrait bien maîtriser pour pouvoir démontrer que l'existence d'un décomposant de Goldbach pour chaque nombre pair découle de l'existence d'au moins une solution pour un certain système de congruences (ou incongruences, c'est quasiment l'opposé) quadratiques, cette dernière existence découlant quant à elle du théorème d'or appliqué aux nombres adéquats. Les articles les plus difficiles, mais peut-être les plus utiles pour notre problème sont **les articles** 104 **et** 105 puis 147**,** 148 **et** 149.

page 69, article 94 : THÉORÈME. Un nombre quelconque m étant pris pour module, il ne peut y avoir dans la suite $1, 2, 3 \dots m-1$, plus de $\frac{1}{2}m+1$ nombres, quand m est pair, et plus de $\frac{1}{2}m+\frac{1}{2}$, quand m est impair, qui soient congrus à un carré.

page 70, article 96 : Le nombre premier p étant pris pour module, la moitié des nombres $1, 2, 3 \dots p-1$, sera composée de résidus quadratiques, et l'autre moitié de non-résidus, c'est-à-dire qu'il y aura $\dfrac{1}{2}(p-1)$ résidus, et autant de non-résidus.

page 72, article 98 : THÉORÈME. Le produit de deux résidus quadratiques d'un nombre premier p est un résidu ; le produit d'un résidu et d'un non-résidu est non-résidu ; enfin le produit de deux non-résidus est résidu.
1°. Soient A et B les résidus qui proviennent des carrés a^2, b^2, ou soient $A \equiv a^2 \ (mod\ p)$ et $B \equiv b^2$, on aura $AB \equiv a^2b^2$, c'est-à-dire qu'il sera un résidu.
2°. Quand A est résidu, ou que $A \equiv a^2$, mais que B est non-résidu, AB est non-résidu. Soit en effet, s'il se peut $AB \equiv k^2$ et $\frac{k}{a} \ (mod\ p) \equiv b$, on aura $a^2B \equiv a^2b^2$ et partant $B \equiv b^2$, contre l'hypothèse.
Autrement. Si l'on multiplie par A les $\frac{p-1}{2}$ nombres de la suite $1, 2, 3 \dots p-1$, qui sont résidus, tous les produits seront des résidus quadratiques, et ils seront tous incongrus. Or si l'on multiplie par A un nombre B non-résidu, le produit ne sera congru à aucun des précédents : donc, s'il était résidu, il y aurait $\frac{1}{2}(p+1)$ résidus incongrus, parmi lesquels ne serait pas 0, ce qui est impossible (n^o 96).
3°. Soient A et B deux nombres non-résidus, en multipliant par A tous les nombres qui sont résidus dans la suite $1, 2, 3, \dots p-1$, on aura $\frac{p-1}{2}$ non-résidus, incongrus entr'eux (2°). Or le produit AB ne peut être congru à aucun de ceux-là ; donc s'il était non-résidu, on aurait $\frac{p+1}{2}$ non-résidus incongrus entr'eux ; ce qui est impossible (n^o 96).
Ces théorèmes se déduisent encore plus facilement des principes de la section précédente. En effet, puisque l'indice d'un résidu est toujours pair, et celui d'un non-résidu toujours impair, l'indice du produit de deux résidus ou non-résidus sera pair, et partant, le produit sera lui-même un résidu. Au contraire, si l'un des facteurs est non-résidu, et l'autre résidu, l'indice sera impair, et le produit non-résidu.
On peut aussi faire usage des deux méthodes pour démontrer ce THÉORÈME[9] : *la valeur de l'expression* $\frac{a}{b} \ (mod\ p)$*, sera un résidu, quand les nombres a et b seront tous les deux résidus ou non-résidus. Elle sera un non-résidu, quand l'un des nombres a et b sera résidu et l'autre non-résidu.* On le démontrerait encore en renversant les théorèmes précédents.

page 73, article 99 : Généralement, le produit de tant de facteurs qu'on voudra est un résidu, soit lorsque tous les facteurs en sont eux-mêmes, soit lorsque le nombre de facteurs non-résidus est pair ; mais quand le nombre des facteurs non-résidus est impair, le produit est non-résidu. On peut donc juger facilement si un nombre composé est résidu ou non ; pourvu qu'on sache ce que sont ses différents facteurs. Aussi dans la Table II, nous n'avons admis que les nombres premiers. Quant à sa disposition, les modules sont en marge[10], en tête les nombres premiers successifs ; quand l'un de ces derniers est résidu, on a placé un trait dans l'espace qui correspond au module et à ce nombre ; quand il est non-résidu, on a laissé l'espace vide.

page 73, article 100 : Si l'on prend pour module la puissance p^n d'un nombre premier, p étant > 2, une moitié des nombres non-divisibles par p et $< p^n$ seront des résidus, et l'autre des non-résidus ; c'est-à-dire

[9] Ici, je mets les petites capitales à ce mot bien qu'elles ne soient pas présentes dans les Recherches Arithmétiques dans la mesure où la démonstration de ce théorème n'est pas fournie.
[10] On verra bientôt comment on peut se passer des modules composés.

qu'il y en aura $\frac{p-1}{2}.p^{n-1}$ de chaque espèce.
En effet, si r est un résidu, il sera congru à un carré dont la racine ne surpasse pas la moitié du module (n^o 94) ; et l'on voit facilement qu'il y a $\frac{1}{2}p^{n-1}(p-1)$ nombres $< \frac{p^n}{2}$ et non-divisibles par p. Ainsi il reste à démontrer que les carrés de tous ces nombres sont incongrus, ou qu'ils donnent des résidus différents. Or si deux nombres a et b non-divisibles par p et plus petits que la moitié du module, avaient leurs carrés congrus, on aurait $a^2 - b^2$ ou $(a+b)(a-b)$ divisible par p^n, en supposant $a > b$, ce qui est permis. Mais cette condition ne peut avoir lieu, à moins que l'un des deux nombres $(a-b)$, $(a+b)$ ne soit divisible par p^n, ce qui est impossible, puisque chacun d'eux est plus petit que p^n, ou bien que l'un étant divisible par p^μ, l'autre le soit par $p^{\nu-\mu}$ ou chacun d'eux par p ; ce qui est encore impossible, puisqu'il s'ensuivrait que la somme $2a$ et la différence $2b$, et partant a et b eux-mêmes seraient divisibles par p, contre l'hypothèse. Donc enfin parmi les nombres non-divisibles par p et moindres que le module, il y a $\frac{p-1}{2}p^{n-1}$ résidus, et les autres, en même nombre, sont non-résidus.

page 74, article 101 : Tout nombre non-divisible par p, qui est résidu de p, sera aussi résidu de p^n ; celui qui ne sera pas résidu de p ne le sera pas non plus de p^n.
La seconde partie de cette proposition est évidente par elle-même ; ainsi si la première n'était pas vraie, parmi les nombres plus petits que p^n et non-divisibles par p, il y en aurait plus qui fussent résidus de p qu'il n'y en aurait qui le fussent de p^n, c'est-à-dire plus de $\frac{1}{2}p^{n-1}(p-1)$. Mais on peut voir sans peine que le nombre des résidus de p qui se trouvent entre 1 et p^n, est précisément $\frac{1}{2}p^{n-1}(p-1)$.
Il est tout aussi facile de trouver effectivement un carré qui soit congru à un résidu donné, suivant le module p^n, si l'on connaît un carré congru à ce résidu suivant le module p.
Soit en effet a^2 un carré congru au résidu donné A, suivant le module p^μ, on en déduira, de la manière suivante, un carré $\equiv A$, suivant le module p^ν, ν étant $> \mu$ et non plus grand que 2μ. Supposons que la racine du carré cherché soit $\pm a + xp^\mu$; et il est aisé de s'assurer que c'est là la forme qu'elle doit avoir. Il faut donc qu'on ait $a^2 \pm 2axp^\mu + x^2p^{2\mu} \equiv A \ (mod\ p^\nu)$, ou comme $2\mu > \nu$, on aura $\pm 2axp^\mu \equiv A - a^2 \ (mod\ p^\nu)$. Soit $A - a^2 = p^\mu.d$, on aura $\pm 2ax \equiv d \ (mod\ p^{\nu-\mu})$; donc x sera la valeur de l'expression $\pm\frac{d}{2a} \ (mod\ p^{\nu-\mu})$. Ainsi étant donné un carré congru à A, suivant le module p, on en déduira un carré congru à A, suivant le module p^2 ; de là au module p^4, au module p^8, etc.
Exemple. Etant proposé le résidu 6 congru au carré 1, suivant le module 5, on trouve le carré 9^2 auquel il est congru suivant le module 25, 16^2 auquel il est congru suivant le module 125, etc.

page 75, article 102 : Quant à ce qui regarde les nombres divisibles par p, il est clair que leurs carrés seront divisibles par p^2, et que partant tous les nombres qui seront divisibles par p et non par p^2, seront non-résidus de p^n. Et en général, si l'on propose le nombre p^kA, A n'étant pas divisible par p, il y aura trois cas à distinguer :
1°. Si $k \geq n$, on aura $p^kA \equiv 0 \ (mod\ p^n)$, c'est-à-dire qu'il sera résidu.
2°. Si $k < n$ et impair, p^kA sera non-résidu.
3°. Si $k < n$ et pair, p^kA sera résidu ou non-résidu de p^n suivant que A sera résidu ou non-résidu de p.

page 76, article 103 : Comme nous avons commencé (n^o 100) par exclure le cas où $p = 2$, il faut ajouter quelque chose à ce sujet. Quand 2 est module, tous les nombres sont résidus, et il n'y en a point de non-résidus. Quand le module est 4, tous les nombres impairs de la forme $4k+1$ sont résidus, et tous ceux de la forme $4k+3$ sont non-résidus. Enfin, quand le module est 8 ou une plus haute puissance de 2, tous les nombres impairs de la forme $8k+1$ sont résidus, et les autres, ou ceux de la forme $8k+3$, $8k+5$, $8k+7$ sont non-résidus ;

page 77, article 104 : Pour ce qui regarde le nombre de valeurs différentes, c'est-à-dire incongrues suivant le module, que peut admettre l'expression $V = \sqrt{A} \ (mod\ p^n)$, pourvu que A soit un résidu de p^n, on déduit facilement de ce qui précède, les conclusions suivantes. Nous supposons toujours que p est un nombre premier et, pour abréger, nous considérons en même temps le cas où $n = 1$.
1^o. Si A n'est pas divisible par p, V n'a qu'une seule valeur pour $p = 2$ et $n = 1$; ce sera $V \equiv 1$; il en a deux quand p est impair, ou bien quand on a $p = 2$ et $n = 2$; et, si l'une est $\equiv \nu$, l'autre sera $\equiv -\nu$; il en a quatre pour $p = 2$ et $n > 2$; et si l'une est $\equiv \nu$, les autres seront $\equiv \nu + 2^{n-1}, -\nu + 2^{n-1}, -\nu$.
2^o. Si A est divisible par p, mais non par p^n, soit $p^{2\mu}$ la plus haute puissance de p qui divise A, car

cette puissance doit être paire (n^o 102), et $A = ap^{2\mu}$; il est clair que toutes les valeurs de V doivent être divisibles par p^μ, et que tous les quotients donnés par ces divisions seront les valeurs de l'expression $V' = \sqrt{a}\ (mod\ p^{n-2\mu})$; on aura donc toutes les valeurs différentes de V, en multipliant par p^μ, toutes celles de V' contenues entre 0 et $p^{n-\mu}$. Elles seront, par conséquent,
$\nu p^\mu, \nu p^\mu + p^{n-\mu}, \nu p^\mu + 2p^{n-\mu}, \ldots \nu p^\mu + (p^\mu - 1)p^{n-\mu}$,
ν étant une valeur quelconque de V : suivant donc que V' aura 1, ou 2, ou [11] valeurs, V en aura p^μ, ou $2p^\mu$ ou $4p^\mu$ (1^o).
3^o. Si A est divisible par p^n, on voit facilement, en posant $n = 2m$ ou $= 2m - 1$, suivant que n est pair ou impair, que tous les nombres divisibles par p^m sont des valeurs de V, et qu'il n'y en a pas d'autres ; mais les nombres divisibles par p^m sont $0, p^m, 2p^m \ldots (p^{n-m} - 1)p^m$, dont le nombre est p^{n-m}.

page 78, article 105 : Il reste à examiner le cas où le module m est composé de plusieurs modules premiers. Soit $m = abc\ etc.$, a, b, c, *etc.* étant des nombres premiers différents. Il est clair d'abord que si n est résidu de m, il le sera aussi des différents nombres, a, b, c, *etc.*, et que partant il sera non-résidu de m, s'il est non-résidu de quelqu'un de ces nombres. Réciproquement, si n est résidu des différents nombres a, b, c, *etc.*, il le sera de leur produit m ; en effet, si l'on a $n \equiv A^2, B^2, C^2, etc.$, suivant les modules a, b, c, *etc.*, respectivement (n^o 32), on aura $n \equiv N^2$, suivant tous ces modules, et conséquemment suivant leur produit.
Comme on voit facilement que la valeur de N résulte de la combinaison d'une valeur quelconque de A, ou de l'expression $\sqrt{n}\ (mod\ a)$, avec une valeur quelconque de B, avec une valeur quelconque de C, *etc*, que les différentes combinaisons donneront des valeurs différentes, et qu'elles les donneront toutes ; le nombre des valeurs de N sera égal au produit des nombres de valeurs de A, B, C, *etc.* que nous avons appris à déterminer dans l'article précédent.

page 78, article 106 : On voit par ce qui précède, qu'il suffit de reconnaître si un nombre donné est résidu ou non-résidu d'un nombre premier donné, et que tous les cas reviennent à celui-là.
Un nombre quelconque A, non divisible par un nombre premier $2m + 1$, est résidu ou non-résidu de ce nombre premier suivant que $A^m \equiv +1 ou \equiv -1\ (mod\ 2m + 1)$.

page 80, article 109 : en effet, il est évident que si r est un résidu, $\frac{1}{r}\ (mod\ p)$ en sera un aussi.

(Les **articles** 108 **à** 124 **des pages** 79 **à** 91 traitent des cas particuliers 1, -1, 2, -2, 3, -3, 5, -5, 7 et -7.)

page 81, article 111 : Si donc r est résidu d'un nombre premier de la forme $4n + 1$, $-r$ le sera aussi, et tous les non-résidus seront encore non-résidus en changeant les signes[12]. Le contraire arrive pour les nombres premiers de la forme $4n + 3$, dont les résidus deviennent non-résidus, et réciproquement quand on change le signe (n^o 98).
Au reste on déduit facilement de ce qui précède cette règle générale : -1 est résidu de tous les nombres qui ne sont divisibles ni par 4, ni par aucun nombre de la forme $4n + 3$. Il est non-résidu de tous les autres.(N^{os} 103 *et* 105).

page 81, article 112 : Passons maintenant aux résidus $+2$ et -2.
Si dans la table II on prend tous les nombres premiers dont le module est $+2$, on trouvera $7, 17, 23, 31, 41, 47, 71, 73, 79, 89, 97$. Or on remarque facilement qu'aucun d'eux n'est de la forme $8n + 3$ ou $8n + 5$.
Voyons donc si cette induction peut devenir une certitude.
Observons d'abord que tout nombre composé de la forme $8n + 3$ ou $8n + 5$ renferme nécessairement un facteur premier de l'une ou l'autre forme ; en effet les nombres premiers de la forme $8n + 1$ et $8n + 7$ ne peuvent former que des nombres de la forme $8n + 1$ ou $8n + 7$. Si donc notre induction est généralement vraie, il n'y aura aucun nombre de la forme $8n + 3$, $8n + 5$, dont le résidu soit $+2$. Or il est bien certain qu'il n'existe aucun nombre de cette forme et au-dessous de 100, dont le résidu soit $+2$; mais s'il y en avait au-dessus de cette limite, supposons que t soit le plus petit de tous ; t sera de la forme $8n + 3$ ou $8n + 5$, et $+2$ sera son résidu ; mais il sera non-résidu de tous les nombres semblables plus petits. Soit $a^2 \equiv 2\ (mod\ t)$, on pourra toujours prendre a impair et $< t$, car a a au moins deux valeurs positives plus

[11] ici, je crois qu'il manque un mot, le chiffre 4 ?
[12] Ainsi quand nous parlerons d'un nombre, en tant qu'il sera résidu ou non-résidu d'un nombre de la forme $4n + 1$, nous pouvons ne faire aucune attention à son signe, ou lui donner le signe $\pm$.

petites que t, dont la somme $= t$, et dont par conséquent l'une est paire et l'autre impaire (N^{os} 104, 105). Cela posé, soit $a^2 = 2 + ut$ ou $ut = a^2 - 2$, a^2 sera de la forme $8n + 1$, et par-conséquent ut de la forme $8n - 1$; donc u sera de la forme $8n + 3$ ou $8n + 5$ suivant que t sera de la forme $8n + 5$ ou $8n + 3$; mais de l'équation $a^2 = 2 + tu$, on tire la congruence $a^2 \equiv 2(mod\ u)$, c'est-à-dire que $+2$ serait aussi résidu de u. Il est aisé de voir qu'on a $u < t$; il s'ensuivrait que t ne serait pas le plus petit nombre qui eût $+2$ pour résidu, ce qui est contre l'hypothèse ; d'où suit enfin une démonstration rigoureuse de cette proposition que nous avions déduite de l'induction.
En combinant cette proposition avec celles du n^o 111, on en déduit les théorèmes suivants :
I. $+2$ est non-résidu, et -2 est résidu de tous les nombres premiers de la forme $8n + 3$.
II. $+2$ et -2 sont non-résidus de tous les nombres premiers de la forme $8n + 5$.

page 82, article 113 : Par une semblable induction on tirera de la Table II, pour les nombres premiers dont le résidu est -2, ceux-ci : $3, 11, 17, 19, 41, 43, 59, 67, 73, 83, 89, 97$[13]. Parmi ces nombres il ne s'en trouve aucun de la forme $8n + 5$ ou $8n + 7$; cherchons donc si de cette induction nous pouvons tirer un théorème général. On fera voir de la même manière que dans l'article précédent, qu'un nombre composé de la forme $8n + 5$ ou $8n + 7$, doit renfermer un facteur premier de la forme $8n + 5$ ou de la forme $8n + 7$; de sorte que si notre induction est généralement vraie, -2 ne peut être résidu d'aucun nombre de la forme $8n + 5$ ou $8n + 7$; or s'il peut y en avoir de tels, soit t le plus petit de tous, et qu'on ait $-2 = a^2 - tu$. Si l'on prend, comme plus haut, a impair et $< t$, u sera de la forme $8n + 5$ ou $8n + 7$ suivant que t sera de la forme $8n + 7$ ou $8n + 5$; mais de ce qu'on a $a < t$ et $ut = a^2 + 2$, il est facile de déduire que u est $< t$; et comme -2 serait aussi résidu de u, il s'ensuivrait que t ne serait pas le plus petit nombre dont -2 est le résidu, ce qui est contre l'hypothèse. Donc -2 sera nécessairement non-résidu de tous les nombres de la forme $8n + 5$ ou $8n + 7$.
En combinant cette proposition avec celles du n^o 111, on en déduit les théorèmes suivants :
I. -2 et $+2$ sont non-résidus de tous les nombres premiers de la forme $8n + 5$; comme nous l'avons déjà trouvé.
II.-2 est non-résidu et $+2$ résidu de tous les nombres premiers de la forme $8n + 7$.
Au reste, nous aurions pu prendre a pair dans les deux démonstrations ; mais alors il eût fallu distinguer le cas où a est de la forme $4n + 2$, de celui où il est de la forme $4n$; d'ailleurs la marche est absolument la même et n'est sujette à aucune difficulté.

page 83, article 114 : Il nous reste encore à traiter le cas où le nombre premier est de la forme $8n + 1$; mais il échappe à la méthode précédente et demande des artifices tout-à-fait particuliers.
Soit, pour le module premier $8n+1$, une racine primitive quelconque a, on aura (n^o 62) $a^{4n} \equiv -1\ (mod\ 8n+1)$; cette congruence peut se mettre sous la forme $(a^{2n} + 1)^2 \equiv 2a^{2n}\ (mod\ 8n + 1)$, ou $(a^{2n} - 1)^2 \equiv -2a^{2n}$; d'où il suit que $2a^{2n}$ et $-2a^{2n}$ sont résidus de $8n + 1$; mais comme a^{2n} est un carré non-divisible par le module, $+2$ et -2 seront aussi résidus (n^o 98).

page 84, article 116 : Au reste on tire facilement de ce qui précède la règle générale suivante : $+2$ est résidu de tout nombre qui n'est divisible ni par 4 ni par aucun nombre premier de la forme $8n + 3$ ou $8n + 5$, et non-résidu de tous les autres, par exemple, de tous ceux de la forme $8n + 3$, $8n + 5$, tant premiers que composés.

page 91, article 125 : Tout nombre premier de la forme $4n + 1$ soit positif, soit négatif, est non-résidu de quelques nombres premiers, et même de nombres premiers plus petits que lui (il est évident qu'il faut éviter $+1$).

page 95, article 129 : Théorème. Si a est un nombre premier de la forme $8n+1$, il y aura nécessairement au-dessous de $2\sqrt{a}$ un nombre premier dont a est non-résidu.

page 95, article 130 : Maintenant que nous avons démontré que tout nombre premier de la forme $4n+1$ positif ou négatif, est toujours non-résidu d'un nombre premier au moins plus petit que lui...

page 98, au milieu du article 132 : mais, avant tout, il faut observer que tout nombre de la forme $4n + 1$ ne renfermera aucun facteur de la forme $4n + 3$, ou en renfermera un nombre pair parmi lesquels

[13] En considérant -2 comme le produit de $+2$ par -1 ; voyez n^o 111.

il pourra y en avoir d'égaux ; tandis que tout nombre de la forme $4n+3$ doit en renfermer un nombre impair. Le nombre des facteurs de la forme $4n+1$ reste indéterminé.

pages 108 et suiv., articles 146 à 150 : Au moyen du théorème fondamental [14] et des propositions relatives à -1, ± 2, on peut toujours déterminer si un nombre donné quelconque est résidu ou non-résidu d'un nombre premier donné.

Ensuite, dans l'**article 146**, Gauss généralise et explique la méthode permettant, étant donnés deux nombres quelconques P et Q, de trouver si l'un d'eux est résidu ou non-résidu de l'autre. Pour cela, il étudie la relation qui lie Q à chaque puissance de premier qui intervient dans la factorisation de P. Ce qui retient l'attention, c'est le début du point III de cet article 146, qui explique comment s'effectue le passage du second degré au premier degré :
On cherchera de la manière suivante la relation d'un nombre quelconque Q à un nombre premier a impair : quand $Q > a$, on substituera à Q son *résidu minimum positif* suivant le module a, ou, ce qui est quelquefois avantageux, son *résidu minimum absolu*, qui aura avec a la même relation que Q.
Or si l'on résoud Q, ou le nombre pris à sa place, en facteurs premiers p, p', p'', *etc.*, auxquels il faut joindre le facteur -1, quand Q est négatif, il est évident que la relation de Q à a dépendra de la relation des facteurs p, p', p'', *etc.* à a : de sorte que, si parmi eux il y en a $2m$ non-résidus de a, on aura QRa [15] ; mais s'il y en a $2m+1$, on aura QNa. Au reste, on voit facilement que si parmi les facteurs p, p', p'', *etc.*, il y en a un nombre pair d'égaux entre eux, on peut les rejeter, puisqu'ils n'influent en rien sur la relation de Q à a.

Dans les **articles** 147**,** 148 **et** 149, Gauss résoud le problème suivant : Etant proposé un nombre quelconque A, on peut trouver certaines formules qui contiennent tous les nombres premiers à A dont A est résidu, ou tous ceux qui sont diviseurs des nombres de la forme $x^2 - A$, x^2 étant un carré indéterminé. Nous appellerons simplement ces nombres *diviseurs* de $x^2 - A$; l'on voit facilement ce que sont les *non-diviseurs*. Mais pour abréger nous ne considérerons que les diviseurs qui sont impairs et premiers à A, les autres cas se ramenant sans peine à celui-là.

On recopie intégralement ces trois articles qui nous semblent très liés à l'idée que l'on cherche à développer.

Suite de l'article 147, page 110 : Soit d'abord A un nombre premier positif de la forme $4n+1$, ou négatif de la forme $4n-1$. Suivant le théorème fondamental, tous les nombres premiers qui, pris positivement, sont résidus de A, seront diviseurs de $x^2 - A$; mais tous les nombres premiers non-résidus de A seront non-diviseurs de $x^2 - A$, si pourtant on en excepte 2, qui est toujours diviseur. Soient r, r', r'', *etc.*, tous les résidus de A qui sont plus petits que lui, et n, n', n'', *etc.*, tous les non-résidus ; alors tout nombre premier contenu dans une des formes $Ak+r$, $Ak+r'$, $Ak+r''$, *etc.*, sera diviseur de $x^2 - A$; mais tout nombre premier contenu dans une des formes $Ak+n$, $Ak+n'$, *etc.*, sera non-diviseur de $x^2 - A$, k étant un nombre entier indéterminé. Nous appellerons les premières *formes des diviseurs* de $x^2 - A$ et les dernières *formes des non-diviseurs*. Le nombre de chacune d'elles sera égal au nombre de résidus r, r', *etc.* ou de non-résidus n, n', *etc.*, et partant, $(n^o\ 96) = \frac{1}{2}(A-1)$. Or si B est un nombre composé impair et que l'on ait ARB, tous les facteurs premiers de B seront contenus dans une des premières formes, et par conséquent, B lui-même ; donc tout nombre composé impair qui sera contenu dans la forme des non-diviseurs sera non-diviseur de $x^2 - A$; mais on ne peut pas dire que les non-diviseurs de $x^2 - A$ sont tous compris dans la forme des non-diviseurs, car en supposant B non-diviseur de $x^2 - A$, et si le nombre de ces facteurs est pair, B sera compris dans quelque forme de diviseurs (n^o 93).
Ainsi, soit $A = -11$; on trouvera que les formes des diviseurs de $x^2 + 11$ sont $11k+1$, 2, 3, 4, 5, 9, et que celles des non-diviseurs sont $11k+2$, 6, 7, 8, 10. Ainsi -11 sera résidu de tous les nombres premiers contenus dans une des premières formes et non-résidu de ceux qui sont contenus dans une des dernières.
On peut trouver des formes semblables pour les diviseurs et les non-diviseurs de $x^2 - A$, quel que soit A ; mais on voit aisément qu'on n'a à considérer que les valeurs de A qui ne sont divisibles par aucun carré ; car si $A = a^2 A'$, tous les diviseurs de $x^2 - A$ premiers avec A, seront diviseurs de $x^2 - A'$, et de même pour les non-diviseurs. Or nous distinguerons trois cas : 1°. quand A est de la forme $4n+1$ ou $-(4n-1)$; 2°. quand A est de la forme $4n-1$ ou $-(4n+1)$; 3°. quand A est pair ou de la forme $\pm(4n+2)$.

[14] communément appelé actuellement la *"loi de réciprocité quadratique"*.
[15] Gauss utilise la lettre R pour signifier *"est résidu quadratique de"* et la lettre N pour signifier *"est non-résidu quadratique de"*.

page 111, article 148 : *Premier cas.* Quand A est de la forme $4n+1$ ou $-(4n-1)$. On résoudra A en facteurs premiers a, b, c, d, *etc.*, en affectant du signe + ceux de la forme $4n+1$, et du signe − ceux de la forme $4n-1$ qui seront en nombre pair ou impair, suivant que A sera de la forme $4n+1$ ou $-(4n-1)$ (n^o 132). On distribuera en deux classes les nombres plus petits que A et premiers avec lui ; en mettant dans la première ceux qui ne sont non-résidus d'aucun diviseur de A, ou qui sont non-résidus d'un nombre pair de ces diviseurs, et dans la seconde ceux qui sont non-résidus d'un nombre impair des mêmes diviseurs. Désignons les premiers par r, r', r'', *etc.* et les seconds par n, n', n'', *etc.* ; alors $Ak+r$, $Ak+r'$, *etc.* sont les formes des diviseurs de x^2-A, et $Ak+n$, $Ak+n'$, *etc.* celles des non-diviseurs. C'est-à-dire que tout nombre premier, excepté 2, sera diviseur ou non-diviseur de x^2-A, suivant qu'il sera contenu dans l'une des premières ou l'une des dernières formes.
En effet, si p est un nombre premier résidu ou non-résidu d'un des facteurs de A, ce facteur sera résidu ou non-résidu de p (théor. fond.) ; donc si parmi les facteurs de A, il y en a m dont p soit non-résidu, il y en aura autant qui seront non-résidus de p, et partant, lorsque p sera contenu dans l'une des premières formes, m sera pair et ARp, et lorsque p sera contenu dans une des dernières, p sera impair et ANp.
Exemple. Soit $A=+105=(-3)\times(+5)\times(-7)$[16] ;
les nombres r, r', r'', *etc.* sont :
1, 4, 16, 46, 64, 79, qui ne sont non-résidus d'aucun facteur. ;
2, 8, 23, 32, 53, 92, qui sont non-résidus de 3 et 5 ;
26, 41, 59, 89, 101, 104, ... 3 et 7 ;
23, 52, 73, 82, 97, 103, ... 5 et 7 ;
les nombres n, n', n'', *etc.* sont :
11, 29, 44, 71, 74, 86, non-résidus de 3 ;
22, 37, 43, 58, 67, 88, ... de 5 ;
19, 31, 34, 61, 76, 94, ... de 7 ;
17, 38, 47, 62, 68, 83, ... de 3, 5 et 7 ;
On déduit facilement de la théorie des combinaisons et des $n^{os}(32,96)$ que la multitude des nombres r, r', *etc.* sera

$$t\Big(1+\frac{l(l-1)}{1.2}+\frac{l(l-1)(l-2)(l-3)}{1.2.3.4}+etc.\Big)$$

et celle des nombres n, n', *etc.*

$$t\Big(l+\frac{l(l-1)(l-2)}{1.2.3}+\frac{l(l-1)(l-2)(l-3)(l-4)}{1.2.3.4.5}+etc.\Big)$$

l désignant le nombre des facteurs a, b, c, d, *etc.*, t étant
$=2^{-l}(a-1)(b-1)(c-1)etc.$, et chaque série devant être continuée jusqu'à ce qu'elle s'arrête d'elle-même. (En effet il y a t nombres résidus de a, b, c, d, *etc.*, $t.\frac{l.(l-1)}{1.2}$ non-résidus de deux de ces facteurs, etc. Mais pour abréger, nous sommes forcés de ne pas donner plus de développement à la démonstration). Or chacune des séries a pour somme $l.2^{l-1}$; car la première provient de
$1+\frac{l-1}{1}+\frac{(l-1)(l-2)}{1.2}+\frac{(l-1)(l-2)(l-3)}{1.2.3}+etc.$ en prenant le premier terme, puis la somme du second et du troisième, puis la somme du quatrième et du cinquième, etc. : la seconde provient aussi de la même série, en joignant le premier terme au second, le troisième au quatrième, etc. Il y a donc autant de formes de diviseurs de x^2-A, que de formes de non-diviseurs ; et ils sont en nombre $2^{l-1}.t$ de chaque espèce, ou $\frac{1}{2}(a-1)(b-1)(c-1)(d-1)etc.$

page 113, article 149 : Nous pouvons traiter ensemble le second et le troisième cas. En effet on pourra toujours poser $A=(-1)Q$, ou $=(+2)Q$, ou $=(-2)Q$, Q étant un nombre de la forme $4n+1$ ou $-(4n-1)$. Soit généralement $A=\alpha Q$, de sorte que α soit ou -1 ou ± 2. Alors A sera résidu de tout nombre dont α et Q seront tous deux résidus, ou tous deux non-résidus : au contraire il sera non-résidu de tout nombre dont l'un d'eux seulement sera non-résidu. De là on déduit sans peine les formes des diviseurs et des non-diviseurs de x^2-A. Si $\alpha=-1$; nous partagerons tous les nombres plus petits que $4A$ et premiers avec lui, en deux classes. La première renfermera ceux qui sont dans quelque forme des diviseurs de x^2-Q, et en même temps de la forme $4n+1$, et aussi ceux qui sont dans quelque forme des non-diviseurs de x^2-Q et en même temps de la forme $4n-1$: la seconde renfermera tous les autres. Soient r, r', r'', *etc.* les premiers et n, n', n'', *etc.* les derniers ; A sera résidu de tous les nombres premiers contenus dans une

[16] Cela peut surprendre d'utiliser ainsi des nombres négatifs dans la factorisation mais Gauss explique qu'il affecte systématiquement les nombres premiers de la forme $4n+3$ du signe − et ceux de la forme $4n+1$ du signe + à cause de leur comportement démontré par le théorème fondamental.

des formes $4Ak+r$, $4Ak+r'$, $4Ak+r''$, *etc.*, et non-résidu de tous les nombres premiers contenus dans une des formes $4Ak+n$, $4Ak+n'$, $4Ak+n''$, *etc.* Si $\alpha = \pm 2$, nous distribuerons tous les nombres plus petits que $8Q$ et premiers avec lui en deux classes : la première renfermera tous ceux qui sont contenus dans quelque forme des diviseurs de $x^2 - Q$, et qui sont de la forme $8n+1$ ou $8n+7$, pour le signe supérieur, et de la forme $8n+1$ ou $8n+3$ pour le signe inférieur ; cette classe comprendra aussi tous ceux qui sont contenus dans quelque forme de non-diviseurs de $x^2 - Q$ et qui sont, pour le signe supérieur, de la forme $8n+3$, $8n+5$, et pour le signe inférieur, de la forme $8n+5$, $8n+7$, et la seconde tous les autres. Alors désignant les nombres de la première classe par r, r', r'', *etc.*, ceux de la seconde par n, n', n'', *etc.*, $\pm 2Q$ sera résidu de tous les nombres premiers contenus dans les formes $8Qk+r$, $8Qk+r'$, $8Qk+r''$, *etc.* et non-résidu de tous ceux contenus dans les formes $8Qk+n$, $8Qk+n'$, $8Qk+n''$, *etc.* Au reste, on peut démontrer facilement qu'il y a autant de formes de diviseurs qu'il y en a de non-diviseurs.
Exemple. On trouve ainsi que 10 est résidu de tous les nombres premiers contenus dans les formes $40K+1$, $+3$, $+9$, $+13$, $+27$, $+31$, $+37$, $+39$, et non-résidu de tous les nombres premiers contenus dans les formes $40K+7$, $+11$, $+17$, $+19$, $+21$, $+23$, $+29$, $+33$.

page 114, article 150 : Ces formes ont plusieurs propriétés assez remarquables ; nous n'en citerons cependant qu'une seule. Si B est un nombre composé premier avec A, tel qu'un nombre $2m$ de ses facteurs premiers soient compris dans quelque forme de non-diviseurs de $x^2 - A$, B sera contenu dans quelque forme de diviseurs de $x^2 - A$; mais si le nombre de facteurs premiers de B contenus dans quelque forme de non-diviseurs de $x^2 - A$ est impair, B sera aussi contenu dans quelque forme de non-diviseurs. Nous omettons la démonstration, qui n'a rien de difficile[17]. Il suit de là que non-seulement tout nombre premier ; mais aussi tout nombre composé impair et premier avec A est non-diviseur dès qu'il est contenu dans une des formes de non-diviseur ; car nécessairement quelque facteur premier de ce nombre sera non-diviseur.

page 116, article 152 : Jusqu'à présent nous n'avons traité que la congruence simple $x^2 \equiv A (mod\ m)$, et nous avons appris à reconnaître les cas où elle est résoluble. Par le n^o 105, la recherche des racines elles-mêmes est ramenée au cas où m est un nombre premier, ou une puissance d'un nombre premier ; et par le n^o 101, ce dernier cas est ramené à celui où m est un nombre premier. Quant à celui-ci, en comparant ce que nous avons dit (n^{os} 61 et suiv.) avec ce que nous enseignerons sect. V et VIII, on aura presque tout ce qui peut se faire par les méthodes générales. Mais dans les cas où elles sont applicables, elles sont infiniment plus longues que les méthodes indirectes que nous exposerons dans la section VI, et partant elles sont moins remarquables par leur utilité dans la pratique que par leur beauté.

Annexe 3 : Deux extraits de la lettre de Carl Frédéric Gauss à Sophie Germain du 30 avril 1807 (extrait des Oeuvres philosophiques de Sophie Germain, 1879, p. 274-282)

Voici une autre proposition relative aux residus quarrés, dont la demonstration est moins cachée : je ne l'ajoute pas, pour ne pas vous derober le plaisir de la developper vous-même, si vous la trouverez digne d'occuper quelques moments de votre loisir.
Soit p un nombre premier. Soient les $p-1$ nombres inférieurs à p partagés en deux classes :
A.....$1, 2, 3, 4....\frac{1}{2}(p-1)$
B.....$\frac{1}{2}(p+1), \frac{1}{2}(p+3), \frac{1}{2}(p+5), ...p-1$ Soit a un nombre quelconque non divisible par p. Multipliés tous les nombres A par a; prenés-en les moindres residus selon le module p, soient, entre ces residus, α appartenants à A, et β appartenants à B, de sorte que $\alpha + \beta = \frac{1}{2}(p-1)$. Je dis que a è residu quarré de p lorsque β è pair, non residu lorsque β è impair.

Le second extrait est davantage *"connu"*

Le goût pour les sciences abstraites en général et surtoût pour les mysteres des nombres est fort rare : on ne s'en étonne pas ; les charmes enchanteurs de cette sublime science ne se decelent dans toute leur

[17] On suppose donc que Gauss l'a faite, dans une quelconque marge...

beauté qu'à ceux qui ont le courage de l'approfondir. Mais lorsqu'une personne de ce sexe, qui, par nos moeurs et par nos préjugés, doit rencontrer infiniment plus d'obstacles et de difficultés, que les hommes, à se familiariser avec ces recherches epineuses, sait neansmoins franchir ces entraves et penétrer ce qu'elles ont de plus caché, il faut sans doute, qu'elle ait le plus noble courage, des talens tout à fait extraordinaires, le génie supérieur. En effet, rien ne pourroit me prouver d'une manière plus flatteuse et moins équivoque, que les attraits de cette science, qui ont embelli ma vie de tant de jouissances, ne sont pas chimériques, que la predilection, dont vous l'avez honorée.

Annexe 4 : un nombre premier non-résidu de tous les diviseurs impairs des nombres pairs n de la deuxième catégorie fournit une décomposition de Goldbach

20, diviseur 5, 3N5, 3+17
28, diviseur 7, 5N7, 5+23
30, diviseurs 3 et 5, 17N3, 17N5, 17+13
40, diviseur 5, 3N5, 3+37
42, diviseurs 3 et 7, 5N3, 5N7, 5+37
44, diviseur 11, 7N11, 7+37
48, diviseur 3, 5N3, 5+43
50, diviseur 5, 3N5, 3+47
56, diviseur 7, 3N7, 3+47
60, diviseurs 3 et 5, 17N3, 17N5, 17+43
66, diviseurs 3 et 11, 29N3, 29N11, 29+47
68, diviseur 17, 7N17, 7+61
72, diviseur 3, 5N3, 5+67
78, diviseurs 3 et 13, 5N3, 5N13, 5+73
80, diviseur 5, 7N5, 7+73
84, diviseurs 3 et 7, 5N3, 5N7, 5+79
88, diviseur 11, 17N11, 17+71
90, diviseurs 3 et 5, 17N3, 17N5, 17+73
92, diviseur 23, 19N23, 19+73
96, diviseur 3, 17N3, 17+79
98, diviseur 7, 19N7, 19+79

Annexe 5 : Illlustrations du théorème fondamental pour les modules impairs

Pour les modules impairs, des relations existent entre le caractère résidu/non-résidu de x à m et de $x + \frac{p+1}{2}$ à m. Les tables ci-dessous illustrent le fait qu'elles sont assez difficiles à trouver. Par exemple, sur les tables associées aux modules 15 et 75, on voit qu'il y a anti-symétrie entre x et $x + \frac{p+1}{2}$ quand ce sont tous deux des $4n+2$ ou des $4n$ et symétrie quand ce sont tous deux des $4n+1$ ou des $4n+3$.

Comme on s'intéresse à la conjecture de Goldbach, on axera plutôt les recherches sur les modules pairs.

5.1 : Illustrations du théorème fondamental pour les modules impairs puissances de nombres premiers impairs

Selon le module 9, de la forme $(4n+3)^2$:

9	8	7	6	5
0	1	2	3	4
0	1	4	0	7

Selon le module 27, de la forme $(4n+3)^3$:

27	26	25	24	23	22	21	20	19	18	17	16	15	14
0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	1	4	9	16	25	9	22	10	0	19	13	9	7

Selon le module 25, de la forme $(4n+1)^2$:

25	24	23	22	21	20	19	18	17	16	15	14	13
0	1	2	3	4	5	6	7	8	9	10	11	12
0	1	4	9	16	0	11	24	14	6	0	2	19

5.2 : Illustrations du théorème fondamental pour les modules impairs produits de nombres premiers impairs

Selon le module 15, de la forme $(4n+3)(4n+1)$:

15	14	13	12	11	10	9	8
0	1	2	3	4	5	6	7
0	1	4	9	1	10	6	4

Selon le module 45, de la forme $(4n+3)^2(4n+1)$:

45	44	43	42	41	40	39	38	37	36	35	34	33	32	31	30	29	28	27	26	25	24	23
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
0	1	4	9	16	25	36	4	19	36	10	31	9	34	16	0	31	19	9	1	40	36	34

Selon le module 75, de la forme $(4n+3)(4n+1)^2$:

75	74	73	72	71	70	69	68	67	66	65	64	63	62	61	60	59	58	57
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	1	4	9	16	25	36	49	64	6	25	46	69	19	21	0	31	64	24

56	55	54	53	52	51	50	49	48	47	46	45	44	43	42	41	40	39	38
19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
61	25	66	34	4	51	25	1	54	34	16	0	61	49	39	31	25	21	19

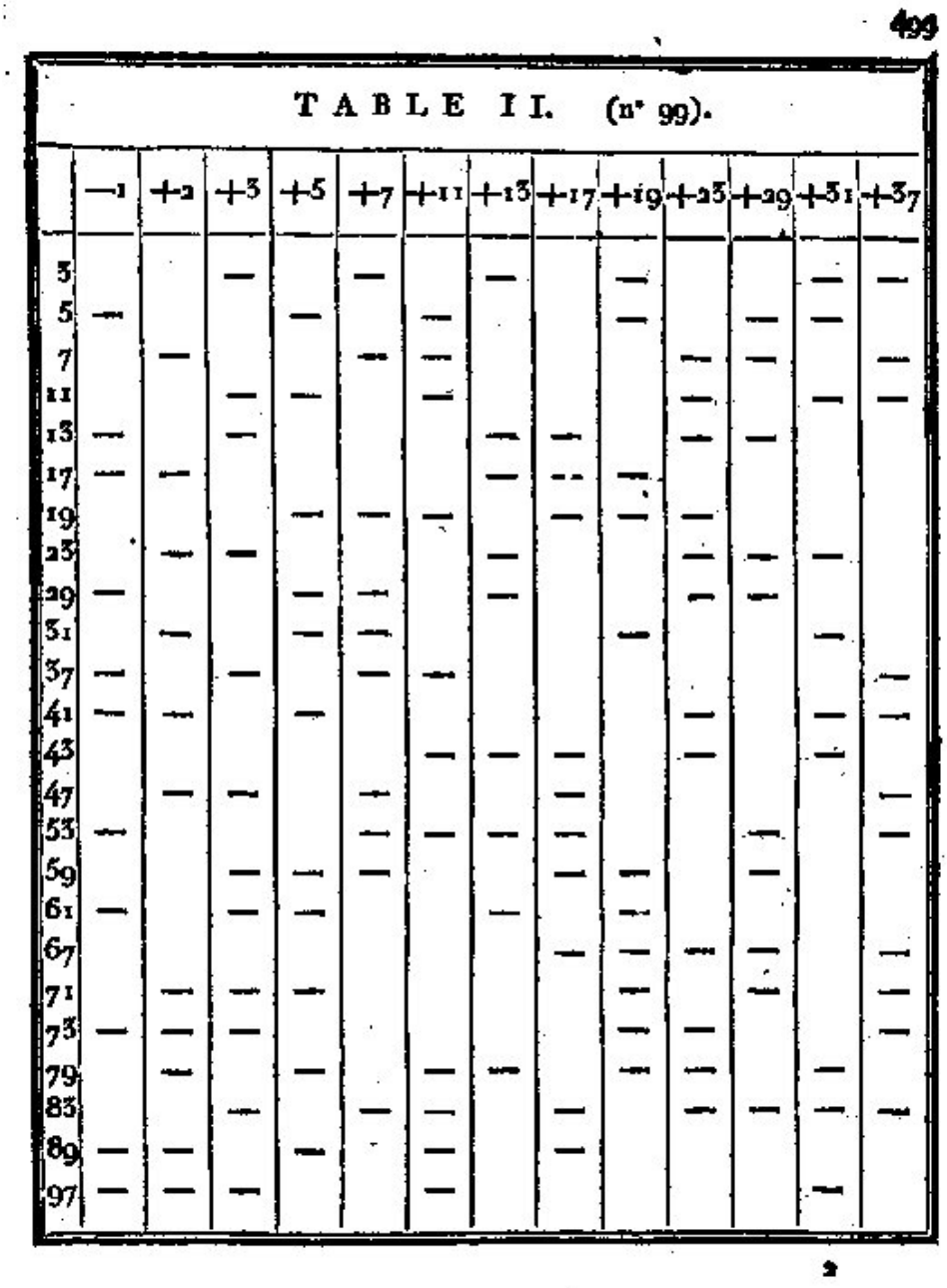
Annexe 6 : L'orthographe des Recherches Arithmétiques

Ici, on recense quelques différences orthographiques par rapport à l'orthographe actuelle :

- quarré, soumultiple, alongeraient
- différens, précédens, quotiens, coefficiens, suivans, élégans
- parceque, parconséquent, ensorte que
- entr'eux, long-temps

Annexe 7 : La table II des Recherches Arithmétiques

La table que nous avons fournie est une inversion lignes-colonnes de la table de Gauss.

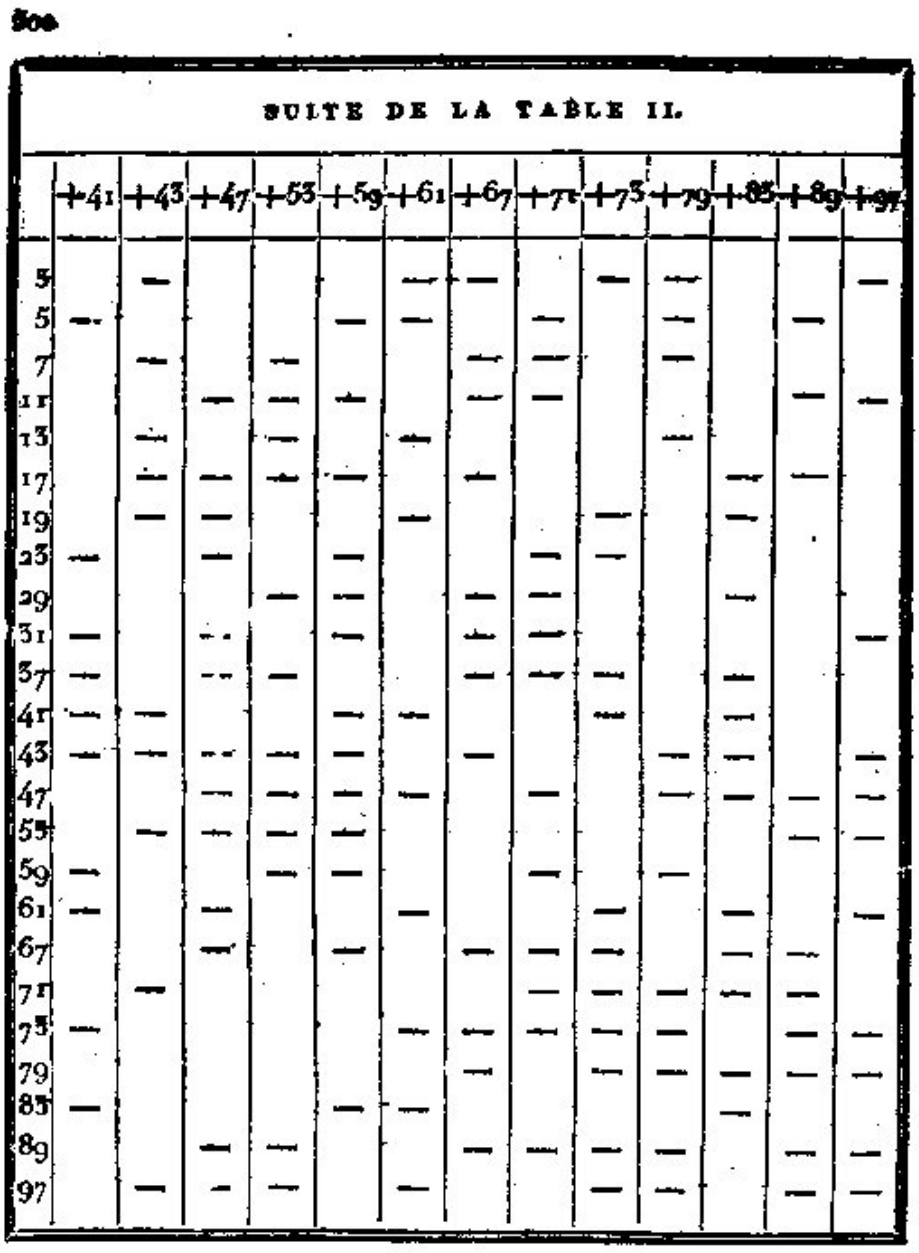


499

TABLE II. (n° 99).

	−1	+2	+3	+5	+7	+11	+13	+17	+19	+23	+29	+31	+37
3			−		−		−		−			−	−
5	−			−		−			−		−	−	
7		−			−	−				−	−		−
11			−	−		−				−		−	−
13	−		−				−	−		−	−		
17	−	−					−	: :	−				
19				−	−	−		−	−	−			
23		−	−				−			−	−	−	
29	−			−	−		−			−	−		
31		−		−	−				−			−	
37	−		−		−	−							−
41	−	−		−						−		−	−
43						−	−	−		−		−	
47		−	−		−			−					−
53	−				−	−	−	−			−		−
59			−	−	−			−	−		−		
61	−		−	−			−		−				
67								−	−	−	−		−
71		−	−	−					−		−		−
73	−	−	−						−	−			−
79		−		−		−	−		−	−		−	
83			−		−	−		−		−	−	−	−
89	−	−		−		−		−					
97	−	−	−			−						−	

2



SUITE DE LA TABLE II.

	+41	+43	+47	+53	+59	+61	+67	+71	+73	+79	+83	+89	+97
5		—				—	—		—	—			—
5	—				—	—		—		—		—	
7		—		—			—	—		—			
11			—	—	—		—	—				—	—
13		—		—		—				—			
17		—	—	—	—		—				—	—	
19		—	—			—			—		—		
23	—		—		—			—	—				
29				—	—		—	—			—		
31	—		—		—		—	—					—
37	—		—	—			—	—	—		—		
41	—	—			—	—			—		—		
43	—	—	—	—	—		—			—	—		—
47			—	—	—	—		—		—	—	—	—
53		—	—	—	—							—	—
59	—			—	—			—		—			
61	—		—			—			—		—		—
67			—		—		—	—	—		—	—	
71		—						—	—	—	—	—	
73	—					—	—	—	—	—		—	—
79							—		—	—	—	—	—
83	—				—	—					—		
89			—	—			—	—	—	—		—	—
97		—	—	—		—			—	—		—	—

Annexe 8 : Initiale G

Goldbach, Gauss, Germain, Galois, Godel, Grothendieck...

Bibliographie

[1] **C. F. Gauss**, *Recherches Arithmétiques*, Editions Jacques Gabay, 1801.

[2] **G. Cantor**, *Vérification jusqu'à 1000 du théorème empirique de Goldbach*, Congrès de Caen de l'A.F.A.S. (Association Française pour l'Avancement des Sciences) du 10 août 1894, p.117 à 134.

[3] **A.-M. Décaillot**, *Cantor et la France*, Ed. Kimé, 2008.

1 Pourquoi y a-t-il un lien entre les caractères *résidu de* $2p$ associés à x et $x+p$ lorsque $2p$ est un double d'impair ?

Si x R $2p$ alors existent y et k qui permettent d'écrire $x = y^2 - 2pk$ car x est congru à un carré selon le module $2p$.

Mais alors $x+p = y^2-2pk+p = y^2-2p\left(k-\frac{1}{2}\right)$ est lui-aussi de la forme y^2-2pk' si on pose $k' = k-\frac{1}{2}$.

Pourquoi ce raisonnement ne peut-il être fait que pour p impair et pas pour p pair ? Parce qu'alors k est un multiple de $\frac{1}{2}$? Non, ça ne va pas du tout, ça donne un non-entier.

Observons par exemple pour $78 = 2.3.13$, double de 39 un impair, de qui les résidus sont les carrés en mettant en vis-à-vis les résidus x et $x+p$ (en fournissant pour chacun entre parenthèses) le nombre dont le carré le rend résidu).

$1(77)$	$\rightarrow$	$40(38)$	$77-38=39$
$4(76)$	$\rightarrow$	$43(67)$	$76-67=9$
$10(58)$	$\rightarrow$	$49(71)$	$71-58=13$
$13(65)$	$\rightarrow$	$52(26)$	$65-26=39$
$64(70)$	$\rightarrow$	$25(73)$	$73-70=3$
$16(74)$	$\rightarrow$	$55(35)$	$74-35=39$
$61(29)$	$\rightarrow$	$22(68)$	$68-29=39$
$3(75)$	$\rightarrow$	$42(48)$	$69-48=21$
$75(45)$	$\rightarrow$	$36(72)$	$72-45=27$
$9(3)$	$\rightarrow$	$48(42)$	$42-3=39$
$69(63)$	$\rightarrow$	$30(54)$	$63-54=9$
$12(60)$	$\rightarrow$	$51(57)$	$60-57=3$
$66(12)$	$\rightarrow$	$27(27)$	$27-12=15$

Dans la troisième colonne, on a mis la différence entre les carrés dont on voit qu'elle est toujours multiple de l'un des diviseurs de $2p$ (ça ne peut pas être un hasard).

En fait, ce qui est intéressant dans cette propriété, c'est que si on considère la ligne du haut dans les tables, deux nombres symétriques l'un de l'autre autour de la ligne médiane ont pour somme $3p$. Modulo $2p$, ils sont donc fatalement incongrus.

2 Reprise de l'idée principale

On cherche

$$p \not\equiv n \begin{pmatrix} 3 \\ 5 \\ 7 \\ 11 \\ \dots \end{pmatrix}$$

.

$$p \not\equiv a^2 b \iff \frac{p}{b} \not\equiv a^2 \begin{pmatrix} 3 & \star o \\ 5 & \\ 7 & \star \\ 11 & \star o \\ \dots & \end{pmatrix} \quad (1)$$

On pose $n = a^2 b$ avec b le produit de tous les facteurs premiers de la factorisation de n de puissance impaire.

On a marqué d'une $\star$ les diviseurs de n, parmi tous les premiers nombres premiers impairs inférieurs à $\sqrt{n}$. Ce sont tous les modules selon lesquels il faut l'incongruence. Parmi eux, on a marqué d'un o ceux de valuation p-adique impaire.

On a l'impression que l'un des nombres premiers qui sont non-résidus de tous les diviseurs impairs de n fournit toujours une décomposition de Goldbach de n. Il faudrait être assuré qu'un tel nombre premier existe forcément et que s'il en existe plusieurs, l'un d'entre eux respecte la contrainte souhaitée d'incongruence selon tous les modules premiers impairs inférieurs à $\sqrt{n}$ sous prétexte par exemple qu'ils ne peuvent pas tous ne pas fournir une telle décomposition simultanément.

Si $\forall d_i | n,\ p\ N\ d_i$ alors $p \not\equiv \alpha^2(d_\alpha)$, $p \not\equiv \beta^2(d_\beta)$, ..., $p \not\equiv \zeta^2(d_\zeta)$.

Mais par l'équivalence (1), on a fait passer seulement les diviseurs de valuation p-adique impaire à gauche (nota : Gauss dit que $\frac{1}{b}$ se comporte comme b à la fin de l'article 98).

1) s'ils étaient en nombre pair, $\frac{1}{b}$, leur produit, est résidu de chacun d'eux. Mais p étant non-résidu de tous les diviseurs de n et en particulier d'eux, vérifie les $\not\equiv$ pour eux et on a bien globalement $\frac{p}{b} \not\equiv a^2$ selon eux, ce qui est satisfaisant. Problème : mais selon les autres, qu'en est-il ?

2) s'ils étaient en nombre impair, $\frac{1}{b}$ leur produit est non-résidu de chacun d'eux. Mais p étant non-résidu de tous les diviseurs de n et en particulier d'eux, on se retrouve avec $\frac{p}{b}$ résidu selon eux. Or on veut justement le contraire. De plus, là encore, qu'en est-il selon les modules non-diviseurs de n ?

Il faut sûrement se servir du théorème inaugurant la section 4, selon lequel il ne peut y avoir plus de $\frac{m+2}{2}$ (resp. $\frac{m+1}{2}$) (note : soit environ la moitié.) des nombres compris entre 1 et $m-1$ qui sont résidus de m lorsque m est pair (resp. impair).

1 Résultats démontrés faisant intervenir des résidus quadratiques

Les éléments qui suivent proviennent essentiellement du livre de Marc Guinot aux éditions Aleas "Une époque de transition : Lagrange et Legendre".

1.1 En utilisant le symbole de Legendre

Lorsqu'on utilise ce symbole $\left(\frac{a}{m}\right)$, le dénominateur m est un nombre premier impair et le numérateur a est un entier non divisible par m.

1) Pour qu'un entier a quelconque soit résidu quadratique de p, il faut et il suffit que a soit congru à l'un des entiers

$$1^2, 2^2, \ldots, \left[\frac{1}{2}(p-1)\right]^2$$

En utilisant le symbole de Jacobi, cela s'écrit :

$$\left(\frac{a}{m}\right) = \begin{cases} 1 \textit{ si } a \textit{ est un carré modulo } m \textit{ (i.e. } \exists\, x \leq m,\ a \equiv x^2 \ (mod\ m)); \\ \text{-1 } \textit{si } a \textit{ n'est pas un carré modulo } m \textit{ (i.e. } \forall\, x \leq m,\ a \not\equiv x^2 \ (mod\ m)). \end{cases}$$

2) Le produit de deux résidus quadratiques de p et le produit de deux résidus non quadratiques de p sont toujours des résidus quadratiques de p. Le produit d'un résidu quadratique et d'un résidu non quadratique est un résidu non quadratique.

2') Un entier premier à p résidu quadratique de p l'est aussi de toute puissance de p car $(\mathbb{Z}/p^r\mathbb{Z})^*$ est un groupe cyclique d'ordre $p^{r-1}(p-1)$ sauf si $p = 2$ car $(\mathbb{Z}/2^r\mathbb{Z})^*$ n'est pas cyclique.

2") Si un entier a est premier avec un nombre $m \geq 1$ et si m se décompose en facteurs premiers sous la forme

$$m = p_1^{n_1} \ldots p_r^{n_r}$$

(avec des nombres premiers p_i deux à deux distincts et des exposants $n_i \geq 1$), alors pour que a soit résidu quadratique modulo m, il faut et il suffit qu'il soit résidu quadratique de $p_i^{n_i}$ quel que soit i[1].

3) Dans un système complet de résidus modulo p un nombre premier impair, il y a exactement $\frac{1}{2}(p-1)$ résidus quadratiques de p et $\frac{1}{2}(p-1)$ résidus non-quadratiques.

4) Le nombre -1 est résidu quadratique de tous les nombres premiers p de la forme $4n+1$ et non-résidu quadratique de tous les nombres premiers de la forme $4n+3$.

Corollaire de 4) : Si p est un nombre premier de la forme $4n+1$, les résidus quadratiques (et les non-résidus) se répartissent symétriquement dans l'intervalle $[1, p-1]$; de façon précise, si a est un résidu (resp. un non-résidu) appartenant à l'ensemble $\{1, 2, \ldots, p-1\}$ alors $p-a$ est encore un résidu (resp. un non-résidu) appartenant au même ensemble.

5) Pour tout nombre premier p impair, le caractère quadratique de 2 modulo p est donné par la formule

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

cette formule signifiant que 2 est résidu quadratique des nombres premiers de la forme $8n+1$ et $8n+7$, et non-résidu des nombres premiers de la forme $8n+3$ et $8n+5$.

[1] Je suis hésitante là, j'avais l'impression d'après Gauss qu'on pouvait également obtenir un résidu si on faisait le produit d'un nombre pair de non-résidus.

5') Les résidus quadratiques a de 2 sont les entiers impairs congrus à 1 modulo 2 ; ceux de 4 sont les entiers impairs congrus à 1 modulo 4 et les résidus quadratiques de 2^n (pour $n \geq 3$ fixé) sont congrus à 1 modulo 8.

$$\left(\frac{a}{2}\right) = 1 \iff a \equiv 1 \ (mod\ 2)$$
$$\left(\frac{a}{4}\right) = 1 \iff a \equiv 1 \ (mod\ 4)$$
$$\left(\frac{a}{8}\right) = 1 \iff a \equiv 1 \ (mod\ 8)$$

6) ***Loi de Réciprocité Quadratique*** : Soient p et q deux nombres premiers impairs différents, les symboles de Legendre $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$ sont toujours égaux sauf lorsque p et q sont tous deux des nombres de la forme $4n+3$. Il revient au même de dire que

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

7) Soient a et b des nombres congrus entre eux modulo p. Si a est résidu quadratique de p, il en est de même de b ; si a n'est pas un résidu quadratique de p, b n'en est pas un non plus.

8) quel que soit a un entier donné et quels que soient m, n deux nombres premiers impairs ne divisant pas a,

$$\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right) \ si\ m \equiv n \ (mod\ 4a)$$

9) ***Lemme de Gauss*** : Pour tout entier a non divisible par p un nombre premier impair, on a

$$\left(\frac{a}{p}\right) = (-1)^{\lambda}$$

où λ est le nombre des entiers $a, 2a, \ldots, \frac{1}{2}(p-1)a$ dont le reste minimal modulo p est négatif.

10) ***Critère d'Euler :*** Si a est un entier quelconque non divisible par p un nombre premier impair, alors on a

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \ (mod\ p)$$

1.2 En utilisant le symbole de Jacobi

Lorsqu'on utilise le symbole de Jacobi $\left(\frac{a}{m}\right)$, le dénominateur m est un nombre impair (non forcément premier) et le numérateur a est un entier quelconque.

1)

$$\left(\frac{a}{m}\right) = \begin{cases} 0 \ si\ a\ est\ un\ multiple\ de\ m\ (i.e.\ m|a); \\ 1 \ si\ a\ est\ un\ carré\ modulo\ m\ (i.e.\ \exists\ x \leq m,\ a \equiv x^2\ (mod\ m); \\ \text{-1 } si\ a\ n'est\ pas\ un\ carré\ modulo\ m\ (i.e.\ \forall\ x \leq m,\ a \not\equiv x^2\ (mod\ m). \end{cases}$$

Les résidus ou non-résidus de m ne sont jamais divisibles par m.

2) quels que soient a, b deux entiers non nuls, et m un nombre impair positif premier à a et b (et donc premier à ab),

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$$

et si a est premier à m,

$$\left(\frac{a^2 b}{m}\right) = \left(\frac{b}{m}\right)$$

3) quel que soit a non nul, m, n impairs positifs premiers à a,

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

4) quel que soit m un entier impair positif quelconque,

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$$

5) quel que soit m un entier impair positif quelconque,

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$

6) ***Loi de Réciprocité Quadratique*** : quels que soient a et b deux nombres impairs positifs premiers entre eux,

$$\left(\frac{b}{a}\right) = \left(\frac{a}{b}\right)(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$$

7) quel que soit m un entier impair positif premier à a (et donc premier à b)

$$\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right) \; si \; a \equiv b \; (mod \; m)$$

8) quels que soient m et n deux entiers positifs impairs premiers à a tous les deux,

$$\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right) \; si \; m \equiv n \; (mod \; 4a)$$

9) ***Lemme de Gauss*** : pour tout entier non nul a et tout m un nombre impair positif premier à a,

$$\left(\frac{a}{m}\right) = (-1)^{\lambda}$$

avec λ le nombre d'éléments de l'ensemble $a, 2a, 3a, \ldots, \frac{1}{2}(m-1)a$ dont les plus petits résidus positifs sont supérieurs à $\dfrac{m}{2}$.

2 Pourquoi y a-t-il un lien entre les caractères quadratiques à $2m$ de x et $x+m$ lorsque $2m$ est un double d'impair ?

Posons $m = 2n + 1$ un nombre entier impair quelconque.
On a $x \equiv x + m \; (mod \; m)$.
Par (7) de la section 1.2, on en déduit que :

$$\left(\frac{x}{m}\right) = \left(\frac{x+m}{m}\right)$$

et par (3) de la section 1.2,

$$\left(\frac{x}{2m}\right) = \left(\frac{x}{2}\right)\left(\frac{x}{m}\right).$$

Mais comme les résidus de 2 sont les nombres impairs (2 est en facteur dans le module), alors

$$\left(\frac{x}{2m}\right) = \left(\frac{x+m}{2m}\right).$$

En fait, ce qui est peut-être intéressant dans cette propriété, c'est que si on considère la ligne du haut dans les tables, deux nombres symétriques l'un de l'autre autour de la ligne médiane ont pour somme $3m$. Exemple pour rappel de la table modulo $2 \times 45 = 90$ (nota : les résidus quadratiques sont bleus et les non-résidus noirs[2]):

[2]Indiquons entre parenthèses pour chaque résidu quadratique au carré de quel nombre il est congru modulo 90 : 1 (19) 4 (38) 9 (33) 10 (10) 16 (14) 19 (37) 25 (5) 31 (29) 34 (32) 36 (36) 40 (20) 45 (45).

90	89	88	87	86	85	84	83	82	81	80	79	78	77	76	75	74	73	72	71	70	69	68
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	×						×				×						×		×			

67	66	65	64	63	62	61	60	59	58	57	56	55	54	53	52	51	50	49	48	47	46	45
23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45
×						×		×						×						×		

31 a même caractère quadratique que $31+45 = 76$ (tous les deux résidus de 90) ou bien 5 a même caractère quadratique que 50 (tous les deux non-résidus de 90).
D'autre part, si l'on ne considère que les nombres de la ligne du haut, 62 et 73 sont symétriques par rapport à la ligne médiane et leur somme est $135 = 3 \times 45$.

3 Reprise de l'idée principale

On cherche

$$p \not\equiv n \ (mod\ p_i),\ \forall\ p_i < \sqrt{n}.$$

Dans la suite, on distingue 3 sortes de nombres premiers impairs inférieurs à $\sqrt{n}$:

- les nombres premiers inférieurs à $\sqrt{n}$ qui ne divisent pas n que l'on note α_i ;
- les diviseurs de n de puissance paire dans la factorisation de n que l'on note β_i ;
- les diviseurs de n de puissance impaire dans la factorisation de n que l'on note γ_i.

On utilise la notation de Gauss : $a\ R\ b$ signifie que $\left(\frac{a}{b}\right) = +1$ tandis que $a\ N\ b$ signifie que $\left(\frac{a}{b}\right) = -1$.

Posons $n = a^2 b$ avec a le plus grand carré divisant n et $b = \gamma_1\gamma_2\ldots\gamma_k$ le produit de tous les facteurs premiers de la factorisation de n de puissance impaire.
On cherche p tel que $\frac{1}{b}.p \not\equiv a^2\ (mod\ p_i)$.

Mais comme $\frac{1}{b}$ a même caractère de résiduosité à p, un nombre premier, que b (cf. article 109 de la section Quatrième des Recherches Arithmétiques de Gauss), cela équivaut à chercher p tel que $bp\ N\ p_i$, quel que soit p_i nombre premier impair inférieur à $\sqrt{n}$.

Puisque $b = \gamma_1\gamma_2\ldots\gamma_k$, on sait déjà que $b\ R\ \gamma_i$ quel que soit γ_i un nombre premier impair inférieur à $\sqrt{n}$. Mais alors pour que $bp\ N\ \gamma_i$, il faut que $p\ N\ \gamma_i$.

Etudions maintenant la relation qui lie b à chacun des β_i et à chacun des α_i.

- si $b\ R\ \beta_1\beta_2\ldots\beta_j$ et $b\ R\ \alpha_1\alpha_2\ldots\alpha_i$ alors $b\ R\ p_i p_2\ldots p_n$ et on cherche p tel que $p\ N\ p_1 p_2\ldots p_n$. Pour ça, il faut compter combien il y a de nombres premiers de la forme $4n+3$ dans $p_1 p_2\ldots p_n$; s'ils sont en nombre impair et que p est de la forme $4n+3$, p doit être un décomposant ; s'ils sont en nombre pair et que p est non-résidu d'un nombre impair d'entre eux, il est non-résidu du tout, et il doit pouvoir également fournir une décomposition ;
- si $b\ N\ \beta_1\beta_2\ldots\beta_j$ et $b\ N\ \alpha_1\alpha_2\ldots\alpha_i$ alors ...
- si $b\ N\ \beta_1\beta_2\ldots\beta_j$ et $b\ R\ \alpha_1\alpha_2\ldots\alpha_i$ alors ...
- si $b\ R\ \beta_1\beta_2\ldots\beta_j$ et $b\ N\ \alpha_1\alpha_2\ldots\alpha_i$ alors ...

Utiliser les congruences quadratiques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

7/9/11

1 Introduction

Dans cette note, on se propose de montrer comment utiliser les congruences quadratiques pour trouver un décomposant de Goldbach d'un nombre pair donné. La conjecture de Goldbach (7 juin 1742), reformulée par Euler, stipule que tout nombre pair (supérieur à 4) est la somme de deux nombres premiers impairs.

2 Rappels

On fournit ci-dessous la table de la relation *est résidu quadratique de*. On rappelle que p est résidu quadratique de q si p est congru à un carré modulo q (i.e. si p est le reste d'une division euclidienne d'un carré par q). Cette table est la table II fournie par Gauss en annexe des Recherches Arithmétiques[1].

	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47
2	×			×			×		×		×		×		×
3	×	×			×	×			×			×			×
5	×		×		×			×		×	×		×		
7	×	×		×				×		×	×	×			×
11	×		×	×	×			×				×		×	
13	×	×				×	×		×	×				×	
17	×					×	×	×						×	×
19	×	×	×				×	×			×				
23	×			×	×	×		×	×	×			×	×	
29	×		×	×		×			×	×					
31	×	×	×		×				×		×		×	×	
37	×	×		×	×							×	×		×
41	×		×						×		×	×	×	×	
43	×	×		×		×	×	×					×	×	
47	×				×		×	×	×		×	×		×	×

Ci-dessous, on rappelle quelques théorèmes de la Section Quatrième des Recherches Arithmétiques de Gauss.

page 73, fin de l'article 98 :
On peut aussi faire usage des deux méthodes pour démontrer ce THÉORÈME[2] : *la valeur de l'expression* $\frac{a}{b}$ $(mod\ p)$*, sera un résidu, quand les nombres* a *et* b *seront tous les deux résidus ou non-résidus. Elle sera un non-résidu, quand l'un des nombres* a *et* b *sera résidu et l'autre non-résidu.*

[1] Dans la table fournie ici, inversement de celle fournie par Gauss, p est à lire en tête d'une ligne tandis que q est à lire en tête d'une colonne

[2] Ici, le mot est calligraphié en petites capitales bien que ces dernières ne soient pas utilisées par Gauss dans les Recherches Arithmétiques dans la mesure où il ne fournit pas la démonstration de ce théorème.

page 80, article 109 : en effet, il est évident que si r est un résidu, $\frac{1}{r}$ $(mod\ p)$ en sera un aussi.

page 84, article 116 : Au reste on tire facilement de ce qui précède la règle générale suivante : $+2$ est résidu de tout nombre qui n'est divisible ni par 4 ni par aucun nombre premier de la forme $8n+3$ ou $8n+5$, et non-résidu de tous les autres, par exemple, de tous ceux de la forme $8n+3$, $8n+5$, tant premiers que composés.

Dans la suite, on utilise la notation de Gauss, plutôt que le symbole de Legendre usité habituellement pour représenter la relation de congruence quadratique qui relie deux nombres : on notera $a\ R\ b$ le fait que a est résidu quadratique de b et $a\ N\ b$ le fait que a est non-résidu de b[3].

3 Mise en oeuvre

On cherche

$$p \not\equiv n\ (mod\ p_i),\ \forall\ p_i < \sqrt{n}.$$

Posons $n = a^2b$ avec a le plus grand carré divisant n et $b = \gamma_1\gamma_2\ldots\gamma_k$ le produit de tous les facteurs premiers de la factorisation de n de puissance impaire.
On cherche p tel que $\frac{1}{b}.p \not\equiv a^2\ (mod\ p_i)$.
En vertu du théorème sur les inverses (de l'article 109), cela équivaut à chercher p tel que $bp\ N\ p_i$, quel que soit p_i nombre premier impair inférieur à $\sqrt{n}$.

Pour chaque nombre premier impair p_i inférieur ou égal à $\sqrt{n}$, si $b\ R\ p_i$, il faut que $p\ N\ p_i$ et inversement, si $b\ N\ p_i$, il faut que $p\ R\ p_i$ pour que $bp\ N\ p_i$.

4 Application de notre méthode pour les nombres pairs inférieurs à 100

Dans la première démonstration de Gauss concernant le caractère de résiduosité quadratique de 2 selon n'importe quel nombre premier (article 112), il utilise une récurrence qui s'appuie sur le caractère de résiduosité quadratique de 2 selon les nombres premiers inférieurs à 100.
Dans sa première démonstration de la Loi de Réciprocité Quadratique, Gauss utilise à nouveau une démonstration par récurrence (article 136 et suivants).
Dans la dernière note (n^o 146) de son journal mathématique, il parle également du fait que Dedekind a vérifié une certaine propriété pour tous les nombres premiers inférieurs à 100.
Enfin, Euler, dans un superbe article "Découverte d'une loi tout extraordinaire des nombres par rapport à la somme de leurs diviseurs" établit le bien-fondé de ses calculs en fournissant leur résultat pour les nombres jusqu'à 100.
En suivant leur enseignement, voyons ici comment appliquer notre méthode pour les nombres inférieurs à 100 et essayons d'en induire une généralisation[4].

$100 = 2^2.5^2$. On cherche p tel que $p\ N\ 3$, $p\ N\ 5$ et $p\ N\ 7$.
17 remplit ces trois conditions et fournit une décomposition de 100.

$98 = 2.7^2$. On cherche p tel que $2p\ N\ 3$, $2p\ N\ 5$ et $2p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditinos et fournit une décomposition de 98.

$96 = 2^5.3$. On cherche p tel que $6p\ N\ 3$, $6p\ N\ 5$, et $6p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ N\ 5$ et $p\ R\ 7$.

[3]En utilisant le symbole de Legendre, : $a\ R\ b$ équivaut à $\left(\frac{a}{b}\right) = +1$ tandis que $a\ N\ b$ équivaut à $\left(\frac{a}{b}\right) = -1$
[4]On ne traite pas les nombres pairs doubles de nombres premiers qui vérifient trivialement la conjecture.

7 remplit ces trois conditions et fournit une décomposition de 96.

$92 = 2^2.23$. On cherche p tel que $23p\ N\ 3$, $23p\ N\ 5$, et $23p\ N\ 7$. Or $23\ N\ 3$, $23\ N\ 5$, et $23\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 92.

$90 = 2.3^2.5$. On cherche p tel que $10p\ N\ 3$, $10p\ N\ 5$, et $10p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $5\ N\ 3$, $5\ R\ 5$, et $5\ N\ 7$. Et donc, $10\ R\ 3$, $10\ N\ 5$, et $10\ N\ 7$. Il faut donc que $p\ N\ 3$, $p\ R\ 5$ et $p\ R\ 7$.
11 remplit ces trois conditions et fournit une décomposition de 90.

$88 = 2^3.11$. On cherche p tel que $22p\ N\ 3$, $22p\ N\ 5$, et $22p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $11\ N\ 3$, $11\ R\ 5$, et $11\ R\ 7$. Et donc, $22\ R\ 3$, $22\ N\ 5$, et $22\ R\ 7$. Il faut donc que $p\ N\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
5 remplit ces trois conditions et fournit une décomposition de 88.

$84 = 2^2.3.7$. On cherche p tel que $21p\ N\ 3$, $21p\ N\ 5$, et $21p\ N\ 7$. Or $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Et $7\ R\ 3$, $7\ N\ 5$, et $7\ R\ 7$. Et donc, $21\ R\ 3$, $21\ R\ 5$, et $21\ N\ 7$. Il faut donc que $p\ N\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
23 remplit ces trois conditions et fournit une décomposition de 84.

$80 = 2^4.5$. On cherche p tel que $5p\ N\ 3$, $5p\ N\ 5$, et $5p\ N\ 7$. Or $5\ N\ 3$, $5\ R\ 5$, et $5\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
7 remplit ces trois conditions et fournit une décomposition de 80.

$78 = 2.3.13$. On cherche p tel que $78p\ N\ 3$, $78p\ N\ 5$, et $78p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Et $13\ R\ 3$, $13\ N\ 5$, et $13\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 78.

$76 = 2^2.19$. On cherche p tel que $19p\ N\ 3$, $19p\ N\ 5$, et $19p\ N\ 7$. Or $19\ R\ 3$, $19\ R\ 5$, et $19\ N\ 7$. Il faut donc que $p\ N\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
23 remplit ces trois conditions et fournit une décomposition de 76.

$72 = 2^3.3^2$. On cherche p tel que $2p\ N\ 3$, $2p\ N\ 5$, et $2p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 72.

$70 = 2.5.7$. On cherche p tel que $70p\ N\ 3$, $70p\ N\ 5$, et $70p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $5\ N\ 3$, $5\ R\ 5$, et $5\ N\ 7$. Et $7\ R\ 3$, $7\ N\ 5$, et $7\ R\ 7$. Il faut donc que $p\ N\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
23 remplit ces trois conditions et fournit une décomposition de 70.

$66 = 2.3.11$. On cherche p tel que $66p\ N\ 3$, $66p\ N\ 5$, et $66p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Et $11\ N\ 3$, $11\ R\ 5$, et $11\ R\ 7$. Il faut donc que $p\ N\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
23 remplit ces trois conditions et fournit une décomposition de 66.

$64 = 2^6$. On cherche p tel que $p\ N\ 3$, $p\ N\ 5$ et $p\ N\ 7$.
17 remplit ces trois conditions et fournit une décomposition de 64.

$60 = 2^2.3.5$. On cherche p tel que $15p\ N\ 3$, $15p\ N\ 5$, et $15p\ N\ 7$. Or $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Et $5\ N\ 3$, $5\ R\ 5$, et $5\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 60.

$56 = 2^3.7$. On cherche p tel que $14p\ N\ 3$, $14p\ N\ 5$, et $14p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $7\ R\ 3$, $7\ N\ 5$, et $7\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ N\ 5$ et $p\ N\ 7$.
3 remplit ces trois conditions et fournit une décomposition de 53.

$54 = 2.3^3$. On cherche p tel que $6p\ N\ 3$, $6p\ N\ 5$, et $6p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Et $3\ R\ 3$, $3\ N\ 5$, et $3\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ N\ 5$ et $p\ R\ 7$.
7 remplit ces trois conditions et fournit une décomposition de 54.

$52 = 2^2.13$. On cherche p tel que $13p\ N\ 3$, $13p\ N\ 5$, et $13p\ N\ 7$. Or $13\ R\ 3$, $13\ N\ 5$, et $13\ N\ 7$. Il faut donc que $p\ N\ 3$, $p\ R\ 5$ et $p\ R\ 7$.
11 remplit ces trois conditions et fournit une décomposition de 52.

$50 = 2.5^2$. On cherche p tel que $2p\ N\ 3$, $2p\ N\ 5$, et $2p\ N\ 7$. Or $2\ N\ 3$, $2\ N\ 5$, et $2\ R\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ N\ 7$.
19 remplit ces trois conditions et fournit une décomposition de 50.

$48 = 2^4.3$. On cherche p tel que $3p\ N\ 3$ et $3p\ N\ 5$. Or $3\ R\ 3$ et $3\ N\ 5$. Il faut donc que $p\ N\ 3$ et $p\ R\ 5$.
5 remplit ces deux conditions et fournit une décomposition de 48.

$44 = 2^2.11$. On cherche p tel que $11p\ N\ 3$ et $11p\ N\ 5$. Or $11\ N\ 3$ et $11\ R\ 5$. Il faut donc que $p\ R\ 3$ et $p\ N\ 5$.
3 remplit ces deux conditions et fournit une décomposition de 44.

$42 = 2.3.7$. On cherche p tel que $42p\ N\ 3$ et $42p\ N\ 5$. Or $2\ N\ 3$ et $2\ N\ 5$. Et $3\ R\ 3$ et $3\ N\ 5$. Et $7\ R\ 3$ et $7\ N\ 5$. Il faut donc que $p\ R\ 3$ et $p\ R\ 5$.
19 remplit ces deux conditions et fournit une décomposition de 42.

$40 = 2^3.5$. On cherche p tel que $10p\ N\ 3$ et $10p\ N\ 5$. Or $2\ N\ 3$ et $2\ N\ 5$. Et $5\ N\ 3$ et $5\ R\ 5$. Il faut donc que $p\ N\ 3$ et $p\ R\ 5$.
11 remplit ces deux conditions et fournit une décomposition de 40.

$36 = 2^2.3^2$. On cherche p tel que $p\ N\ 3$ et $p\ N\ 5$.
17 remplit ces deux conditions et fournit une décomposition de 36.

$32 = 2^5$. On cherche p tel que $2p\ N\ 3$ et $2p\ N\ 5$. Or $2\ N\ 3$ et $2\ N\ 5$. Il faut donc que $p\ R\ 3$ et $p\ R\ 5$.
19 remplit ces deux conditions et fournit une décomposition de 32.

$30 = 2.3.5$. On cherche p tel que $30p\ N\ 3$ et $30p\ N\ 5$. Or $2\ N\ 3$ et $2\ N\ 5$. Et $3\ R\ 3$ et $3\ N\ 5$. Et $5\ N\ 3$ et $5\ R\ 5$.Il faut donc que $p\ N\ 3$ et $p\ N\ 5$.
17 remplit ces deux conditions et fournit une décomposition de 30.

$28 = 2^2.7$. On cherche p tel que $7p\ N\ 3$ et $7p\ N\ 5$. Or $7\ R\ 3$ et $7\ N\ 5$. Il faut donc que $p\ N\ 3$ et $p\ R\ 5$.
5 remplit ces deux conditions et fournit une décomposition de 28.

$24 = 2^3.3$. On cherche p tel que $6p\ N\ 3$. Or $2\ N\ 3$ et $3\ R\ 3$. Il faut donc que $p\ R\ 3$.
7 remplit cette condition et fournit une décomposition de 24.

$20 = 2^2.5$. On cherche p tel que $5p\ N\ 3$. Or $5\ N\ 3$. Il faut donc que $p\ R\ 3$.
3 remplit cette condition et fournit une décomposition de 20.

$18 = 2.3^2$. On cherche p tel que $2p\ N\ 3$. Or $2\ N\ 3$. Il faut donc que $p\ R\ 3$.
7 remplit cette condition et fournit une décomposition de 18.

$16 = 2^4$. On cherche p tel que $p\ N\ 3$.
5 remplit cette condition et fournit une décomposition de 16.

$12 = 2^2.3$. On cherche p tel que $3p\ N\ 3$. Or $3\ R\ 3$. Il faut donc que $p\ N\ 3$.
5 remplit cette condition et fournit une décomposition de 12.

On remarquera qu'on n'a pas traité le cas du nombre pair 68. En effet, il met en défaut la méthode de la façon suivante :
$68 = 2^2.17$. On cherche p tel que $17p\ N\ 3$, $17p\ N\ 5$, et $17p\ N\ 7$. Or $17\ N\ 3$, $17\ N\ 5$, et $17\ N\ 7$. Il faut donc que $p\ R\ 3$, $p\ R\ 5$ et $p\ R\ 7$.
Et là, aucun nombre premier ne vérifie les trois congruences quadratiques souhaitées.

Annexe : un extrait de la biographie *Poincaré : philosophe et mathématicien* d'Umberto Bottazzini aux éditions Belin Pour la Science

Au sujet du raisonnement par récurrence : le terrain le plus naturel et le plus favorable pour cette étude est l'arithmétique élémentaire, c'est à dire les opérations mettant en jeu des nombres entiers. Quand nous analysons des opérations telles que l'addition et la multiplication, nous nous rendons compte qu'un type de raisonnement se *retrouve à chaque pas*, c'est la démonstration *par récurrence* : on établit d'abord un théorème pour n égal à 1 ; on montre ensuite que, s'il est vrai de $n-1$, il est vrai de n, et on en conclut qu'il est vrai pour tous les nombres entiers. C'est là le raisonnement mathématique par excellence, déclare Poincaré. Sa particularité est qu'il contient, sous une forme condensée, une infinité de syllogismes, et qu'il permet de passer du particulier au général, du fini à l'infini, concept qui apparaît dès les premiers pas de l'arithmétique élémentaire et sans lequel il n'y aurait pas de science parce qu'il n'y aurait rien de général, mais uniquement des énoncés particuliers. D'où nous vient ce raisonnement pas récurrence, s'interroge Poincaré ? Certainement pas de l'expérience. Celle-ci peut nous suggérer que la règle est vraie pour les dix ou les cent premiers nombres, mais elle est désarmée face à l'infinité de tous les nombres naturels. Le principe de contradiction (on dirait aujourd'hui le raisonnement par l'absurde) est aussi impuissant : il nous permet d'obtenir certaines vérités, mais non d'en enfermer une infinité en une seule formule. Cette règle (le raisonnement par récurrence), inaccessible à la démonstration analytique et à l'expérience, est le véritable type du jugement synthétique a priori, conclut Poincaré. L'irrésistible évidence avec laquelle ce principe s'impose n'est autre que l'affirmation de la puissance de l'esprit qui se sait capable de concevoir la répétition indéfinie d'un même acte dès que cet acte est une fois possible.

Bibliographie

[1] **C. F. Gauss**, *Recherches Arithmétiques*, Editions Jacques Gabay, 1801.

[2] **G. Cantor**, *Vérification jusqu'à 1000 du théorème empirique de Goldbach*, Congrès de Caen de l'A.F.A.S. (Association Française pour l'Avancement des Sciences) du 10 août 1894, p.117 à 134.

[3] **R. Cuculière**, *Histoire de la Loi de Réciprocité Quadratique : Gauss et Tate*, Groupe de travail d'analyse ultramétrique, tome 7-8 (1979-1981), exp. n^o 36, p. 1-14.

Conjecture de Goldbach et résidus quadratiques

Denise Vella-Chemla

25/9/11

1 Quelles incongruences de second degré permettent de garantir les incongruences de premier degré souhaitées ?

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Cette conjecture est trivialement vérifiée par les nombres pairs doubles de nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru* à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\, n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\, q \leq \sqrt{n},\ \ p \not\equiv n\ (q)^{\dagger}$$

Dans la suite, on utilise la notation de Gauss : $a\ R\ b$ représente le fait que a est résidu quadratique de b tandis que $a\ N\ b$ représente le fait que a est non-résidu quadratique de b.

Posons $n\ =\ 2^{\alpha_0}A$ avec $A\ =\ p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_i^{\alpha_i}$.

On cherche à démontrer qu'il existe toujours un nombre premier q qui est non-résidu de tout diviseur premier impair p_k de n ($q\ N\ p_k$) et qui fournit une décomposition de Goldbach de n ($n\ =\ q+r$, avec q et r deux nombres premiers impairs).

Théorème‡ :

$$q\ N\ p_k\ \Longrightarrow\ q\ N\ p_k^{\alpha_k}$$

En vertu de la règle des produits (le produit de deux résidus ou de deux non-résidus est un résidu, le produit d'un résidu et d'un non-résidu est un non-résidu), deux cas sont à considérer selon que i est pair ou impair.

1) i est pair $\Longrightarrow\ q\ R\ A$.
On étudie alors la relation quadratique qui lie q à 2^{α_0}.
On utilise les résultats de l'article 103 des Recherches Arithmétiques (voir en annexe 2.).

- Si $\alpha_0 = 1$, si $q\ N\ 2$ alors $q\ N\ n$;
- Si $\alpha_0 = 2$, il faut trouver q de forme $4l+3$ pour que $q\ N\ 2^{\alpha_0} = 4$ et par conséquent $q\ N\ n$;

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

†Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17 sont tous congrus à 98 selon "quelqu'un".

$$98 = 2.7^2.$$
$$98 \equiv 3\ (mod\ 5).$$
$$98 \equiv 5\ (mod\ 3).$$
$$98 \equiv 7\ (mod\ 7).$$
$$98 \equiv 11\ (mod\ 3).$$
$$98 \equiv 13\ (mod\ 5).$$
$$98 \equiv 17\ (mod\ 3).$$

‡article 101 des Recherches Arithmétiques (voir en annexe 2.)

- Si $\alpha_0 \geq 3$, il faut qu'on trouve q de forme $8l+3$, $8l+5$ ou $8l+7$ de façon à ce que $q\ N\ 2^{\alpha_0}$ et par conséquent $q\ N\ n$;

2) i est impair $\implies q\ N\ A$. On étudie alors la relation quadratique qui lie q à 2^{α_0}.

- Si $\alpha_0 = 1$, $q\ R\ 2^{\alpha_0} = 2$ et par conséquent $q\ N\ n$;
- Si $\alpha_0 = 2$, il faut qu'on trouve q de forme $4l+1$ pour que $q\ R\ 2^{\alpha_0} = 4$ et par conséquent $q\ N\ n$;
- Si $\alpha_0 \geq 3$, il faut qu'on trouve q de forme $8l+1$ pour que $q\ R\ 2^{\alpha_0}$ et par conséquent $q\ N\ n$.

Dans tous les cas où on a pu aboutir à la conclusion $q\ N\ n$, tous les non-résidus quadratiques de n ne pouvant être simultanément congrus à n, l'un d'entre eux est non-congru à n[§], son complémentaire à n est premier également et il fournit une décomposition de Goldbach de n.

Annexe 1 : Illustration de l'énoncé "un nombre premier non-résidu de tous les diviseurs impairs du nombre pair n fournit une décomposition de Goldbach de n" pour les nombres pairs de 8 à 100

8, diviseur 2, 3N2, 3+5
12, diviseur 3, 5N3, 5+7
16, diviseur 2, 3N2, 3+13
18, diviseur 3, 5N3, 5+13
20, diviseur 5, 3N5, 3+17
24, diviseur 3, 5N3, 5+19
28, diviseur 7, 5N7, 5+23
30, diviseurs 3 et 5, 17N3, 17N5, 17+13
32, diviseur 2, 3N2, 3+29
36, diviseur 3, 5N3, 5+31
40, diviseur 5, 3N5, 3+37
42, diviseurs 3 et 7, 5N3, 5N7, 5+37
44, diviseur 11, 7N11, 7+37
48, diviseur 3, 5N3, 5+43
50, diviseur 5, 3N5, 3+47
52, diviseurs 3 et 13, 5N3, 5N13, 5+47
54, diviseur 3, 11N3, 11+43
56, diviseur 7, 3N7, 3+47
60, diviseurs 3 et 5, 17N3, 17N5, 17+43
64, diviseur 2, 3N2, 3+61
66, diviseurs 3 et 11, 29N3, 29N11, 29+47
68, diviseur 17, 7N17, 7+61
70, diviseurs 5 et 7, 17N5, 17N7, 17+53
72, diviseur 3, 5N3, 5+67
76, diviseur 19, 23N19, 23+53
78, diviseurs 3 et 13, 5N3, 5N13, 5+73
80, diviseur 5, 7N5, 7+73
84, diviseurs 3 et 7, 5N3, 5N7, 5+79
88, diviseur 11, 17N11, 17+71
90, diviseurs 3 et 5, 17N3, 17N5, 17+73
92, diviseur 23, 19N23, 19+73
96, diviseur 3, 17N3, 17+79
98, diviseur 7, 19N7, 19+79
100, diviseur 5, 3N5, 3+97.

[§]Là, le bât blesse, je crois, il doit être non congru à n selon tout les p_i inférieurs à $\sqrt{n}$ alors qu'il ne l'est là que selon les nombres premiers impairs divisant n.

Annexe 2 : Extraits des articles 101 et 103 des Recherches Arithmétiques

page 74, article 101 : Tout nombre non-divisible par p, qui est résidu de p, sera aussi résidu de p^n ; celui qui ne sera pas résidu de p ne le sera pas non plus de p^n.
La seconde partie de cette proposition est évidente par elle-même ; ainsi si la première n'était pas vraie, parmi les nombres plus petits que p^n et non-divisibles par p, il y en aurait plus qui fussent résidus de p qu'il n'y en aurait qui le fussent de p^n, c'est-à-dire plus de $\frac{1}{2}p^{n-1}(p-1)$. Mais on peut voir sans peine que le nombre des résidus de p qui se trouvent entre 1 et p^n, est précisément $\frac{1}{2}p^{n-1}(p-1)$.
Il est tout aussi facile de trouver effectivement un carré qui soit congru à un résidu donné, suivant le module p^n, si l'on connaît un carré congru à ce résidu suivant le module p.
Soit en effet a^2 un carré congru au résidu donné A, suivant le module p^μ, on en déduira, de la manière suivante, un carré $\equiv A$, suivant le module p^ν, ν étant $> \mu$ et non plus grand que 2μ. Supposons que la racine du carré cherché soit $\pm a + xp^\mu$; et il est aisé de s'assurer que c'est là la forme qu'elle doit avoir. Il faut donc qu'on ait $a^2 \pm 2axp^\mu + x^2p^{2\mu} \equiv A \ (mod\ p^\nu)$, ou comme $2\mu > \nu$, on aura $\pm 2axp^\mu \equiv A - a^2 \ (mod\ p^\nu)$. Soit $A - a^2 = p^\mu.d$, on aura $\pm 2ax \equiv d \ (mod\ p^{\nu-\mu})$; donc x sera la valeur de l'expression $\pm\frac{d}{2a} \ (mod\ p^{\nu-\mu})$.
Ainsi étant donné un carré congru à A, suivant le module p, on en déduira un carré congru à A, suivant le module p^2 ; de là au module p^4, au module p^8, etc.
Exemple. Etant proposé le résidu 6 congru au carré 1, suivant le module 5, on trouve le carré 9^2 auquel il est congru suivant le module 25, 16^2 auquel il est congru suivant le module 125, etc.

page 76, article 103 : Comme nous avons commencé (n^o 100) par exclure le cas où $p = 2$, il faut ajouter quelque chose à ce sujet. Quand 2 est module, tous les nombres sont résidus, et il n'y en a point de non-résidus. Quand le module est 4, tous les nombres impairs de la forme $4k + 1$ sont résidus, et tous ceux de la forme $4k + 3$ sont non-résidus. Enfin, quand le module est 8 ou une plus haute puissance de 2, tous les nombres impairs de la forme $8k + 1$ sont résidus, et les autres, ou ceux de la forme $8k + 3$, $8k + 5$, $8k + 7$ sont non-résidus ;

Bibliographie

[1] **C. F. Gauss**, *Recherches Arithmétiques*, Editions Jacques Gabay, 1801.

[2] **G. Cantor**, *Vérification jusqu'à 1000 du théorème empirique de Goldbach*, Congrès de Caen de l'A.F.A.S. (Association Française pour l'Avancement des Sciences) du 10 août 1894, p.117 à 134.

Conjecture de Goldbach et résidus quadratiques

Denise Vella-Chemla

28/9/11

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Cette conjecture est trivialement vérifiée par les nombres pairs doubles de nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru* à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\, n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\, q \leq \sqrt{n},\quad p \not\equiv n\ (q)^{\dagger}$$

Dans la suite, on utilise la notation de Gauss : $a\ R\ b$ représente le fait que a est résidu quadratique de b tandis que $a\ N\ b$ représente le fait que a est non-résidu quadratique de b.

On cherche à démontrer qu'il existe toujours un nombre premier q non-résidu de n ($q\ N\ n$) qui fournit une décomposition de Goldbach de n ($n\ =\ q+r$, avec q et r deux nombres premiers impairs).

Une telle existence provient vraisemblablement du fait que toutes les racines carrées des résidus quadratiques de n premiers à n ne peuvent être simultanément chacune congrue à n selon un nombre premier impair inférieur à $\sqrt{n}$.

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

†Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17 sont tous congrus à 98 selon "quelqu'un".

$$98 = 2.7^2.$$
$$98 \equiv 3\ (mod\ 5).$$
$$98 \equiv 5\ (mod\ 3).$$
$$98 \equiv 7\ (mod\ 7).$$

Annexe 1 : Résidus quadratiques de n premiers à n pour les nombres de 2 à 100

2 : 1
3 : 1
4 : 1
5 : 1 4
6 : 1
7 : 1 2 4
8 : 1
9 : 1 4 7
10 : 1 9
11 : 1 3 4 5 9
12 : 1
13 : 1 3 4 9 10 12
14 : 1 9 11
15 : 1 4
16 : 1 9
17 : 1 2 4 8 9 13 15 16
18 : 1 7 13
19 : 1 4 5 6 7 9 11 16 17
20 : 1 9
21 : 1 4 16
22 : 1 3 5 9 15
23 : 1 2 3 4 6 8 9 12 13 16 18
24 : 1
25 : 1 4 6 9 11 14 16 19 21 24
26 : 1 3 9 17 23 25
27 : 1 4 7 10 13 16 19 22 25
28 : 1 9 25
29 : 1 4 5 6 7 9 13 16 20 22 23 24 25 28
30 : 1 19
31 : 1 2 4 5 7 8 9 10 14 16 18 19 20 25 28
32 : 1 9 17 25
33 : 1 4 16 25 31
34 : 1 9 13 15 19 21 25 33
35 : 1 4 9 11 16 29
36 : 1 13 25
37 : 1 3 4 7 9 10 11 12 16 21 25 26 27 28 30 33 34 36
38 : 1 5 7 9 11 17 23 25 35
39 : 1 4 10 16 22 25
40 : 1 9
41 : 1 2 4 5 8 9 10 16 18 20 21 23 25 31 32 33 36 37 39 40
42 : 1 25 37
43 : 1 4 6 9 10 11 13 14 15 16 17 21 23 24 25 31 35 36 38 40 41
44 : 1 5 9 25 37
45 : 1 4 16 19 31 34
46 : 1 3 9 13 25 27 29 31 35 39 41
47 : 1 2 3 4 6 7 8 9 12 14 16 17 18 21 24 25 27 28 32 34 36 37 42
48 : 1 25
49 : 1 2 4 8 9 11 15 16 18 22 23 25 29 30 32 36 37 39 43 44 46
50 : 1 9 11 19 21 29 31 39 41 49

51 : 1 4 13 16 19 25 43 49
52 : 1 9 17 25 29 49
53 : 1 4 6 7 9 10 11 13 15 16 17 24 25 28 29 36 37 38 40 42 43 44 46 47 49 52
54 : 1 7 13 19 25 31 37 43 49
55 : 1 4 9 14 16 26 31 34 36 49
56 : 1 9 25
57 : 1 4 7 16 25 28 43 49 55
58 : 1 5 7 9 13 23 25 33 35 45 49 51 53 57
59 : 1 3 4 5 7 9 12 15 16 17 19 20 21 22 25 26 27 28 29 35 36 41 45 46 48 49 51 53 57
60 : 1 49
61 : 1 3 4 5 9 12 13 14 15 16 19 20 22 25 27 34 36 39 41 42 45 46 47 48 49 52 56 57 58 60
62 : 1 5 7 9 19 25 33 35 39 41 45 47 49 51 59
63 : 1 4 16 22 25 37 43 46 58
64 : 1 9 17 25 33 41 49 57
65 : 1 4 9 14 16 29 36 49 51 56 61 64
66 : 1 25 31 37 49
67 : 1 4 6 9 10 14 15 16 17 19 21 22 23 24 25 26 29 33 35 36 37 39 40 47 49 54 55 56 59 60
62 64 65
68 : 1 9 13 21 25 33 49 53
69 : 1 4 13 16 25 31 49 52 55 58 64
70 : 1 9 11 29 39 51
71 : 1 2 3 4 5 6 8 9 10 12 15 16 18 19 20 24 25 27 29 30 32 36 37 38 40 43 45 48 49 50
54 57 58 60 64
72 : 1 25 49
73 : 1 2 3 4 6 8 9 12 16 18 19 23 24 25 27 32 35 36 37 38 41 46 48 49 50 54 55 57 61 64
65 67 69 70 71 72
74 : 1 3 7 9 11 21 25 27 33 41 47 49 53 63 65 67 71 73
75 : 1 4 16 19 31 34 46 49 61 64
76 : 1 5 9 17 25 45 49 61 73
77 : 1 4 9 15 16 23 25 36 37 53 58 60 64 67 71
78 : 1 25 43 49 55 61
79 : 1 2 4 5 8 9 10 11 13 16 18 19 20 21 22 23 25 26 31 32 36 38 40 42 44 45 46
49 50 51 52 55 62 64 65 67 72 73 76
80 : 1 9 41 49
81 : 1 4 7 10 13 16 19 22 25 28 31 34 37 40 43 46 49 52 55 58 61 64 67 70 73 76 79
82 : 1 5 9 21 23 25 31 33 37 39 43 45 49 51 57 59 61 73 77 81
83 : 1 3 4 7 9 10 11 12 16 17 21 23 25 26 27 28 29 30 31 33 36 37 38 40 41 44 48 49
51 59 61 63 64 65 68 69 70 75 77 78 81
84 : 1 25 37
85 : 1 4 9 16 19 21 26 36 49 59 64 66 69 76 81 84
86 : 1 9 11 13 15 17 21 23 25 31 35 41 47 49 53 57 59 67 79 81 83
87 : 1 4 7 13 16 22 25 28 34 49 52 64 67 82
88 : 1 9 25 49 81
89 : 1 2 4 5 8 9 10 11 16 17 18 20 21 22 25 32 34 36 39 40 42 44 45 47 49 50 53 55
57 64 67 68 69 71 72 73 78 79 80 81 84 85 87 88
90 : 1 19 31 49 61 79
91 : 1 4 9 16 22 23 25 29 30 36 43 51 53 64 74 79 81 88
92 : 1 9 13 25 29 41 49 73 77 81 85
93 : 1 4 7 10 16 19 25 28 40 49 64 67 70 76 82
94 : 1 3 7 9 17 21 25 27 37 49 51 53 55 59 61 63 65 71 75 79 81 83 89
95 : 1 4 6 9 11 16 24 26 36 39 44 49 54 61 64 66 74 81
96 : 1 25 49 73
97 : 1 2 3 4 6 8 9 11 12 16 18 22 24 25 27 31 32 33 35 36 43 44 47 48 49 50 53 54
61 62 64 65 66 70 72 73 75 79 81 85 86 88 89 91 93 94 95 96
98 : 1 9 11 15 23 25 29 37 39 43 51 53 57 65 67 71 79 81 85 93 95
99 : 1 4 16 25 31 34 37 49 58 64 67 70 82 91 97
100 : 1 9 21 29 41 49 61 69 81 89

Annexe 2 : Illustration de l'énoncé "On trouve toujours un nombre premier non-résidu de n dont le carré est congru à un résidu de n premier à n qui fournisse une décomposition de Goldbach de n" pour les nombres pairs de 8 à 100

8, 3 N 8, $3^2 \equiv 1(8)$, 1 R 8 et 1 premier à 8, 3+5.

12, 5 N 12, $5^2 \equiv 1(12)$, 1 R 12 et 1 premier à 12, 5+7.

16, 3 N 16, $3^2 \equiv 9(16)$, 9 R 16 et 9 premier à 16, 3+13.

18, 5 N 18, $5^2 \equiv 7(18)$, 7 R 18 et 7 premier à 18, 5+13.

20, 3 N 20, $3^2 \equiv 9(20)$, 9 R 20 et 9 premier à 20, 3+17.

24, 5 N 24, $5^2 \equiv 1(24)$, 1 R 24 et 1 premier à 24, 5+19.

28, 5 N 28, $5^2 \equiv 25(28)$, 25 R 28 et 25 premier à 28, 5+23.

30, 17 N 30, $17^2 \equiv 19(30)$, 19 R 30 et 19 premier à 30, 17+13.

32, 3 N 32, $3^2 \equiv 9(32)$, 9 R 32 et 9 premier à 32, 3+29.

36, 5 N 36, $5^2 \equiv 25(36)$, 25 R 36 et 25 premier à 36, 5+31.

40, 3 N 40, $3^2 \equiv 9(40)$, 9 R 40 et 9 premier à 40, 3+37.

42, 5 N 42, $5^2 \equiv 25(42)$, 25 R 42 et 25 premier à 42, 5+37.

44, 3 N 44, $3^2 \equiv 9(44)$, 9 R 44 et 9 premier à 44, 3+41.

48, 5 N 48, $5^2 \equiv 25(48)$, 25 R 48 et 25 premier à 48, 5+43.

50, 3 N 50, $3^2 \equiv 9(50)$, 9 R 50 et 9 premier à 50, 3+47.

52, 5 N 52, $5^2 \equiv 25(52)$, 25 R 52 et 25 premier à 52, 5+47.

54, 11 N 54, $11^2 \equiv 13(54)$, 13 R 54 et 13 premier à 54, 11+43.

56, 3 N 56, $3^2 \equiv 9(56)$, 9 R 56 et 9 premier à 56, 3+53.

60, 17 N 60, $17^2 \equiv 49(60)$, 49 R 60 et 49 premier à 60, 17+43.

64, 3 N 64, $3^2 \equiv 9(64)$, 9 R 64 et 9 premier à 64, 3+61.

66, 29 N 66, $29^2 \equiv 49(66)$, 49 R 66 et 49 premier à 66, 29+37.

68, 7 N 68, $7^2 \equiv 49(68)$, 49 R 68 et 49 premier à 68, 7+61.

70, 17 N 70, $17^2 \equiv 9(70)$, 9 R 70 et 9 premier à 70, 17+73.

72, 5 N 72, $5^2 \equiv 25(72)$, 25 R 72 et 25 premier à 72, 5+67.

76, 23 N 76, $23^2 \equiv 73(76)$, 73 R 76 et 73 premier à 76, 23+53.

78, 5 N 78, $5^2 \equiv 25(78)$, 25 R 78 et 25 premier à 78, 5+73.

80, 7 N 80, $7^2 \equiv 49(80)$, 49 R 80 et 49 premier à 80, 7+73.

84, 5 N 84, $5^2 \equiv 25(84)$, 25 R 84 et 25 premier à 84, 5+79.

88, 17 N 88, $17^2 \equiv 25(88)$, 25 R 88 et 25 premier à 88, 17+71.

90, 17 N 90, $17^2 \equiv 19(90)$, 19 R 90 et 19 premier à 90, 17+73.

92, 19 N 92, $19^2 \equiv 85(92)$, 85 R 92 et 85 premier à 92, 19+73.

96, 17 N 96, $17^2 \equiv 1(96)$, 1 R 96 et 1 premier à 96, 17+79.

98, 19 N 98, $19^2 \equiv 67(98)$, 67 R 98 et 67 premier à 98, 19+79.

100, 3 N 100, $3^2 \equiv 9(100)$, 9 R 100 et 9 premier à 100, 3+97.

Bibliographie

[1] **C. F. Gauss**, *Recherches Arithmétiques*, Editions Jacques Gabay, 1801.

[2] **G. Cantor**, *Vérification jusqu'à 1000 du théorème empirique de Goldbach*, Congrès de Caen de l'A.F.A.S. (Association Française pour l'Avancement des Sciences) du 10 août 1894, p.117 à 134.

Nombre de résidus quadratiques de n quelconque qui sont premiers à n

On note RQP(n) le nombre de résidus quadratiques de n qui sont premiers à n.

$$RQP(2^2) = \frac{\varphi(n)}{2}$$

$$RQP(2^{k \geq 3}) = \frac{\varphi(n)}{4}$$

$$RQP(p) = \frac{p-1}{2}$$

$$RQP(p^2) = \frac{\varphi(n)}{2}$$

$$RQP(p^3) = \frac{\varphi(n)}{2}$$

$$RQP(p^4) = \frac{\varphi(n)}{2}$$

J'imagine que ça continue pour les puissances supérieures de p.

$$RQP(2p) = \frac{\varphi(n)}{2}$$

$$RQP(2p^2) = \frac{\varphi(n)}{2}$$

$$RQP(2p^3) = \frac{\varphi(n)}{2}$$

J'imagine que ça continue pour les puissances supérieures de p.

$$RQP(4p) = \frac{\varphi(n)}{4}$$

$$RQP(4p^2) = \frac{\varphi(n)}{4}$$

J'imagine que ça continue pour les puissances supérieures de p.

$$RQP(8p) = \frac{\varphi(n)}{8}$$

$$RQP(8p^2) = \frac{\varphi(n)}{8}$$

J'imagine que ça continue pour les puissances supérieures de p.

$$RQP(2^4p) = \frac{\varphi(n)}{8}$$

$$RQP(2^5p) = \frac{\varphi(n)}{8}$$

J'imagine que ça continue pour les puissances supérieures de 2.

$$RQP(pq) = \frac{\varphi(n)}{4}$$

$$RQP(p^2q) = \frac{\varphi(n)}{4}$$

J'imagine que ça continue pour les puissances supérieures de p.

$$RQP(2pq) = \frac{\varphi(n)}{4}$$

$$RQP(2p^2q) = \frac{\varphi(n)}{4}$$

J'imagine que ça continue pour les puissances supérieures de p.

$$RQP(2^2pq) = \frac{\varphi(n)}{8}$$

Il semblerait que l'exposant de 2 soit à prendre en compte en plus du nombre de diviseurs impairs.

Dans les tables suivantes, seules sont fournies les décompositions mettant en jeu par colonne deux unités du groupe $(Z/nZ)*$. Les décompositions de Goldbach sont marquées d'une croix. Les résidus quadratiques de n sont colorés en bleu. Remarque : comme Cantor, on considèrera que la décomposition $1 + (n - 1)$ est une décomposition de Goldbach lorsque $n - 1$ est premier.

1 Nombres pairs doubles d'impairs non premiers

Selon les modules qui sont des nombres pairs doubles d'impairs non-premiers (les $4n + 2$ qui ne sont pas doubles d'un nombre premier impair), $x\ R\ 2p \iff x + p\ R\ 2p$.

Selon le module $18 = 2.3^2$, de la forme $2(4n + 3)^2$:

17	13	11
1	5	7
	×	×

Selon le module $30 = 2p = 2.3.5$, de la forme $2(4n + 3)(4n + 1)$:

29	23	19	17
1	7	11	13
	×	×	×

Selon le module $42 = 2.3.7$, de la forme $2(4n + 3)(4n' + 3)$:

41	37	31	29	25	23
1	5	11	13	17	19
×	×	×	×		×

Selon le module $50 = 2.5^2$, de la forme $2(4n + 1)^2$:

49	47	43	41	39	37	33	31	29	27
1	3	7	9	11	13	17	19	21	23
	×	×			×		×		

Selon le module $54 = 2.3^3$, de la forme $2(4n + 3)^3$:

53	49	47	43	41	37	35	31	29
1	5	7	11	13	17	19	23	25
×		×	×	×	×		×	

Selon le module $66 = 2.3.11$, de la forme $2(4n + 3)(4n' + 3)$:

65	61	59	53	49	47	43	41	37	35
1	5	7	13	17	19	23	25	29	31
	×	×	×		×	×		×	

Selon le module $70 = 2.5.7$, de la forme $2(4n + 1)(4n' + 3)$:

69	67	61	59	57	53	51	47	43	41	39	37
1	3	9	11	13	17	19	23	27	29	31	33
	×		×		×		×		×		

Selon le module $78 = 2.3.13$, de la forme $2(4n+3)(4n'+1)$:

77	73	71	67	61	59	55	53	49	47	43	41
1	5	7	11	17	19	23	25	29	31	35	37
	×	×	×	×	×				×		×

Selon le module $90 = 2.3^2.5$, de la forme $2(4n+3)^2(4n'+1)$:

89	83	79	77	73	71	67	61	59	53	49	47
1	7	11	13	17	19	23	29	31	37	41	43
×	×	×		×	×	×	×	×	×		×

Selon le module $98 = 2.7^2$, de la forme $2(4n+3)^2$:

97	95	93	89	87	85	83	81	79	75	73	71	69	67	65	61	59	57	55	53	51
1	3	5	9	11	13	15	17	19	23	25	27	29	31	33	37	39	41	43	45	47
×								×					×		×					

On peut démontrer que x et $x+p$ ont le même caractère de résiduosité à n.

2 Nombres pairs doubles de pairs

Pour les nombres pairs doubles de pairs, on constate parfois des symétries telles que l'on a deux décompositions de Goldbach possibles, symétriques l'une de l'autre par rapport au milieu des tables.

Selon le module 8, de la forme 2^3 :

7	5
1	3
×	×

Selon le module $12 = 2^2.3$, de la forme $4(4n+3)$:

11	7
1	5
×	×

Selon le module 16, de la forme 2^4 :

15	13	11	9
1	3	5	7
	×	×	

Selon le module $20 = 2^2.5$, de la forme $4(4n+1)$:

19	17	13	11
1	3	7	9
×	×	×	

Selon le module $24 = 2^3.3$, de la forme $2^3(4n+3)$:

23	19	17	13
1	5	7	11
×	×	×	×

Selon le module $28 = 2^2.7$, de la forme $4(4n+3)$:

27	25	23	19	17	15
1	3	5	9	11	13
		×		×	

Selon le module 32, de la forme 2^5 :

31	29	27	25	23	21	19	17
1	3	5	7	9	11	13	15
×	×					×	

Selon le module $36 = 2^2.3^2$, de la forme $4(4n+3)^2$:

35	31	29	25	23	19
1	5	7	11	13	17
	×	×		×	×

Selon le module $40 = 2^4.5$, de la forme $2^4(4n+1)$:

39	37	33	31	29	27	23	21
1	3	7	9	11	13	17	19
	×			×		×	

Selon le module $44 = 2^2.11$, de la forme $4(4n+3)$:

43	41	39	37	35	31	29	27	25	23
1	3	5	7	9	13	15	17	19	21
×	×		×		×				

Selon le module $48 = 2^4.3$, de la forme $2^4(4n+3)$:

47	43	41	37	35	31	29	25
1	5	7	11	13	17	19	23
	×	×	×		×	×	

Selon le module $52 = 2^2.13$, de la forme $4(4n+1)$:

51	49	47	45	4	41	37	35	33	31	29	27
1	3	5	7	9	11	15	17	19	21	23	25
		×			×					×	

Selon le module $56 = 2^3.7$, de la forme $2^3(4n+3)$:

55	53	51	47	45	43	41	39	37	33	31	29
1	3	5	9	11	13	15	17	19	23	25	27
	×				×			×			

Selon le module $60 = 2^2.3.5$, de la forme $4(4n+3)(4n'+1)$:

59	53	49	47	43	41	37	31
1	7	11	13	17	19	23	29
×	×		×	×	×	×	×

Selon le module 64, de la forme 2^6 :

63	61	59	57	55	53	51	49	47	45	43	41	39	37	35	33
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
	×	×			×			×			×				

Selon le module $68 = 2^2.17$, de la forme $4(4n+1)$:

67	65	63	61	59	57	55	53	49	47	45	43	41	39	37	35
1	3	5	7	9	11	13	15	19	21	23	25	27	29	31	33
×			×											×	

Selon le module $72 = 2^3.3^2$, de la forme $2^3(4n+3)^2$:

71	67	65	61	59	55	53	49	47	43	41	37
1	5	7	11	13	17	19	23	25	29	31	35
×	×		×	×		×			×	×	

Selon le module $76 = 2^2.19$, de la forme $4(4n+3)$:

75	73	71	69	67	65	63	61	59	55	53	51	49	47	45	43	41	39
1	3	5	7	9	11	13	15	17	21	23	25	27	29	31	33	35	37
	×	×						×		×			×				

Selon le module $80 = 2^4.5$, de la forme $2^4(4n+1)$:

79	77	73	71	69	67	63	61	59	57	53	51	49	47	43	41
1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
×		×			×		×							×	

Selon le module $84 = 2^2.3.7$, de la forme $4(4n+3)(4n'+3)$:

83	79	73	71	67	65	61	59	55	53	47	43
1	5	11	13	17	19	23	25	29	31	37	41
×	×	×	×	×		×			×	×	×

Selon le module $88 = 2^3.11$, de la forme $2^3(4n+3)$:

87	85	83	81	79	75	73	71	69	67	65	61	59	57	55	53	51	47	45
1	3	5	9	11	13	15	17	19	23	25	27	29	31	33	37	39	41	43
		×					×					×					×	

Selon le module $92 = 2^2.23$, de la forme $4(4n+3)$:

91	89	87	85	83	81	79	77	75	73	71	67	65	63	61	59	57	55	53	51	49	47
1	3	5	7	9	11	13	15	17	19	21	25	27	29	31	33	35	37	39	41	43	45
	×					×			×					×							

Selon le module $96 = 2^5.3$, de la forme $2^5(4n+3)$:

95	91	89	85	83	79	77	73	71	67	65	61	59	55	53	49
1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
		×		×	×		×		×			×		×	

Selon le module $100 = 2^2.5^2$, de la forme $4(4n+1)^2$:

99	97	93	91	89	87	83	81	79	77	73	71	69	67	63	61	59	57	53	51
1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39	41	43	47	49
	×			×		×					×					×		×	

Pourquoi tout nombre pair sauf 2 est-il la somme de deux nombres premiers ?

Denise Vella-Chemla

5/10/11

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Cette conjecture est trivialement vérifiée par les nombres pairs doubles de nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru[1] à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\, n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\, q \leq \sqrt{n},\quad p \not\equiv n\ (q)^2$$

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z})/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Il y a $\varphi(n)$ décompositions possibles qui font intervenir deux unités complémentaires (on les a notées en annexe 2 dans chacune des colonnes de tables que l'on fournit pour les nombres pairs de 8 à 100). Le groupe des unités forme un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, \times)$. Son ordre divise l'ordre du groupe en question. Il y a donc au plus $\varphi(n)/2$ décompositions qui sont constituées de deux sommants qui sont tous les deux des unités. Par le principe des tiroirs, cela entraîne dans la plupart des cas qu'il y a au plus un résidu quadratique par colonne (ou inversement, au moins un non-résidu par colonne) ; remarque : cela n'est pas le cas lorsque les résidus quadratiques sont *"en face"* (cf par exemple la table en annexe d'un nombre de la forme $2.(4n+3)^2$ comme 50). Dans la plupart des cas donc, une décomposition de Goldbach a l'un de ses deux sommants qui est un non-résidu quadratique. Le carré de ce non-résidu est un résidu puisque le produit de deux non-résidus est un résidu. Un tel nombre est donc à chercher, s'il existe, parmi les racines carrés des résidus quadratiques inversibles de n (en annexe 1, sont fournies les racines carrées des résidus quadratiques inversibles de n pour n compris entre 2 et 100).

Il reste à comprendre, et c'est là l'essentiel, pourquoi l'une des racines carrées en question est forcément incongrue à n selon tous les nombres premiers impairs inférieurs à $\sqrt{n}$.

[1] On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

[2] Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17 sont tous congrus à 98 selon "quelqu'un".

$$98 = 2.7^2.$$
$$98 \equiv 3\ (mod\ 5).$$
$$98 \equiv 5\ (mod\ 3).$$
$$98 \equiv 7\ (mod\ 7).$$
$$98 \equiv 11\ (mod\ 3).$$
$$98 \equiv 13\ (mod\ 5).$$
$$98 \equiv 17\ (mod\ 3).$$

Annexe 1 : Résidus quadratiques inversibles de n et leur racine carrée

2 : 1 (1)
4 : 1 (3)
6 : 1 (5)
8 : 1 (7)
10 : 1 (9) 9 (7)
12 : 1 (11)
14 : 1 (13) 9 (11) 11 (9)
16 : 1 (15) 9 (13)
18 : 1 (17) 7 (13) 13 (11)
20 : 1 (19) 9 (17)
22 : 1 (21) 3 (17) 5 (15) 9 (19) 15 (13)
24 : 1 (23)
26 : 1 (25) 3 (17) 9 (23) 17 (15) 23 (19) 25 (21)
28 : 1 (27) 9 (25) 25 (23)
30 : 1 (29) 19 (23)
32 : 1 (31) 9 (29) 17 (25) 25 (27)
34 : 1 (33) 9 (31) 13 (25) 15 (27) 19 (23) 21 (19) 25 (29) 33 (21)
36 : 1 (35) 13 (29) 25 (31)
38 : 1 (37) 5 (29) 7 (27) 9 (35) 11 (31) 17 (25) 23 (21) 25 (33) 35 (23)
40 : 1 (39) 9 (37)
42 : 1 (41) 25 (37) 37 (31)
44 : 1 (43) 5 (37) 9 (41) 25 (39) 37 (35)
46 : 1 (45) 3 (39) 9 (43) 13 (29) 25 (41) 27 (25) 29 (35) 31 (33) 35 (37) 39 (27) 41 (31)
48 : 1 (47) 25 (43)
50 : 1 (49) 9 (47) 11 (31) 19 (37) 21 (39) 29 (27) 31 (41) 39 (33) 41 (29) 49 (43)
52 : 1 (51) 9 (49) 17 (41) 25 (47) 29 (43) 49 (45)
54 : 1 (53) 7 (41) 13 (43) 19 (37) 25 (49) 31 (29) 37 (35) 43 (31) 49 (47)
56 : 1 (55) 9 (53) 25 (51)
58 : 1 (57) 5 (47) 7 (35) 9 (55) 13 (39) 23 (49) 25 (53) 33 (31) 35 (37) 45 (33) 49 (51)
51 (43) 53 (45) 57 (41)
60 : 1 (59) 49 (53)
62 : 1 (61) 5 (37) 7 (41) 9 (59) 19 (53) 25 (57) 33 (39) 35 (33) 39 (47) 41 (45) 45 (49) 47 (35)
49 (55) 51 (43) 59 (51)
64 : 1 (63) 9 (61) 17 (55) 25 (59) 33 (49) 41 (51) 49 (57) 57 (53)
66 : 1 (65) 25 (61) 31 (47) 37 (53) 49 (59)
68 : 1 (67) 9 (65) 13 (59) 21 (53) 25 (63) 33 (55) 49 (61) 53 (57)
70 : 1 (69) 9 (67) 11 (61) 29 (57) 39 (47) 51 (59)
72 : 1 (71) 25 (67) 49 (65)
74 : 1 (73) 3 (59) 7 (65) 9 (71) 11 (51) 21 (61) 25 (69) 27 (45) 33 (49) 41 (39) 47 (63) 49 (67)
53 (41) 63 (47) 65 (55) 67 (57) 71 (53) 73 (43)
76 : 1 (75) 5 (67) 9 (73) 17 (63) 25 (71) 45 (65) 49 (69) 61 (59) 73 (61)
78 : 1 (77) 25 (73) 43 (67) 49 (71) 55 (61) 61 (55)
80 : 1 (79) 9 (77) 41 (69) 49 (73)
82 : 1 (81) 5 (69) 9 (79) 21 (53) 23 (49) 25 (77) 31 (61) 33 (63) 37 (59) 39 (71) 43 (65) 45 (43)
49 (75) 51 (57) 57 (45) 59 (51) 61 (67) 73 (55) 77 (47) 81 (73)
84 : 1 (83) 25 (79) 37 (73)
86 : 1 (85) 9 (83) 11 (65) 13 (63) 15 (55) 17 (67) 21 (51) 23 (61) 25 (81) 31 (69) 35 (75) 41 (59)
47 (45) 49 (79) 53 (71) 57 (53) 59 (47) 67 (57) 79 (49) 81 (77) 83 (73)
88 : 1 (87) 9 (85) 25 (83) 49 (81) 81 (79)
90 : 1 (89) 19 (73) 31 (79) 49 (83) 61 (59) 79 (77)

92 : 1 (91) 9 (89) 13 (75) 25 (87) 29 (81) 41 (77) 49 (85) 73 (71) 77 (79) 81 (83) 85 (73)
94 : 1 (93) 3 (59) 7 (77) 9 (91) 17 (55) 21 (63) 25 (89) 27 (83) 37 (79) 49 (87) 51 (49)
53 (57) 55 (61) 59 (71) 61 (69) 63 (51) 65 (73) 71 (67) 75 (81) 79 (75) 81 (85) 83 (53) 89 (65)
96 : 1 (95) 25 (91) 49 (89) 73 (83)
98 : 1 (97) 9 (95) 11 (65) 15 (57) 23 (87) 25 (93) 29 (83) 37 (73) 39(75) 43(71) 51(59)
53(51) 57(69) 65(53) 67(79) 71(85) 79(67) 81(89) 85(55) 93(81) 95(61)
100 : 1 (99) 9 (97) 21 (89) 29 (77) 41 (79) 49 (93) 61 (81) 69 (87) 81 (91) 89 (83)

Annexe 2 : tables des inversibles $(\mathbb{Z}/n\mathbb{Z})^*$ fournissant les résidus quadratiques et les décompositions de Goldbach de n

Dans les tables suivantes, seules sont fournies les décompositions mettant en jeu par colonne deux unités du groupe $(\mathbb{Z}/n\mathbb{Z})^*$. Les décompositions de Goldbach sont marquées d'une croix. Les résidus quadratiques de n sont colorés en bleu. Remarque : comme Cantor, on considèrera que la décomposition $1 + (n-1)$ est une décomposition de Goldbach lorsque $n-1$ est premier.

A2.1 : Nombres pairs doubles d'impairs non premiers

Selon les modules qui sont des nombres pairs doubles d'impairs non-premiers (les $4n+2$ qui ne sont pas doubles d'un nombre premier impair), $x\ R\ 2p \iff x+p\ R\ 2p$.

Selon le module $18 = 2.3^2$, de la forme $2(4n+3)^2$:

17	13	11
1	5	7
	×	×

Selon le module $30 = 2p = 2.3.5$, de la forme $2(4n+3)(4n+1)$:

29	23	19	17
1	7	11	13
	×	×	×

Selon le module $42 = 2.3.7$, de la forme $2(4n+3)(4n'+3)$:

41	37	31	29	25	23
1	5	11	13	17	19
×	×	×	×		×

Selon le module $50 = 2.5^2$, de la forme $2(4n+1)^2$:

49	47	43	41	39	37	33	31	29	27
1	3	7	9	11	13	17	19	21	23
	×	×			×		×		

Selon le module $54 = 2.3^3$, de la forme $2(4n+3)^3$:

53	49	47	43	41	37	35	31	29
1	5	7	11	13	17	19	23	25
×		×	×	×	×		×	

Selon le module $66 = 2.3.11$, de la forme $2(4n+3)(4n'+3)$:

65	61	59	53	49	47	43	41	37	35
1	5	7	13	17	19	23	25	29	31
	×	×	×		×	×		×	

Selon le module $70 = 2.5.7$, de la forme $2(4n+1)(4n'+3)$:

69	67	61	59	57	53	51	47	43	41	39	37
1	3	9	11	13	17	19	23	27	29	31	33
	×		×		×		×		×		

Selon le module $78 = 2.3.13$, de la forme $2(4n+3)(4n'+1)$:

77	73	71	67	61	59	55	53	49	47	43	41
1	5	7	11	17	19	23	25	29	31	35	37
	×	×	×	×	×				×		×

Selon le module $90 = 2.3^2.5$, de la forme $2(4n+3)^2(4n'+1)$:

89	83	79	77	73	71	67	61	59	53	49	47
1	7	11	13	17	19	23	29	31	37	41	43
×	×	×		×	×	×	×	×	×		×

Selon le module $98 = 2.7^2$, de la forme $2(4n+3)^2$:

97	95	93	89	87	85	83	81	79	75	73	71	69	67	65	61	59	57	55	53	51
1	3	5	9	11	13	15	17	19	23	25	27	29	31	33	37	39	41	43	45	47
×								×					×		×					

On peut démontrer que x et $x+p$ ont le même caractère de résiduosité à n.

A2.2 : Nombres pairs doubles de pairs

Pour les nombres pairs doubles de pairs, on constate parfois des symétries telles que l'on a deux décompositions de Goldbach possibles, symétriques l'une de l'autre par rapport au milieu des tables.

Selon le module 8, de la forme 2^3 :

7	5
1	3
×	×

Selon le module $12 = 2^2.3$, de la forme $4(4n+3)$:

11	7
1	5
×	×

Selon le module 16, de la forme 2^4 :

15	13	11	9
1	3	5	7
	×	×	

Selon le module $20 = 2^2.5$, de la forme $4(4n+1)$:

19	17	13	11
1	3	7	9
×	×	×	

Selon le module $24 = 2^3.3$, de la forme $2^3(4n+3)$:

23	19	17	13
1	5	7	11
×	×	×	×

Selon le module $28 = 2^2.7$, de la forme $4(4n+3)$:

27	25	23	19	17	15
1	3	5	9	11	13
		×		×	

Selon le module 32, de la forme 2^5 :

31	29	27	25	23	21	19	17
1	3	5	7	9	11	13	15
×	×					×	

Selon le module $36 = 2^2.3^2$, de la forme $4(4n+3)^2$:

35	31	29	25	23	19
1	5	7	11	13	17
	×	×		×	×

Selon le module $40 = 2^4.5$, de la forme $2^4(4n+1)$:

39	37	33	31	29	27	23	21
1	3	7	9	11	13	17	19
	×			×		×	

Selon le module $44 = 2^2.11$, de la forme $4(4n+3)$:

43	41	39	37	35	31	29	27	25	23
1	3	5	7	9	13	15	17	19	21
×	×		×		×				

Selon le module $48 = 2^4.3$, de la forme $2^4(4n+3)$:

47	43	41	37	35	31	29	25
1	5	7	11	13	17	19	23
	×	×	×		×	×	

Selon le module $52 = 2^2.13$, de la forme $4(4n+1)$:

51	49	47	45	4	41	37	35	33	31	29	27
1	3	5	7	9	11	15	17	19	21	23	25
		×			×					×	

Selon le module $56 = 2^3.7$, de la forme $2^3(4n+3)$:

55	53	51	47	45	43	41	39	37	33	31	29
1	3	5	9	11	13	15	17	19	23	25	27
	×				×			×			

Selon le module $60 = 2^2.3.5$, de la forme $4(4n+3)(4n'+1)$:

59	53	49	47	43	41	37	31
1	7	11	13	17	19	23	29
×	×		×	×	×	×	×

Selon le module 64, de la forme 2^6 :

63	61	59	57	55	53	51	49	47	45	43	41	39	37	35	33
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
	×	×			×			×			×				

Selon le module $68 = 2^2.17$, de la forme $4(4n+1)$:

67	65	63	61	59	57	55	53	49	47	45	43	41	39	37	35
1	3	5	7	9	11	13	15	19	21	23	25	27	29	31	33
×			×											×	

Selon le module $72 = 2^3.3^2$, de la forme $2^3(4n+3)^2$:

71	67	65	61	59	55	53	49	47	43	41	37
1	5	7	11	13	17	19	23	25	29	31	35
×	×		×	×		×			×	×	

Selon le module $76 = 2^2.19$, de la forme $4(4n+3)$:

75	73	71	69	67	65	63	61	59	55	53	51	49	47	45	43	41	39
1	3	5	7	9	11	13	15	17	21	23	25	27	29	31	33	35	37
	×	×						×		×			×				

Selon le module $80 = 2^4.5$, de la forme $2^4(4n+1)$:

79	77	73	71	69	67	63	61	59	57	53	51	49	47	43	41
1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39
×		×			×		×							×	

Selon le module $84 = 2^2.3.7$, de la forme $4(4n+3)(4n'+3)$:

83	79	73	71	67	65	61	59	55	53	47	43
1	5	11	13	17	19	23	25	29	31	37	41
×	×	×	×	×		×			×	×	×

Selon le module $88 = 2^3.11$, de la forme $2^3(4n+3)$:

87	85	83	81	79	75	73	71	69	67	65	61	59	57	55	53	51	47	45
1	3	5	7	9	13	15	17	19	23	25	27	29	31	33	37	39	41	43
		×					×					×					×	

Selon le module $92 = 2^2.23$, de la forme $4(4n+3)$:

91	89	87	85	83	81	79	77	75	73	71	67	65	63	61	59	57	55	53	51	49	47
1	3	5	7	9	11	13	15	17	19	21	25	27	29	31	33	35	37	39	41	43	45
	×					×			×					×							

Selon le module $96 = 2^5.3$, de la forme $2^5(4n+3)$:

95	91	89	85	83	79	77	73	71	67	65	61	59	55	53	49
1	5	7	11	13	17	19	23	25	29	31	35	37	41	43	47
		×		×	×		×		×			×		×	

Selon le module $100 = 2^2.5^2$, de la forme $4(4n+1)^2$:

99	97	93	91	89	87	83	81	79	77	73	71	69	67	63	61	59	57	53	51
1	3	7	9	11	13	17	19	21	23	27	29	31	33	37	39	41	43	47	49
	×			×		×					×					×		×	

Pourquoi tout nombre pair sauf 2 est-il la somme de deux nombres premiers ?

Denise Vella-Chemla

22/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Démonstration

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Il y a $\frac{\varphi(n)}{2}$ décompositions possibles qui font intervenir deux unités complémentaires.

On considère donc l'ensemble des unités à n, n étant un nombre pair supérieur ou égal à 6. On va démontrer que si tous les nombres premiers (forcément impairs) unités à n sont congrus à n selon un certain module, on aboutit à une contradiction. Cela aura pour conséquence que l'un des nombres premiers impairs inférieurs à n et premiers à n devant être incongru à n selon tout module premier impair inférieur à $\sqrt{n}$, ce nombre premier a son complémentaire à n qui est premier également. Le nombre premier en question est donc un décomposant de Goldbach de n.

Pour cela, on va utiliser trois éléments :

- l'article 78 des Recherches Arithmétiques : Le théorème de *Wilson* peut être rendu plus général en l'énonçant comme il suit : *le produit de tous les nombres premiers avec un nombre donné A et moindres que ce nombre, est congru suivant A, à l'unité prise positivement ou négativement.* L'unité doit être prise négativement quand A est de la forme p^m ou $2p^m$, p étant un nombre premier différent de 2, ou encore quand $A = 4$, et positivement dans tous les autres cas. Le théorème de Wilson est contenu dans le premier cas. *Exemple.* Pour $A = 15$, le produit des nombres $1, 2, 4, 7, 8, 11, 13, 14$ est $\equiv 1$ (mod 15). Nous supprimons, pour abréger, la démonstration. Nous observerons seulement qu'on peut y parvenir comme dans l'article précédent, excepté que la congruence $x^2 \equiv 1$ peut avoir plus de deux racines ; ce qui demande certaines considérations particulières. On pourrait aussi la tirer de la considération des indices, comme dans le $n°75$, si l'on y joint ce que nous dirons tout à l'heure des modules composés. ;

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

- un *"artifice technique"* que Gauss présente à la fin de la section 4 des Recherches Arithmétiques : $a \equiv b\ (mod\ m)$ est équivalent à $ca \equiv cb\ (mod\ cm)$[†].
  Par exemple, $5 \equiv 17\ (mod\ 3) \iff 35 \equiv 119\ (mod\ 21)$;
- enfin, l'extrait de l'article 5 de la section 1 des Recherches : *"On doit supposer la même identité de module dans ce qui suit."*, et plus loin, dans l'article 7, *Si* $A \equiv a$ *et* $B \equiv b$, $AB \equiv ab$ (conservation des congruences par le produit).

Ecrivons comme hypothèse initiale que chaque nombre premier impair inversible est congru à n selon un module :

$$\begin{cases} p_1 \equiv n\ (mod\ p'_1) \\ p_2 \equiv n\ (mod\ p'_2) \\ \vdots \\ p_i \equiv n\ (mod\ p'_i) \end{cases}$$

Cela nous permet d'ajouter les congruences suivantes.

$$\begin{cases} n - p_1 \equiv 0\ (mod\ p'_1) \\ n - p_2 \equiv 0\ (mod\ p'_2) \\ \vdots \\ n - p_i \equiv 0\ (mod\ p'_i) \end{cases}$$

Utilisons l'*artifice technique* pour ramener toutes les congruences selon le même module, de manière à pouvoir ensuite les multiplier entre elles. Pour cela, appelons G le plus petit commun multiple des modules p'_i[‡]. On note car cela servira ensuite que le nombre G étant un produit d'éléments inversibles ne peut être nul.

$$\begin{cases} p_1.\frac{G}{p'_1} \equiv n.\frac{G}{p'_1}\ (mod\ G) \\ p_2.\frac{G}{p'_2} \equiv n.\frac{G}{p'_2}\ (mod\ G) \\ \vdots \\ p_i.\frac{G}{p'_i} \equiv n.\frac{G}{p'_i}\ (mod\ G) \\ (n-p_1).\frac{G}{p'_1} \equiv 0.\frac{G}{p'_1}\ (mod\ G) \\ (n-p_2).\frac{G}{p'_2} \equiv 0.\frac{G}{p'_2}\ (mod\ G) \\ \vdots \\ (n-p_i).\frac{G}{p'_i} \equiv 0.\frac{G}{p'_i}\ (mod\ G) \end{cases}$$

Pour avoir une congruence portant sur chacune des unités, il nous faut cependant ajouter également les congruences suivantes, qui portent sur les c_j, les c_j étant les nombres composés premiers à n dont le complémentaire à n est lui-aussi composé. Le nombre particulier $n-1$ fait partie des p_i s'il est premier et des c_i s'il est composé même si son complémentaire, le nombre 1, n'est pas un nombre composé. Ces congruences supplémentaires vont nous permettre d'obtenir notre *"produit des unités"* de l'article 78.

$$\begin{cases} c_1 \equiv \alpha_1\ (mod\ G) \\ \vdots \\ c_j \equiv \alpha_j\ (mod\ G) \end{cases}$$

[†]L'extrait de l'article 152, page 117 est *Soit la congruence* $ax^2 + bx + c \equiv 0\ (mod\ m)$ *; elle sera équivalente à celle-ci :* $4a^2x^2 + 4abx + 4ac \equiv 0\ (mod\ 4am)$.

[‡]Il faut noter que les p'_i ne sont pas une substitution des p_i, il peut y avoir des redondances (un p'_i égal à un p'_j) et des "disparitions" (un p_i n'intervenant jamais comme module).

On obtient alors le système de congruences suivant :

$$\begin{cases} p_1.\frac{G}{p'_1} \equiv n.\frac{G}{p'_1}\ (mod\ G) \\ p_2.\frac{G}{p'_2} \equiv n.\frac{G}{p'_2}\ (mod\ G) \\ \vdots \\ p_i.\frac{G}{p'_i} \equiv n.\frac{G}{p'_i}\ (mod\ G) \\ (n-p_1).\frac{G}{p'_1} \equiv 0.\frac{G}{p'_1}\ (mod\ G) \\ (n-p_2).\frac{G}{p'_2} \equiv 0.\frac{G}{p'_2}\ (mod\ G) \\ \vdots \\ (n-p_i).\frac{G}{p'_i} \equiv 0.\frac{G}{p'_i}\ (mod\ G) \\ c_1 \equiv \alpha_1\ (mod\ G) \\ \vdots \\ c_j \equiv \alpha_j\ (mod\ G) \end{cases}$$

Du fait de la conservation des congruences par le produit lorsque le module est le même dans les différentes congruences, on peut réécrire cela en :

$$\underbrace{p_1.p_2.\ldots.p_i.(n-p_1).(n-p_2).\ldots.(n-p_i).c_1.\ldots.c_j}_{\prod_{i=1}^{\varphi(n)} u_i}.\frac{G^{2\pi(n)}}{\prod {p'_i}^2} \equiv 0.\frac{G^{2\pi(n)}}{\prod {p'_i}^2}.\prod \alpha_i\ (mod\ G)$$

On reconnaît dans le produit des éléments de gauche le produit des unités auquel Gauss fait référence dans l'article 78, qui vaut $+1$ ou -1 selon les cas.
Les produits sont nul quant à celui de gauche et nul quant à celui de droite. On a abouti à une tautologie.

Snif !

Donc on ne peut toujours pas dire qu'il existe un nombre premier incongru à n selon tout nombre premier inférieur à $\sqrt{n}$. Dommage, ce nombre premier aurait eu son complémentaire à n qui aurait été premier également et aurait ainsi fourni une décomposition de Goldbach de n...

Pourquoi tout nombre pair sauf 2 est-il la somme de deux nombres premiers ?

Denise Vella-Chemla

25/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Eléments de démonstration

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Il y a $\frac{\varphi(n)}{2}$ décompositions possibles qui font intervenir deux unités complémentaires.

On considère donc l'ensemble des unités à n, n étant un nombre pair supérieur ou égal à 6. On va démontrer que si tous les nombres premiers (forcément impairs) unités à n sont congrus à n selon un certain module, on aboutit à une contradiction. Cela aura pour conséquence que l'un des nombres premiers impairs inférieurs à n et premiers à n devant être incongru à n selon tout module premier impair inférieur à $\sqrt{n}$, ce nombre premier a son complémentaire à n qui est premier également. Le nombre premier en question est donc un décomposant de Goldbach de n.

Pour cela, on va utiliser trois éléments :

- les articles 129 page 95 et suivants des Recherches Arithmétiques : Théorème. *Si a est un nombre premier de la forme $8n+1$, il y aura nécessairement au-dessous de $2\sqrt{a}$ un nombre premier dont a est non-résidu.* ainsi que les articles suivants qui démontrent la Loi de Réciprocité Quadratique. Par exemple, dans l'article 131, *Tout nombre qui, pris positivement, est résidu ou non-résidu de p, aura pour résidu ou non-résidu, $+p$ ou $-p$, selon que p sera de la forme $4n+1$ ou $4n+3$.* Cela signifie entre les lignes que, modulo un certain nombre pair n, tous les nombres premiers unités de n ne peuvent être simultanément tous des résidus quadratiques de n ou bien tous des non-résidus quadratiques de n.

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

- enfin, l'extrait de l'article 5 de la section 1 des Recherches : *"On doit supposer la même identité de module dans ce qui suit."*, et plus loin, dans l'article 7, *Si* $A \equiv a$ *et* $B \equiv b$, $AB \equiv ab$ (conservation des congruences par le produit).

Ecrivons comme hypothèse initiale que chaque nombre premier impair inversible est congru à n selon un module :

$$\begin{cases} p_1 \equiv n \ (mod\ p'_1) \\ p_2 \equiv n \ (mod\ p'_2) \\ \vdots \\ p_i \equiv n \ (mod\ p'_i) \end{cases}$$

Première remarque : les p'_i ne peuvent être des diviseurs de n ; en effet, d'une congruence de la forme $p_i \equiv n \ (mod\ p'_i)$, on tire une congruence de la forme $n - p_i \equiv 0 \ (mod\ p'_i)$. Mais pour que p'_i puisse être un diviseur de n tout en étant module d'une telle congruence, il faudrait que p'_i divise également p_i ce qui est impossible.

Si l'on s'intéresse à deux congruences faisant intervenir respectivement les nombres premiers p_u et p'_u d'une part, et les nombres premiers p_v et p'_v d'autre part, on se trouve alors face à deux cas de figure :

- soit, sous prétexte que les p'_i ne sont jamais des diviseurs de n et qu'ils sont donc en nombre moindre que les p_i, on a une redondance des deux modules qui s'avèrent égaux $p'_u = p'_v$. Les deux congruences :

  $$\begin{cases} p_u \equiv n \ (mod\ p'_u) \\ p_v \equiv n \ (mod\ p'_v) \end{cases}$$

  se transforment en une seule

  $$p_u.p_v \equiv n^2 \ (mod\ p'_u)$$

  qui est une congruence quadratique, et nous amène à conclure que soit et p_u et p_v sont deux résidus quadratiques de n, soit et p_u et p_v sont deux non-résidus quadratiques de n (seul le produit de deux résidus ou de deux non-résidus quadratiques peut être congru à un carré) ;

- soit, on a à affaire à deux congruences de modules différents :

  $$\begin{cases} p_u \equiv n \ (mod\ p'_u) \\ p_v \equiv n \ (mod\ p'_v) \end{cases}$$

  Et là, on ne sait pas quoi faire pour se ramener à une congruence quadratique, qui nous permettrait par exemple de proche en proche d'aboutir à une contradiction sous-prétexte que tous les nombres premiers s'avèreraient être des résidus quadratiques seulement ou bien des non-résidus quadratiques seulement, ce qui est impossible.

  Donc on ne peut toujours pas dire qu'il existe un nombre premier incongru à n selon tout nombre premier impair inférieur à $\sqrt{n}$ et qui fournit une décomposition de Goldbach de n.

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à n est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$.* Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale et qui est fournie en annexe.
On réalise à ces lectures que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tous racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5+3.7+3.11+5.7+5.11+7.11.$$
$$886 = 3.5.7+3.5.11+3.7.11+5.7.11.$$
$$1155 = 3.5.7.11.$$

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$\pm x^{\pi(n-2)-1} \pm \sigma_1.x^{\pi(n-2)-2} \pm \sigma_2.x^{\pi(n-2)-3} \pm \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

La plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1+(n-1)$ n'est jamais considérée comme une décomposition de Goldbach[†], le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers considérés. Par exemple, $\sigma_1 = p_1+p_2+p_3+p_4... = 3+5+7+11...$, $\sigma_2 = p_1p_2+p_1p_3+...+p_2p_3+p_2p_4+...$ et le dernier sigma est le produit de tous les nombres premiers inférieurs à $n-2$.

Pour exprimer que $n-x$, le complémentaire du nombre à chercher doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on utilise l'équation polynomiale suivante :

$$((n-x)-3)((n-x)-5)((n-x)-7)((n-x)-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

L'élévation aux différentes puissances du monome $n-x$ donne les résultats ci-dessous :

$$\begin{aligned}(n-x)^4 &= x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 &= -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 &= n^2 - 2nx + x^2.\end{aligned}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n-x$ à la puissance i.

Les résultats de la théorie de Galois sur la résolubilité des équations polynomiales ne pourraient-ils pas être utilisés ici pour montrer que notre système de deux équations admet toujours une solution en x au moins ?...

3 Exemples

Traitons les exemples $n = 8$ et $n = 10$. Il n'y a que trois nombres premiers impairs inférieurs à n, 3, 5 *et* 7.
L'équation polynomiale $(x-3)(x-5)(x-7) = 0$ se développe en $x^3 - 15x^2 + 71x - 105 = 0$.
L'équation polynomiale portant sur $n-x$ se développe quant à elle en :
$-x^3 + (3n-15)x^2 + (-3n^2+30n-71)x + (n^3-15n^2+71n-105) = 0$.
Si on remplace n par 8, on aboutit au système

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 911 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8

Si on remplace n par 10, on aboutit au système

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

[†] même si Cantor la comptait comme telle.

Annexe

limite n. Il faut remarquer surtout que les coefficiens des variables x, y, z, ... etc., dans le développement en série de l'intégrale qui forme le premier membre de l'équation (13.), sont tels qu'en calculant un certain nombre de termes, il ne reste à peu près que ce qu'il faut pour donner le nombre des solutions de l'équation proposée. C'est de cette considération, et de l'examen attentif de la nature de ces coefficiens (qui s'expriment aussi par des intégrales définies) que l'on pourrait déduire des considérations qui jetteraient beaucoup de lumière sur la marche de la fonction représentée par la formule (13.): mais ces recherches ne sauraient trouver place ici, et nous les exposerons dans un travail particulier.

Cet aperçu suffirait déjà pour montrer de quelle manière on pourrait réduire la théorie des nombres à l'analyse ordinaire: mais nous allons reprendre maintenant cette question dans toute sa généralité.

Étant proposée une équation à plusieurs inconnues à résoudres en nombres rationnels, fractionnaires ou entiers, on pourra toujours la préparer de manière que tous les nombres cherchés doivent être entiers et positifs: puisqu'en général, si l'équation proposée est de la forme

$$\varphi(x, y, z, \ldots \text{etc.}) = 0,$$

et que l'on cherche pour x, y, z, ... etc., des valeurs fractionnaires, en faisant

$$x = \frac{x_1}{x_2}, \quad y = \frac{y_1}{y_2}, \quad z = \frac{z_1}{z_2}, \ldots \text{etc.},$$

on aura l'équation

$$\varphi\left(\frac{x_1}{x_2}, \frac{y_1}{y_2}, \frac{z_1}{z_2}, \ldots \text{etc.}\right) = 0,$$

dans laquelle il ne faudra chercher pour

$$x_1, x_2, y_1, y_2, z_1, z_2, \ldots \text{etc.},$$

que des valeurs entières: et d'ailleurs s'il y avait des solutions négatives on les obtiendrait en changeant les signes des variables. Nous supposerons par conséquent que ces réductions soient toujours effectuées dans les équations dont nous chercherons la résolution.

Soit proposé de résoudre en nombres entiers et positifs l'équation

$$\varphi(x, y, z, \ldots \text{etc.}) = 0$$

que nous représenterons comme auparavant par $\varphi = 0$. Avec les méthodes connues on s'arrête là, et on tâche de résoudre cette équation en s'aidant de la forme particulière de ses coefficiens. Mais l'équatiou $\varphi = 0$, exprime seulement les relations qui doivent exister entre les inconnues,

et n'indique pas que ces inconnues ne doivent recevoir que des valeurs entières et positives: pour exprimer cette dernière condition l'on supposera d'abord que l'on veuille trouver toutes les solutions qui s'obtiennent en donnant à x des valeurs moindres qu'une limite donnée a; à y des valeurs plus petites que b; à z des valeurs moindres que c; et ainsi de suite: $a, b, c, \ldots$ etc., étant des nombres entiers et positifs. Il est clair qu'à cet effet l'on devra donner à $x, y, z, \ldots$ etc., toutes les valeurs comprises dans les séries

$$x = 0, 1, 2, 3, \ldots\ldots\ldots a-1;$$
$$y = 0, 1, 2, 3, \ldots\ldots\ldots b-1;$$
$$z = 0, 1, 2, 3, \ldots\ldots\ldots c-1;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots \text{ etc.;}$$

et faire toutes les combinaisons possibles dans l'équation $\varphi = 0$. On observera que toutes ces valeurs de x se trouveront parmi les racines de l'équation

$$X = x(x-1)(x-2)\ldots\ldots(x-(a-1)) = 0;$$

et que de mêmes les valeurs de y et de z seront comprises parmi les racines des équations

$$Y = y(y-1)(y-2)\ldots\ldots(y-(b-1)) = 0;$$
$$Z = z(z-1)(z-2)\ldots\ldots(z-(c-1)) = 0;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{ etc.}$$

Les équations précédentes expriment les conditions que x soit un nombre entier positif moindre que a; que y soit un nombre entier positif moindre que b; et ainsi de suite. Ces équations dont le nombre est égal à celui des inconnues, étant combinées avec l'équation $\varphi = 0$, fournissent toutes les conditions du problème; de manière qu'ayant un nombre total d'équations qui surpasse de l'unité le nombre des inconnues, le problème sera plus que déterminé; en éliminant successivement toutes les inconnues entre ces équations, on aura une autre équation de condition $F = 0$, qui comprendra les limites $a, b, c, \ldots$ etc., assignées aux variables, et les coefficiens de l'équation proposée; et qui exprimera la relation qui doit exister entre ces quantités afin que le problème soit résoluble. Lorsque l'équation de condition sera satisfaite, et que l'on sera assuré que l'équation proposé peut être résolue, on reprendra l'une des équations à une seule inconnue que l'on a obtenues par l'élimination avant de parvenir à l'équation $F = 0$. Soit $X_1 = 0$, cette équation en x seul;

en cherchant le plus grand diviseur commun entre $X=0$, et $X_1=0$, on aura une équation de la forme $X_2=0$, qui ne contiendra que l'inconnue x, et dont le degré sera égal au nombre des valeurs de x qui satisfont à l'équation proposée; et en résolvant l'équation $X_2=0$, on aura toutes les valeurs de x qui satisfont à l'équation $\varphi=0$. On pourrait trouver de même les valeurs des autres inconnues, qui résolvent l'équation proposée; et l'on voit que ce principe s'applique encore à la recherche directe des racines rationnelles d'une équation à une seule inconnue; car ce problème aussi dépend de la théorie des nombres.

Avec la méthode que nous venons d'indiquer, on a seulement les racines inégales; mais s'il y a des racines égales, elles peuvent se trouver avec facilité de la manière suivante. Nous supposerons d'abord, pour simplifier la question, qu'il s'agisse d'une équation à deux inconnues seulement; puisque la méthode est absolument la même lorsque le nombre des variables est plus grand.

Maintenant soit proposé de résoudre en nombres rationnels l'équation

$$\varphi(x,y) = 0;$$

et supposons que n valeurs rationnelles de $x=a$, correspondent à une seule valeur rationnelles de $y=b$; (n étant un nombre plus grand que l'unité) en différentiant l'équation proposée par rapport à x, et cherchant le plus grand commun diviseur Δ, entre

$$\frac{d.\varphi(x,y)}{dx} \quad \text{et} \quad \varphi(x,y),$$

on aura $\Delta=F(x,y)$, et il y aura un reste $R=f(y)$ qui ne contiendra plus x, et qui par supposition devra se réduire à zéro. Si l'on fait par conséquent $f(y)=0$, on cherchera les racines rationnelles $y=b$, $y=b_1$, $y=b_2$, ... etc., de cette équation, lorsqu'il en existe, et en substituant successivement b, b_1, b_2, ... etc., pour y dans l'expression de Δ on aura les équations

$$F(x,b)=0; \quad F(x,b_1)=0; \quad F(x,b_2)=0; \ldots\ldots \text{etc.}$$

que l'on tâchera de réduire à la forme $(x-a)^{n-1}=0$; et on trouvera de cette manière les valeurs multiples de x que l'on cherche.

Si l'on avait identiquement $R=0$, on trouverait l'équation

$$\Delta = F(x,y) = (x-\psi(y))^{n-1} = 0,$$

qui devrait exister en même tems que l'équation $\varphi(x,y)=0$, et qui en serait un facteur: l'on ne pourrait donc pas déterminer de cette manière

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à n est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$"*. Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale et qui est fournie en annexe.
On réalise à ces lectures que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tous racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5+3.7+3.11+5.7+5.11+7.11.$$
$$886 = 3.5.7+3.5.11+3.7.11+5.7.11.$$
$$1155 = 3.5.7.11.$$

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$x^{\pi(n-2)-1} - \sigma_1.x^{\pi(n-2)-2} + \sigma_2.x^{\pi(n-2)-3} - \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

La plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1+(n-1)$ n'est jamais considérée comme une décomposition de Goldbach[†], le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers impairs considérés. Par exemple, $\sigma_1 = p_1 + p_2 + p_3 + p_4 ... = 3 + 5 + 7 + 11 ...$, $\sigma_2 = p_1p_2 + p_1p_3 + ... + p_2p_3 + p_2p_4 + ...$ et le dernier sigma est le produit de tous les nombres premiers impairs inférieurs à $n-2$.

Pour exprimer que $n-x$, le complémentaire du nombre à chercher doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on utilise la même équation polynomiale en remplaçant x par $n-x$:

$$((n-x)-3)((n-x)-5)((n-x)-7)((n-x)-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

L'élévation aux différentes puissances du monome $n-x$ donne les résultats ci-dessous :

$$\begin{array}{l}(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 = n^2 - 2nx + x^2.\end{array}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n-x$ à la puissance i.

Si on développe et qu'on regroupe ensemble les coefficients concernant une même puissance de x, on obtient :

$$x^4+(-4n+26)x^3+(6n^2-78n+236)x^2+(-4n^3+78n^2-472n+886)x+(n^4-26n^3+236n^2-886n+1155) = 0$$

On reconnaît dans la dernière parenthèse le polynôme initial dans lequel x a été remplacé par n. Puis pour les coefficients des puissances supérieures de x, on voit qu'on dérive successivement le polynôme initial puis les polynômes obtenus, qu'on prend l'opposé du résultat à chaque fois et qu'on divise successivement les résultats intermédiaires par 2, 3, etc.

Le polynôme initial est :

$$n^4 - 26n^3 + 236n^2 - 886n + 1155$$

On le dérive et on en prend l'opposé :

$$-4n^3 + 78n^2 - 472n + 886$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 2 :

$$6n^2 - 78n + 236$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 3 :

$$-4n + 26$$

Les coefficients d'expression $\frac{(-1)^n P^{(n)}(x)}{n!}$ sont appelés coefficients du développement de Taylor.

Les résultats de la théorie de Galois sur la résolubilité des équations polynomiales ne pourraient-ils pas être utilisés ici pour montrer que notre système de deux équations admet toujours une solution en x au moins ?...[‡]

[†] même si Cantor la comptait comme telle.

[‡] En annexe, on fournit les équations polynomiales de degré 5 qui permettent laborieusement de trouver les décomposants de Goldbach des nombres 14 et 16 qui ont comme nombres premiers impairs inférieurs à eux les nombres premiers $3, 5, 7, 11$ et 13 (!).

3 Exemples

Traitons les exemples $n = 8$ et $n = 10$. Il n'y a que trois nombres premiers impairs inférieurs à n, 3, 5 *et* 7.
L'équation polynomiale $(x-3)(x-5)(x-7) = 0$ se développe en $x^3 - 15x^2 + 71x - 105 = 0$.
L'équation polynomiale portant sur $n - x$ se développe quant à elle en :
$-x^3 + (3n-15)x^2 + (-3n^2 + 30n - 71)x + (n^3 - 15n^2 + 71n - 105) = 0$.
Si on remplace n par 8, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8.

Si on remplace n par 10, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

4 Passer d'un degré au degré supérieur

Considérons d'abord les deux premières équations des deux systèmes pour les degrés 4 et 5. On passe de l'équation :

$$x^4 - \sigma_{1,4}x^3 + \sigma_{2,4}x^2 - \sigma_{3,4}x + \sigma_{4,4} = 0$$

à l'équation :

$$x^5 - \sigma_{1,5}x^4 + \sigma_{2,5}x^3 - \sigma_{3,5}x^2 + \sigma_{4,5}x - \sigma_{5,5} = 0$$

Les coefficients de l'équation de degré 5 ont été obtenus ainsi à partir de ceux de l'équation de degré 4.

$$\begin{array}{ll} \sigma_{1,5} = \sigma_{1,4} & +p_5 \\ \sigma_{2,5} = \sigma_{2,4} & +\sigma_{1,4}.p_5 \\ \sigma_{3,5} = \sigma_{3,4} & +\sigma_{2,4}.p_5 \\ \sigma_{4,5} = \sigma_{4,4} & +\sigma_{3,4}.p_5 \\ \sigma_{5,5} = & \sigma_{4,4}.p_5 \end{array}$$

Plus généralement, si p_i désigne le $p^{ième}$ nombre premier impair,

$$\begin{array}{ll} \sigma_{1,i} = \sigma_{1,i-1} & +p_i \\ \sigma_{2,i} = \sigma_{2,i-1} & +\sigma_{1,i-1}.p_i \\ \sigma_{3,i} = \sigma_{3,i-1} & +\sigma_{2,i-1}.p_i \\ \vdots & \\ \sigma_{i-1,i} = \sigma_{i-1,i-1} & +\sigma_{i-2,i-1}.p_i \\ \sigma_{i,i} = & +\sigma_{i-1,i-1}.p_i \end{array}$$

Considérons maintenant les deux secondes équations des deux systèmes :

Peut-être est-ce à cause de ce mécanisme de passage d'un degré au degré supérieur que les équations sont toujours résolubles ?...

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

Annexe 1 : extrait du Mémoire sur la théorie des nombres de Libri qui explique comment trouver les solutions entières d'une équation

limite n. Il faut remarquer surtout que les coefficiens des variables x, y, z, ... etc., dans le développement en série de l'intégrale qui forme le premier membre de l'équation (13.), sont tels qu'en calculant un certain nombre de termes, il ne reste à peu près que ce qu'il faut pour donner le nombre des solutions de l'équation proposée. C'est de cette considération, et de l'examen attentif de la nature de ces coefficiens (qui s'expriment aussi par des intégrales définies) que l'on pourrait déduire des considérations qui jetteraient beaucoup de lumière sur la marche de la fonction représentée par la formule (13.): mais ces recherches ne sauraient trouver place ici, et nous les exposerons dans un travail particulier.

Cet aperçu suffirait déjà pour montrer de quelle manière on pourrait réduire la théorie des nombres à l'analyse ordinaire: mais nous allons reprendre maintenant cette question dans toute sa généralité.

Étant proposée une équation à plusieurs inconnues à résoudre en nombres rationnels, fractionnaires ou entiers, on pourra toujours la préparer de manière que tous les nombres cherchés doivent être entiers et positifs: puisqu'en général, si l'équation proposée est de la forme

$$\varphi(x, y, z, \ldots \text{etc.}) = 0,$$

et que l'on cherche pour x, y, z, ... etc., des valeurs fractionnaires, en faisant

$$x = \frac{x_1}{x_2}, \quad y = \frac{y_1}{y_2}, \quad z = \frac{z_1}{z_2}, \ldots \text{etc.},$$

on aura l'équation

$$\varphi\left(\frac{x_1}{x_2}, \frac{y_1}{y_2}, \frac{z_1}{z_2}, \ldots \text{etc.}\right) = 0,$$

dans laquelle il ne faudra chercher pour

$$x_1, x_2, y_1, y_2, z_1, z_2, \ldots \text{etc.},$$

que des valeurs entières: et d'ailleurs s'il y avait des solutions négatives on les obtiendrait en changeant les signes des variables. Nous supposerons par conséquent que ces réductions soient toujours effectuées dans les équations dont nous chercherons la résolution.

Soit proposé de résoudre en nombres entiers et positifs l'équation

$$\varphi(x, y, z, \ldots \text{etc.}) = 0$$

que nous représenterons comme auparavant par $\varphi = 0$. Avec les méthodes connues on s'arrête là, et on tâche de résoudre cette équation en s'aidant de la forme particulière de ses coefficiens. Mais l'équation $\varphi = 0$, exprime seulement les relations qui doivent exister entre les inconnues,

et n'indique pas que ces inconnues ne doivent recevoir que des valeurs entières et positives: pour exprimer cette dernière condition l'on supposera d'abord que l'on veuille trouver toutes les solutions qui s'obtiennent en donnant à x des valeurs moindres qu'une limite donnée a; à y des valeurs plus petites que b; à z des valeurs moindres que c; et ainsi de suite: $a, b, c, \ldots$ etc., étant des nombres entiers et positifs. Il est clair qu'à cet effet l'on devra donner à $x, y, z, \ldots$ etc., toutes les valeurs comprises dans les séries

$$x = 0, 1, 2, 3, \ldots\ldots\ldots a-1;$$
$$y = 0, 1, 2, 3, \ldots\ldots\ldots b-1;$$
$$z = 0, 1, 2, 3, \ldots\ldots\ldots c-1;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots \text{ etc.};$$

et faire toutes les combinaisons possibles dans l'équation $\varphi = 0$. On observera que toutes ces valeurs de x se trouveront parmi les racines de l'équation

$$X = x(x-1)(x-2)\ldots\ldots(x-(a-1)) = 0;$$

et que de mêmes les valeurs de y et de z seront comprises parmi les racines des équations

$$Y = y(y-1)(y-2)\ldots\ldots(y-(b-1)) = 0;$$
$$Z = z(z-1)(z-2)\ldots\ldots(z-(c-1)) = 0;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{ etc.}$$

Les équations précédentes expriment les conditions que x soit un nombre entier positif moindre que a; que y soit un nombre entier positif moindre que b; et ainsi de suite. Ces équations dont le nombre est égal à celui des inconnues, étant combinées avec l'équation $\varphi = 0$, fournissent toutes les conditions du problème; de manière qu'ayant un nombre total d'équations qui surpasse de l'unité le nombre des inconnues, le problème sera plus que déterminé; en éliminant successivement toutes les inconnues entre ces équations, on aura une autre équation de condition $F = 0$, qui comprendra les limites $a, b, c, \ldots$ etc., assignées aux variables, et les coefficiens de l'équation proposée; et qui exprimera la relation qui doit exister entre ces quantités afin que le problème soit résoluble. Lorsque l'équation de condition sera satisfaite, et que l'on sera assuré que l'équation proposé peut être résolue, on reprendra l'une des équations à une seule inconnue que l'on a obtenues par l'élimination avant de parvenir à l'équation $F = 0$. Soit $X_1 = 0$, cette équation en x seul;

en cherchant le plus grand diviseur commun entre $X=0$, et $X_1=0$, on aura une équation de la forme $X_2=0$, qui ne contiendra que l'inconnue x, et dont le degré sera égal au nombre des valeurs de x qui satisfont à l'équation proposée; et en résolvant l'équation $X_2=0$, on aura toutes les valeurs de x qui satisfont à l'équation $\varphi=0$. On pourrait trouver de même les valeurs des autres inconnues, qui résolvent l'équation proposée; et l'on voit que ce principe s'applique encore à la recherche directe des racines rationnelles d'une équation à une seule inconnue; car ce problème aussi dépend de la théorie des nombres.

Avec la méthode que nous venons d'indiquer, on a seulement les racines inégales; mais s'il y a des racines égales, elles peuvent se trouver avec facilité de la manière suivante. Nous supposerons d'abord, pour simplifier la question, qu'il s'agisse d'une équation à deux inconnues seulement; puisque la méthode est absolument la même lorsque le nombre des variables est plus grand.

Maintenant soit proposé de résoudre en nombres rationnels l'équation

$$\varphi(x,y) = 0;$$

et supposons que n valeurs rationnelles de $x=a$, correspondent à une seule valeur rationnelles de $y=b$; (n étant un nombre plus grand que l'unité) en différentiant l'équation proposée par rapport à x, et cherchant le plus grand commun diviseur Δ, entre

$$\frac{d.\varphi(x,y)}{dx} \quad \text{et} \quad \varphi(x,y),$$

on aura $\Delta=F(x,y)$, et il y aura un reste $R=f(y)$ qui ne contiendra plus x, et qui par supposition devra se réduire à zéro. Si l'on fait par conséquent $f(y)=0$, on cherchera les racines rationnelles $y=b$, $y=b_1$, $y=b_2$, ... etc., de cette équation, lorsqu'il en existe, et en substituant successivement b, b_1, b_2, ... etc., pour y dans l'expression de Δ on aura les équations

$$F(x,b)=0; \quad F(x,b_1)=0; \quad F(x,b_2)=0; \ldots . \text{ etc.}$$

que l'on tâchera de réduire à la forme $(x-a)^{n-1}=0$; et on trouvera de cette manière les valeurs multiples de x que l'on cherche.

Si l'on avait identiquement $R=0$, on trouverait l'équation

$$\Delta = F(x,y) = (x-\psi(y))^{n-1} = 0,$$

qui devrait exister en même tems que l'équation $\varphi(x,y)=0$, et qui en serait un facteur: l'on ne pourrait donc pas déterminer de cette manière

Annexe 2 : exemples de degrés 4 et 5

Si on résoud les équations dont on a calculé les coefficients en remplaçant n successivement par les valeurs 12 (équations de degré 4 car il y a 4 nombres premiers impairs inférieurs à 12 qui sont $3, 5, 7$ et 11) puis par les valeurs 14 et 16 pour n (équations polynomiales de degré 5 car on a rajouté le nombre premier impair 13) avec un outil tel que l'outil libre Sage qui permet la résolution d'équations polynomiales, on arrive à résoudre les systèmes ci-dessous.

Pour $n = 12$, il faut résoudre le système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 + (26 - 4n)x^3 + (6n^2 - 78n + 236)x^2 + (-4n^3 + 78n^2 - 472n + 886)x + (n^4 - 26n^3 + 236n^2 - 886n + 1155) = 0 \end{cases}$$

qui se ramène au système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont bien 5 et 7 qui sont bien les décomposants de Goldbach de 12.

Calculons les équations pour le degré 5 (nombres premiers impairs 3, 5, 7, 11 et 13).

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 10725 = 0$$

avec

$3 + 5 + 7 + 11 + 13 = 39$
$3.5 + 3.7 + 3.11 + 3.13 + 5.7 + 5.11 + 5.13 + 7.11 + 7.13 + 11.13 = 574$
$3.5.7 + 3.5.11 + 3.5.13 + 3.7.11 + 3.7.13 + 3.11.13 + 5.7.11 + 5.7.13 + 5.11.13 + 7.11.13 = 3954$
$3.5.7.11 + 3.5.7.13 + 3.5.11.13 + 3.7.11.13 + 5.7.11.13 = 12673$
$3.5.7.11.13 = 15015.$

En remplaçant x par $n - x$, on obtient le polynôme suivant dont on cherche quelles valeurs de x l'annulent.

$$\begin{array}{rrrrrrr} & & & & & & -x^5 \\ & & & & +(5n & -39) & x^4 \\ & & & +(-10n^2 & +156n & -574) & x^3 \\ & & +(10n^3 & -234n^2 & +1722n & -3954) & x^2 \\ & +(-5n^4 & +156n^3 & -1722n^2 & +7908n & -12673) & x^1 \\ +(n^5 & -39n^4 & +574n^3 & -3954n^2 & +12673n & -15015) & \end{array}$$

Pour $n = 14$ ou $n = 16$, il faut résoudre le système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + (5n - 39)x^4 + (-10n^2 + 156n - 574)x^3 + (10n^3 - 234n^2 + 1722n - 3954)x^2 + \\ \qquad (-5n^4 + 156n^3 - 1722n^2 + 7908n - 12673)x + (n^5 - 39n^4 + 574n^3 - 3954n^2 + 12673n - 15015) = 0 \end{cases}$$

qui se ramène dans le cas de $n = 14$ au système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont $3, 7$ et 11, qui sont bien les décomposants de Goldbach de 14.

Pour $n = 16$, le système final à résoudre est :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont $3, 5, 11$ et 13, qui sont bien les décomposants de Goldbach de 16.

Conjecture de Goldbach et résidus quadratiques

Denise Vella-Chemla

28/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru* à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\, n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\, q \leq \sqrt{n},\ \ p \not\equiv n\ (mod\ q)^{\dagger}$$

Un décomposant de Goldbach de n, s'il existe, est un élément du groupe des unités $(\mathbb{Z}/n\mathbb{Z})^*$. Son complémentaire à n appartient lui aussi au groupe des unités. Le groupe des unités forme un sous-groupe de $(\mathbb{Z}/n\mathbb{Z}, \times)$. Son ordre divise l'ordre du groupe en question. Il y a donc au plus $\varphi(n)/2$ décompositions qui sont constituées de deux sommants qui sont tous les deux des unités. Par le principe des tiroirs, cela entraîne dans la plupart des cas qu'il y a au plus un résidu quadratique par colonne (ou inversement, au moins un non-résidu par colonne) ; remarque : cela n'est pas le cas lorsque les résidus quadratiques sont *"en face"*, ce qui arrive à chaque fois que n est de la forme $2p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_i^{\alpha_i}$ avec tous les p_i de forme $4n+1$.
Dans la plupart des cas donc, une décomposition de Goldbach a l'un de ses deux sommants qui est un non-résidu quadratique (cf en Annexe 2 les décompositions de Goldbach des nombres pairs n de 8 à 100 constituées d'un sommant non-résidu quadratique de n).

2 Tentative de démonstration

Il reste à comprendre, et c'est là l'essentiel, pourquoi l'un des nombres premiers non-résidus de n est forcément incongru à n selon tous les nombres premiers impairs inférieurs à $\sqrt{n}$.
Pour cela, on aimerait utiliser un extrait du Mémoire sur la théorie des nombres de Libri [1] (4° de la page en annexe) qui énonce *En multipliant le résidu quadratique a_r, successivement par tous les non-résidus quadratiques,*

$$b_1, b_2, b_3, \ldots, b_u, \ldots, b_p,$$

on aura de nouveau, après avoir divisé tous les produits par n, p restes différents, qui seront tous les non-résidus quadratiques de n.

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

†Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17 sont tous congrus à 98 selon "quelqu'un".

$$98 = 2.7^2.$$
$$98 \equiv 3\ (mod\ 5).$$
$$98 \equiv 5\ (mod\ 3).$$
$$98 \equiv 7\ (mod\ 7).$$
$$98 \equiv 11\ (mod\ 3).$$
$$98 \equiv 13\ (mod\ 5).$$
$$98 \equiv 17\ (mod\ 3).$$

On peut représenter cela de la manière suivante :

$$r.\begin{pmatrix} n_1 \\ n_2 \\ \vdots \\ n_k \end{pmatrix} = \begin{pmatrix} n'_1 \\ n'_2 \\ \vdots \\ n'_k \end{pmatrix} \begin{matrix} (mod\ n) \\ (mod\ n) \\ \vdots \\ (mod\ n) \end{matrix}$$

avec r désignant un résidu quadratique de n, $n_1, \ldots, n_k$ désignant les non-résidus quadratiques de n et les n'_i étant une substitution des n_i.
Si l'on note $f_r : \mathcal{N}_n \to \mathcal{N}_n$ la substitution en question, au bout d'un certain nombre d'applications de f_r, on va retrouver l'ensemble de non-résidus dans l'ordre initial, ce que l'on écrit :

$$\exists m, (f_r)^m = 1_{\mathcal{N}_n}.$$

La contradiction pourrait peut-être venir du fait que n étant un résidu quadratique particulier de n, on peut multiplier l'ensemble des non-résidus par ce résidu particulier en place de r, mais comme $n \equiv 0\ (mod\ n)$, les non-résidus vont "être absorbés" par cette multiplication par n et on ne va pas pouvoir trouver tous les non-résidus, à de multiples substitutions près, au fur et à mesure de l'application de f_r.

On pourrait alors dire qu'il existe un nombre premier (il se trouve que c'est un non-résidu quadratique de n) incongru à n selon tout nombre premier inférieur à $\sqrt{n}$ (Le problème vient ici du fait qu'on n'a pas travaillé modulo des nombres premiers inférieurs à $\sqrt{n}$ mais modulo n, ce qui ne va pas.). Si on trouvait le moyen d'aboutir à une contradiction en partant de l'hypothèse que tous les nombres premiers non-résidus quadratiques de n ne peuvent être simultanément congrus à n selon un certain module chacun, un nombre premier non-résidu quadratique de n aurait son complémentaire à n qui serait premier également et il fournirait une décomposition de Goldbach de n.

Bibliographie

[1], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

Annexe 1 : page 44 du Mémoire sur la théorie des nombres de Guillaume Libri

$$b_1,\ b_2,\ b_3,\ \ldots\ b_u,\ \ldots\ b_p,$$

les p non-résidus quadratiques, on aura les équations

$$\sum_{x=1}^{x=n}\cos\frac{2x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n};\quad \sum_{x=1}^{x=n}\sin\frac{2x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n};$$

$$\sum_{u=1}^{u=p+1}\left(\cos\frac{2a_u\pi}{n}+\cos 2\frac{b_u\pi}{n}\right)=\sum_{\gamma=1}^{\gamma=n}\cos\frac{2\gamma\pi}{n};\quad \sum_{u=1}^{u=p+1}\left(\sin\frac{2a_u\pi}{n}+\sin\frac{2b_u\pi}{n}\right)=\sum_{\gamma=1}^{\gamma=n}\sin\frac{2\gamma\pi}{n}.$$

3°. En multipliant successivement un résidu quadratique quelconque a_r, par tous les autres, on aura la série

$$a_r a_1,\ a_r a_2,\ a_r a_3,\ \ldots\ a_r a_p,$$

qui fournira de nouveau, en divisant tous ses termes par n, p restes différens, qui seront tous les résidus quadratiques de n disposés dans un ordre quelconque; d'où l'on déduira

$$30.\quad \begin{cases}\displaystyle\sum_{x=1}^{x=n}\cos\frac{2a_r x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\cos\frac{2a_r a_u\pi}{n}=2\sum_{u=1}^{u=p+1}\cos\frac{2a_u\pi}{n};\\ \displaystyle\sum_{x=1}^{x=n}\sin\frac{2a_r x^2\pi}{n}=2\sum_{u=1}^{u=p+1}\sin\frac{2a_r a_u\pi}{n}=2\sum_{u=1}^{u=p+1}\sin\frac{2a_u\pi}{n}.\end{cases}$$

4°. En multipliant le résidu quadratique a_r, successivement par tous les non-résidus quadratiques

$$b_1,\ b_2,\ b_3,\ \ldots\ b_u,\ \ldots\ b_p,$$

on aura de nouveau, après avoir divisé tous les produits par n, p restes différens, qui seront tous les non-résidus quadratiques de n, et on trouvera

$$31.\quad \begin{cases}\displaystyle\sum_{u=1}^{u=p+1}\cos\frac{2a_r b_u\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n};\\ \displaystyle\sum_{u=1}^{u=p+1}\sin\frac{2a_r b_u\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}.\end{cases}$$

5°. En multipliant le non-résidu quadratique b_r, successivement par tous les résidus quadratiques

$$a_1,\ a_2,\ a_3,\ \ldots\ a_u,\ \ldots\ a_p,$$

et divisant tous les produits par n, on aura pour restes tous les non-résidus quadratiques; et par conséquent on obtiendra

$$32.\quad \begin{cases}\displaystyle\sum_{u=1}^{u=p+1}\cos\frac{2b_r a_u\pi}{n}=\sum_{u=1}^{u=p+1}\cos\frac{2b_u\pi}{n};\\ \displaystyle\sum_{u=1}^{u=p+1}\sin\frac{2b_r a_u\pi}{n}=\sum_{u=1}^{u=p+1}\sin\frac{2b_u\pi}{n}.\end{cases}$$

6°. Enfin en multipliant successivement un non-résidu quadratique quelconque b_r, par tous les non-résidus quadratiques

$$b_1,\ b_2,\ b_3,\ \ldots\ b_u,\ \ldots\ b_p,$$

Annexe 2 : Illustration de l'énoncé "On trouve toujours un nombre premier non-résidu de n qui fournisse une décomposition de Goldbach de n" pour les nombres pairs de 8 à 100

8, 3 N 8, 3+5.
12, 5 N 12, 5+7.
16, 3 N 16, 3+13.
18, 5 N 18, 5+13.
20, 3 N 20, 3+17.
24, 5 N 24, 5+19.
28, 5 N 28, 5+23.
30, 17 N 30, 17+13.
32, 3 N 32, 3+29.
36, 5 N 36, 5+31.
40, 3 N 40, 3+37.
42, 5 N 42, 5+37.
44, 3 N 44, 3+41.
48, 5 N 48, 5+43.
50, 3 N 50, 3+47.
52, 5 N 52, 5+47.
54, 11 N 54, 11+43.
56, 3 N 56, 3+53.
60, 17 N 60, 17+43.
64, 3 N 64, 3+61.
66, 29 N 66, 29+37.
68, 7 N 68, 7+61.
70, 17 N 70, 17+73.
72, 5 N 72, 5+67.
76, 23 N 76, 23+53.
78, 5 N 78, 5+73.
80, 7 N 80, 7+73.
84, 5 N 84, 5+79.
88, 17 N 88, 17+71.
90, 17 N 90, 17+73.
92, 19 N 92, 19+73.
96, 17 N 96, 17+79.
98, 19 N 98, 19+79.
100, 3 N 100, 3+97.

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à n est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$.* Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale et qui est fournie en annexe.
On réalise à ces lectures que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tous racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5+3.7+3.11+5.7+5.11+7.11.$$
$$886 = 3.5.7+3.5.11+3.7.11+5.7.11.$$
$$1155 = 3.5.7.11.$$

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$x^{\pi(n-2)-1} - \sigma_1.x^{\pi(n-2)-2} + \sigma_2.x^{\pi(n-2)-3} - \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

La plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1+(n-1)$ n'est jamais considérée comme une décomposition de Goldbach[†], le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers impairs considérés. Par exemple, $\sigma_1 = p_1 + p_2 + p_3 + p_4 ... = 3 + 5 + 7 + 11 ...$, $\sigma_2 = p_1p_2 + p_1p_3 + ... + p_2p_3 + p_2p_4 + ...$ et le dernier sigma est le produit de tous les nombres premiers inférieurs à $n-2$.

Pour exprimer que $n-x$, le complémentaire du nombre à chercher doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on utilise la même équation polynomiale en remplaçant x par $n-x$:

$$((n-x)-3)((n-x)-5)((n-x)-7)((n-x)-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

L'élévation aux différentes puissances du monome $n-x$ donne les résultats ci-dessous :

$$\begin{array}{l}(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 = n^2 - 2nx + x^2.\end{array}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n-x$ à la puissance i.

Si on développe et qu'on regroupe ensemble les coefficients concernant une même puissance de x, on obtient :

$$x^4+(-4n+26)x^3+(6n^2-78n+236)x^2+(-4n^3+78n^2-472n+886)x+(n^4-26n^3+236n^2-886n+1155) = 0$$

On reconnaît dans la dernière parenthèse le polynôme initial dans lequel x a été remplacé par n. Puis pour les coefficients des puissances supérieures de x, on voit qu'on dérive successivement le polynôme initial puis les polynômes obtenus, qu'on prend l'opposé du résultat à chaque fois et qu'on divise successivement les résultats intermédiaires par 2, 3, etc.

Le polynôme initial est :

$$n^4 - 26n^3 + 236n^2 - 886n + 1155$$

On le dérive et on en prend l'opposé :

$$-4n^3 + 78n^2 - 472n + 886$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 2 :

$$6n^2 - 78n + 236$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 3 :

$$-4n + 26$$

Les coefficients d'expression $\frac{(-1)^n P^{(n)}(x)}{n!}$ sont appelés coefficients du développement de Taylor.

Les résultats de la théorie de Galois sur la résolubilité des équations polynomiales ne pourraient-ils pas être utilisés ici pour montrer que notre système de deux équations admet toujours une solution en x au moins ?...[‡]

[†] même si Cantor la comptait comme telle.

[‡] En annexe, on fournit les équations polynomiales de degré 5 qui permettent laborieusement de trouver les décomposants de Goldbach des nombres 14 et 16 qui ont comme nombres premiers impairs inférieurs à eux les nombres premiers $3, 5, 7, 11$ et 13 (!).

3 Exemples

Traitons les exemples $n = 8$ et $n = 10$. Il n'y a que trois nombres premiers impairs inférieurs à n, 3, 5 *et* 7.
L'équation polynomiale $(x-3)(x-5)(x-7) = 0$ se développe en $x^3 - 15x^2 + 71x - 105 = 0$.
L'équation polynomiale portant sur $n - x$ se développe quant à elle en :
$-x^3 + (3n-15)x^2 + (-3n^2 + 30n - 71)x + (n^3 - 15n^2 + 71n - 105) = 0$.
Si on remplace n par 8, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 911 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8.

Si on remplace n par 10, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

Annexe 1 : extrait du Mémoire sur la théorie des nombres de Libri qui explique comment trouver les solutions entières d'une équation

limite n. Il faut remarquer surtout que les coefficiens des variables x, y, z, ... etc., dans le développement en série de l'intégrale qui forme le premier membre de l'équation (13.), sont tels qu'en calculant un certain nombre de termes, il ne reste à peu près que ce qu'il faut pour donner le nombre des solutions de l'équation proposée. C'est de cette considération, et de l'examen attentif de la nature de ces coefficiens (qui s'expriment aussi par des intégrales définies) que l'on pourrait déduire des considérations qui jetteraient beaucoup de lumière sur la marche de la fonction représentée par la formule (13.): mais ces recherches ne sauraient trouver place ici, et nous les exposerons dans un travail particulier.

Cet aperçu suffirait déjà pour montrer de quelle manière on pourrait réduire la théorie des nombres à l'analyse ordinaire: mais nous allons reprendre maintenant cette question dans toute sa généralité.

Étant proposée une équation à plusieurs inconnues à résoudre en nombres rationnels, fractionnaires ou entiers, on pourra toujours la préparer de manière que tous les nombres cherchés doivent être entiers et positifs: puisqu'en général, si l'équation proposée est de la forme

$$\varphi(x, y, z, \ldots \text{etc.}) = 0,$$

et que l'on cherche pour x, y, z, ... etc., des valeurs fractionnaires, en faisant

$$x = \frac{x_1}{x_2}, \quad y = \frac{y_1}{y_2}, \quad z = \frac{z_1}{z_2}, \ldots \text{etc.},$$

on aura l'équation

$$\varphi\left(\frac{x_1}{x_2}, \frac{y_1}{y_2}, \frac{z_1}{z_2}, \ldots \text{etc.}\right) = 0,$$

dans laquelle il ne faudra chercher pour

$$x_1, x_2, y_1, y_2, z_1, z_2, \ldots \text{etc.},$$

que des valeurs entières: et d'ailleurs s'il y avait des solutions négatives on les obtiendrait en changeant les signes des variables. Nous supposerons par conséquent que ces réductions soient toujours effectuées dans les équations dont nous chercherons la résolution.

Soit proposé de résoudre en nombres entiers et positifs l'équation

$$\varphi(x, y, z, \ldots \text{etc.}) = 0$$

que nous représenterons comme auparavant par $\varphi = 0$. Avec les méthodes connues on s'arrête là, et on tâche de résoudre cette équation en s'aidant de la forme particulière de ses coefficiens. Mais l'équation $\varphi = 0$, exprime seulement les relations qui doivent exister entre les inconnues,

et n'indique pas que ces inconnues ne doivent recevoir que des valeurs entières et positives: pour exprimer cette dernière condition l'on supposera d'abord que l'on veuille trouver toutes les solutions qui s'obtiennent en donnant à x des valeurs moindres qu'une limite donnée a; à y des valeurs plus petites que b; à z des valeurs moindres que c; et ainsi de suite: $a, b, c, \ldots$ etc., étant des nombres entiers et positifs. Il est clair qu'à cet effet l'on devra donner à $x, y, z, \ldots$ etc., toutes les valeurs comprises dans les séries

$$x = 0, 1, 2, 3, \ldots\ldots\ldots a-1;$$
$$y = 0, 1, 2, 3, \ldots\ldots\ldots b-1;$$
$$z = 0, 1, 2, 3, \ldots\ldots\ldots c-1;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots \text{ etc.};$$

et faire toutes les combinaisons possibles dans l'équation $\varphi = 0$. On observera que toutes ces valeurs de x se trouveront parmi les racines de l'équation

$$X = x(x-1)(x-2)\ldots\ldots(x-(a-1)) = 0;$$

et que de mêmes les valeurs de y et de z seront comprises parmi les racines des équations

$$Y = y(y-1)(y-2)\ldots\ldots(y-(b-1)) = 0;$$
$$Z = z(z-1)(z-2)\ldots\ldots(z-(c-1)) = 0;$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \text{ etc.}$$

Les équations précédentes expriment les conditions que x soit un nombre entier positif moindre que a; que y soit un nombre entier positif moindre que b; et ainsi de suite. Ces équations dont le nombre est égal à celui des inconnues, étant combinées avec l'équation $\varphi = 0$, fournissent toutes les conditions du problème; de manière qu'ayant un nombre total d'équations qui surpasse de l'unité le nombre des inconnues, le problème sera plus que déterminé; en éliminant successivement toutes les inconnues entre ces équations, on aura une autre équation de condition $F = 0$, qui comprendra les limites $a, b, c, \ldots$ etc., assignées aux variables, et les coefficiens de l'équation proposée; et qui exprimera la relation qui doit exister entre ces quantités afin que le problème soit résoluble. Lorsque l'équation de condition sera satisfaite, et que l'on sera assuré que l'équation proposé peut être résolue, on reprendra l'une des équations à une seule inconnue que l'on a obtenues par l'élimination avant de parvenir à l'équation $F = 0$. Soit $X_1 = 0$, cette équation en x seul;

en cherchant le plus grand diviseur commun entre $X=0$, et $X_1=0$, on aura une équation de la forme $X_2=0$, qui ne contiendra que l'inconnue x, et dont le degré sera égal au nombre des valeurs de x qui satisfont à l'équation proposée; et en résolvant l'équation $X_2=0$, on aura toutes les valeurs de x qui satisfont à l'équation $\varphi=0$. On pourrait trouver de même les valeurs des autres inconnues, qui résolvent l'équation proposée; et l'on voit que ce principe s'applique encore à la recherche directe des racines rationnelles d'une équation à une seule inconnue; car ce problème aussi dépend de la théorie des nombres.

Avec la méthode que nous venons d'indiquer, on a seulement les racines inégales; mais s'il y a des racines égales, elles peuvent se trouver avec facilité de la manière suivante. Nous supposerons d'abord, pour simplifier la question, qu'il s'agisse d'une équation à deux inconnues seulement; puisque la méthode est absolument la même lorsque le nombre des variables est plus grand.

Maintenant soit proposé de résoudre en nombres rationnels l'équation

$$\varphi(x,y) = 0;$$

et supposons que n valeurs rationnelles de $x=a$, correspondent à une seule valeur rationnelles de $y=b$; (n étant un nombre plus grand que l'unité) en différentiant l'équation proposée par rapport à x, et cherchant le plus grand commun diviseur Δ, entre

$$\frac{d.\varphi(x,y)}{dx} \quad \text{et} \quad \varphi(x,y),$$

on aura $\Delta=F(x,y)$, et il y aura un reste $R=f(y)$ qui ne contiendra plus x, et qui par supposition devra se réduire à zéro. Si l'on fait par conséquent $f(y)=0$, on cherchera les racines rationnelles $y=b$, $y=b_1$, $y=b_2$, ... etc., de cette équation, lorsqu'il en existe, et en substituant successivement b, b_1, b_2, ... etc., pour y dans l'expression de Δ on aura les équations

$$F(x,b)=0; \quad F(x,b_1)=0; \quad F(x,b_2)=0; \ldots . \text{ etc.}$$

que l'on tâchera de réduire à la forme $(x-a)^{n-1}=0$; et on trouvera de cette manière les valeurs multiples de x que l'on cherche.

Si l'on avait identiquement $R=0$, on trouverait l'équation

$$\Delta = F(x,y) = (x-\psi(y))^{n-1} = 0,$$

qui devrait exister en même tems que l'équation $\varphi(x,y)=0$, et qui en serait un facteur: l'on ne pourrait donc pas déterminer de cette manière

Annexe 2 : nos deux équations pour le degré 5

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 10725 = 0$$

avec

$3 + 5 + 7 + 11 + 13 = 39$
$3.5 + 3.7 + 3.11 + 3.13 + 5.7 + 5.11 + 5.13 + 7.11 + 7.13 + 11.13 = 574$
$3.5.7 + 3.5.11 + 3.5.13 + 3.7.11 + 3.7.13 + 3.11.13 + 5.7.11 + 5.7.13 + 5.11.13 + 7.11.13 = 3954$
$3.5.7.11 + 3.5.7.13 + 3.5.11.13 + 3.7.11.13 + 5.7.11.13 = 12673$
$3.5.7.11.13 = 10725.$

En remplaçant x par $n - x$, on obtient le polynôme suivant dont on cherche quelles valeurs de x l'annulent.

$$\begin{array}{rrrrrrr}
 & & & & & & -x^5 \\
 & & & & (5n & -39) & x^4 \\
 & & & (-10n^2 & +156n & -574) & x^3 \\
 & & (10n^3 & -234n^2 & +1722n & -3954) & x^2 \\
 & (-5n^4 & +156n^3 & -1722n^2 & +7908n & -12673) & x^1 \\
(n^5 & -39n^4 & +574n^3 & -3954n^2 & +12673n & -10725) &
\end{array}$$

Conjecture de Goldbach d'un point de vue analytique

Denise Vella-Chemla

31/10/2011

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
On rappelle que p est un décomposant de Goldbach de n si p est un nombre premier incongru* à n selon tout module premier inférieur à $\sqrt{n}$.

$$\forall\ n \geq 6,\ \ n\ =\ p+q,\ p\ et\ q\ premiers\ impairs \iff \forall\ q \leq \sqrt{n},\quad p \not\equiv n\ (mod\ q)^{\dagger}$$

On note $\pi(x;q,a)$ l'ensemble des nombres premiers $p \leq x$ tels que $p \equiv a\ (mod\ q)$.

Théorème de Brun-Titchmarsh : Soit $q \geq 1$ un entier et a un entier premier à q. Pour M et N deux entiers ≥ 1, le nombre Z de nombres premiers congrus à a modulo q et dans l'intervalle $[M+1, M+N]$ est au plus $\frac{2N}{\varphi(q)ln(N/q)}$.

$$\pi(x;q,a) \leq \frac{2x}{\varphi(q)ln(x/q)}\ pour\ tout\ x > q.$$

.

Si on note $NbGoldbach(n)$ le nombre de décompositions de Goldbach de n, on a vu qu'il suffit d'enlever de l'ensemble des nombres premiers inférieurs à $n/2$ dont le nombre est $\pi(n/2)$ (qui tend vers $\frac{n/2}{ln(n/2)}$ selon le théorème d'Hadamard-De La Vallée Poussin) le nombre de nombres premiers à $n/2$ et congrus à $n/2$ modulo chacun des nombres premiers p_i inférieur à $\sqrt{n}$.
On obtient finalement le résultat :

$$NbGoldbach(n) = \frac{n^2}{2ln(n/2)\prod_{p_i}\varphi(p_i)ln(n/2p_i)}$$

p_i désignant tout nombre premier impair inférieur à $\sqrt{n}$.

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

†Par exemple, 98 a pour plus petit décomposant de Goldbach 19 parce que 3, 5, 7, 11, 13 et 17 sont tous congrus à 98 selon "quelqu'un".

$98 = 2.7^2$.
$98 \equiv 3\ (mod\ 5)$.
$98 \equiv 5\ (mod\ 3)$.
$98 \equiv 7\ (mod\ 7)$.
$98 \equiv 11\ (mod\ 3)$.
$98 \equiv 13\ (mod\ 5)$.
$98 \equiv 17\ (mod\ 3)$.

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à n est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$"*. Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale et qui est fournie en annexe.
On réalise à ces lectures que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tous racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5+3.7+3.11+5.7+5.11+7.11.$$
$$886 = 3.5.7+3.5.11+3.7.11+5.7.11.$$
$$1155 = 3.5.7.11.$$

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$x^{\pi(n-2)-1} - \sigma_1.x^{\pi(n-2)-2} + \sigma_2.x^{\pi(n-2)-3} - \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

La plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1+(n-1)$ n'est jamais considérée comme une décomposition de Goldbach[†], le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers impairs considérés. Par exemple, $\sigma_1 = p_1 + p_2 + p_3 + p_4 ... = 3 + 5 + 7 + 11 ...$, $\sigma_2 = p_1p_2 + p_1p_3 + ... + p_2p_3 + p_2p_4 + ...$ et le dernier sigma est le produit de tous les nombres premiers impairs inférieurs à $n-2$.

Pour exprimer que $n-x$, le complémentaire du nombre à chercher doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on utilise la même équation polynomiale en remplaçant x par $n-x$; si l'on considère les 4 premiers nombres premiers impairs seulement, l'équation polynomiale devient :

$$((n-x)-3)((n-x)-5)((n-x)-7)((n-x)-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

L'élévation aux différentes puissances du monome $n-x$ donne les résultats ci-dessous :

$$\begin{array}{l}(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 = n^2 - 2nx + x^2.\end{array}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n-x$ à la puissance i.

Si on développe et qu'on regroupe ensemble les coefficients concernant une même puissance de x, on obtient :

$$x^4+(-4n+26)x^3+(6n^2-78n+236)x^2+(-4n^3+78n^2-472n+886)x+(n^4-26n^3+236n^2-886n+1155) \;=\; 0$$

On reconnaît dans la dernière parenthèse le polynôme initial dans lequel x a été remplacé par n. Puis pour les coefficients des puissances supérieures de x, on voit qu'on dérive successivement le polynôme initial puis les polynômes obtenus, qu'on prend l'opposé du résultat à chaque fois et qu'on divise successivement les résultats intermédiaires par 2, 3, etc.

Pour le degré 4, le polynôme initial est :

$$n^4 - 26n^3 + 236n^2 - 886n + 1155$$

On le dérive et on en prend l'opposé :

$$-4n^3 + 78n^2 - 472n + 886$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 2 :

$$6n^2 - 78n + 236$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 3 :

$$-4n + 26$$

Les coefficients d'expression $\frac{(-1)^n P^{(n)}(x)}{n!}$ sont appelés coefficients du développement de Taylor.

[†]même si Cantor la comptait comme telle.

On est donc systématiquement ramené au système d'équations à deux équations de degré i suivant, dont il faudrait réussir à prouver qu'il admet systématiquement au moins une solution :

$$\begin{cases} P(x) : x^{\pi(n-2)-1} - \sigma_1.x^{\pi(n-2)-2} + \sigma_2.x^{\pi(n-2)-3} - \sigma_3.x^{\pi(n-2)-1} \ldots = 0 \\ \sum_{i=0}^{i=\pi(n-2)-1} \frac{(-1)^i P^{(i)}(n)}{i!} x^i = 0 \end{cases}$$

Les résultats de la théorie de Galois sur la résolubilité des équations polynomiales ne pourraient-ils pas être utilisés ici pour montrer que notre système de deux équations admet toujours une solution en x au moins ?...[‡]

3 Exemples

Traitons les exemples $n = 8$ et $n = 10$. Il n'y a que trois nombres premiers impairs inférieurs à n, 3, 5 *et* 7.
L'équation polynomiale $(x-3)(x-5)(x-7) = 0$ se développe en $x^3 - 15x^2 + 71x - 105 = 0$.
L'équation polynomiale portant sur $n - x$ se développe quant à elle en :
$-x^3 + (3n-15)x^2 + (-3n^2 + 30n - 71)x + (n^3 - 15n^2 + 71n - 105) = 0$.
Si on remplace n par 8, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8.

Si on remplace n par 10, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

4 Passer d'un degré au degré supérieur

Considérons d'abord les deux premières équations des deux systèmes pour les degrés 4 et 5. On passe de l'équation :

$$x^4 - \sigma_{1,4}x^3 + \sigma_{2,4}x^2 - \sigma_{3,4}x + \sigma_{4,4} = 0$$

à l'équation :

$$x^5 - \sigma_{1,5}x^4 + \sigma_{2,5}x^3 - \sigma_{3,5}x^2 + \sigma_{4,5}x - \sigma_{5,5} = 0$$

Les coefficients de l'équation de degré 5 ont été obtenus ainsi à partir de ceux de l'équation de degré 4.

$$\begin{array}{ll} \sigma_{1,5} = \sigma_{1,4} & +p_5 \\ \sigma_{2,5} = \sigma_{2,4} & +\sigma_{1,4}.p_5 \\ \sigma_{3,5} = \sigma_{3,4} & +\sigma_{2,4}.p_5 \\ \sigma_{4,5} = \sigma_{4,4} & +\sigma_{3,4}.p_5 \\ \sigma_{5,5} = & \sigma_{4,4}.p_5 \end{array}$$

Plus généralement, si p_i désigne le $p^{ième}$ nombre premier impair,

$$\begin{array}{ll} \sigma_{1,i} = \sigma_{1,i-1} & +p_i \\ \sigma_{2,i} = \sigma_{2,i-1} & +\sigma_{1,i-1}.p_i \\ \sigma_{3,i} = \sigma_{3,i-1} & +\sigma_{2,i-1}.p_i \\ \vdots & \\ \sigma_{i-1,i} = \sigma_{i-1,i-1} & +\sigma_{i-2,i-1}.p_i \\ \sigma_{i,i} = & +\sigma_{i-1,i-1}.p_i \end{array}$$

[‡]En annexe, on fournit les équations polynomiales de degré 5 qui permettent laborieusement de trouver les décomposants de Goldbach des nombres 14 et 16 qui ont comme nombres premiers impairs inférieurs à eux les nombres premiers $3, 5, 7, 11$ et 13 (!).

Il faudrait trouver également comment on passe de la deuxième équation du système à deux équations d'un certain degré à la deuxième équation du système de degré immédiatement supérieur.

Peut-être est-ce à cause de ce mécanisme de passage d'un degré au degré immédiatement supérieur que les équations sont toujours résolubles ?...

5 Exprimer les coefficients de la deuxième équation en fonction de ceux de la première

La première équation polynomiale (dont on est sûr qu'elle a des solutions puisqu'elle a comme solution tout nombre premier impair compris entre 3 et n-2) s'écrit :

$$\prod_1^m (x - p_i) = 0 = \sum_0^m a_i x^i.$$

Un polynôme de degré m a $m + 1$ termes d'où le 0 au lieu du 1.

La deuxième équation polynomiale s'écrit :

$$\prod_1^m ((n - x) - p_i) = 0$$

On peut prendre l'opposé, c'est équivalent.

$$\prod_1^m (x - (n - p_i)) = 0 = \sum_0^m b_i x^i.$$

$a_m = 1$.

$b_m = a_m$.

$a_{m-1} = \sum_1^m p_i$.

$b_{m-1} = \sum_1^m (n - p_i) = nm + a_{m-1}$.

$a_{m-2} = \sum_{1 \leq i < j \leq m} p_i p_j$.

$b_{m-2} = \sum_{1 \leq i < j \leq m} (n - p_i)(n - p_j) = \sum_{1 \leq i < j \leq m} (n^2 - (p_i + p_j)n + p_i p_j) = mn^2 - 2a_{m-1}n + a_{m-2}$.

$a_{m-3} = \sum_{1 \leq i < j < k \leq m} p_i p_j p_k$.

$$\begin{aligned} b_{m-3} &= \sum_{1 \leq i < j < k \leq m} (n - p_i)(n - p_j)(n - p_k) \\ &= \sum_{1 \leq i < j < k \leq m} (n^3 - \sigma_1 n^2 + \sigma_2 n - \sigma_3) \quad . \\ &= mn^3 - 3a_{m-1}n^2 + 2a_{m-2}n - a_{m-3} \end{aligned}$$

6 Pgcd de polynomes

Dans la mesure où l'on cherche une racine r qui vérifie et la première et la deuxième équation, le fait que les deux polynômes en question aient un pgcd différent de 1 assurerait l'existence d'une telle racine.

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

Annexe : exemples de degrés 4 et 5

Si on résoud les équations dont on a calculé les coefficients en remplaçant n successivement par les valeurs 12 (équations de degré 4 car il y a 4 nombres premiers impairs inférieurs à 12 qui sont $3, 5, 7$ et 11) puis par les valeurs 14 et 16 pour n (équations polynomiales de degré 5 car on a rajouté le nombre premier impair 13) avec un outil tel que l'outil libre Sage qui permet la résolution d'équations polynomiales, on arrive à résoudre les systèmes ci-dessous.

Pour $n = 12$, il faut résoudre le système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 + (26 - 4n)x^3 + (6n^2 - 78n + 236)x^2 + (-4n^3 + 78n^2 - 472n + 886)x + (n^4 - 26n^3 + 236n^2 - 886n + 1155) = 0 \end{cases}$$

qui se ramène au système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont bien 5 et 7 qui sont bien les décomposants de Goldbach de 12.

Calculons les équations pour le degré 5 (nombres premiers impairs 3, 5, 7, 11 et 13).

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 10725 = 0$$

avec

$$\begin{aligned} &3 + 5 + 7 + 11 + 13 = 39 \\ &3.5 + 3.7 + 3.11 + 3.13 + 5.7 + 5.11 + 5.13 + 7.11 + 7.13 + 11.13 = 574 \\ &3.5.7 + 3.5.11 + 3.5.13 + 3.7.11 + 3.7.13 + 3.11.13 + 5.7.11 + 5.7.13 + 5.11.13 + 7.11.13 = 3954 \\ &3.5.7.11 + 3.5.7.13 + 3.5.11.13 + 3.7.11.13 + 5.7.11.13 = 12673 \\ &3.5.7.11.13 = 15015. \end{aligned}$$

En remplaçant x par $n - x$, on obtient le polynôme suivant dont on cherche quelles valeurs de x l'annulent.

$$\begin{array}{rrrrrrr} & & & & & & -x^5 \\ & & & & +(5n & -39) & x^4 \\ & & & +(-10n^2 & +156n & -574) & x^3 \\ & & +(10n^3 & -234n^2 & +1722n & -3954) & x^2 \\ & +(-5n^4 & +156n^3 & -1722n^2 & +7908n & -12673) & x^1 \\ +(n^5 & -39n^4 & +574n^3 & -3954n^2 & +12673n & -15015) & \end{array}$$

Pour $n = 14$ ou $n = 16$, il faut résoudre le système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + (5n - 39)x^4 + (-10n^2 + 156n - 574)x^3 + (10n^3 - 234n^2 + 1722n - 3954)x^2 + \\ \qquad (-5n^4 + 156n^3 - 1722n^2 + 7908n - 12673)x + (n^5 - 39n^4 + 574n^3 - 3954n^2 + 12673n - 15015) = 0 \end{cases}$$

qui se ramène dans le cas de $n = 14$ au système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont $3, 7$ et 11, qui sont bien les décomposants de Goldbach de 14.

Pour $n = 16$, le système final à résoudre est :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont $3, 5, 11$ et 13, qui sont bien les décomposants de Goldbach de 16.

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p est incongru* à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à n est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$"*. Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale et qui est fournie en annexe.
On réalise à ces lectures que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tous racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5+3.7+3.11+5.7+5.11+7.11.$$
$$886 = 3.5.7+3.5.11+3.7.11+5.7.11.$$
$$1155 = 3.5.7.11.$$

*On utilise le terme proposé par Gauss dans les Recherches Arithmétiques.

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$x^{\pi(n-2)-1} - \sigma_1.x^{\pi(n-2)-2} + \sigma_2.x^{\pi(n-2)-3} - \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

La plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1+(n-1)$ n'est jamais considérée comme une décomposition de Goldbach[†], le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers impairs considérés. Par exemple, $\sigma_1 = p_1 + p_2 + p_3 + p_4 ... = 3 + 5 + 7 + 11 ...$, $\sigma_2 = p_1p_2 + p_1p_3 + ... + p_2p_3 + p_2p_4 + ...$ et le dernier sigma est le produit de tous les nombres premiers impairs inférieurs à $n-2$.

Pour exprimer que $n-x$, le complémentaire du nombre à chercher doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on utilise la même équation polynomiale en remplaçant x par $n-x$; si l'on considère les 4 premiers nombres premiers impairs seulement, l'équation polynomiale devient :

$$((n-x)-3)((n-x)-5)((n-x)-7)((n-x)-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

L'élévation aux différentes puissances du monôme $n-x$ donne les résultats ci-dessous :

$$\begin{array}{l}(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 = n^2 - 2nx + x^2.\end{array}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n-x$ à la puissance i.

Si on développe et qu'on regroupe ensemble les coefficients concernant une même puissance de x, on obtient :

$$x^4+(-4n+26)x^3+(6n^2-78n+236)x^2+(-4n^3+78n^2-472n+886)x+(n^4-26n^3+236n^2-886n+1155) \;=\; 0$$

On reconnaît dans la dernière parenthèse le polynôme initial dans lequel x a été remplacé par n. Puis pour les coefficients des puissances supérieures de x, on voit qu'on dérive successivement le polynôme initial puis les polynômes obtenus, qu'on prend l'opposé du résultat à chaque fois et qu'on divise successivement les résultats intermédiaires par 2, 3, etc.

Pour le degré 4, le polynôme initial est :

$$n^4 - 26n^3 + 236n^2 - 886n + 1155$$

On le dérive et on en prend l'opposé :

$$-4n^3 + 78n^2 - 472n + 886$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 2 :

$$6n^2 - 78n + 236$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 3 :

$$-4n + 26$$

Les coefficients d'expression $\frac{(-1)^n P^{(n)}(x)}{n!}$ sont appelés coefficients du développement de Taylor.

[†]même si Cantor la comptait comme telle.

On est donc systématiquement ramené au système d'équations à deux équations de degré i suivant, dont il faudrait réussir à prouver qu'il admet systématiquement au moins une solution :

$$\begin{cases} P(x) : x^{\pi(n-2)-1} - \sigma_1.x^{\pi(n-2)-2} + \sigma_2.x^{\pi(n-2)-3} - \sigma_3.x^{\pi(n-2)-1} \ldots = 0 \\ \sum_{i=0}^{i=\pi(n-2)-1} \frac{(-1)^i P^{(i)}(n)}{i!} x^i = 0 \end{cases}$$

Les résultats de la théorie de Galois sur la résolubilité des équations polynomiales ne pourraient-ils pas être utilisés ici pour montrer que notre système de deux équations admet toujours une solution en x au moins ?...[‡]

3 Exemples

Traitons les exemples $n = 8$ et $n = 10$. Il n'y a que trois nombres premiers impairs inférieurs à n, 3, 5 *et* 7.
L'équation polynomiale $(x-3)(x-5)(x-7) = 0$ se développe en $x^3 - 15x^2 + 71x - 105 = 0$.
L'équation polynomiale portant sur $n - x$ se développe quant à elle en :
$-x^3 + (3n-15)x^2 + (-3n^2 + 30n - 71)x + (n^3 - 15n^2 + 71n - 105) = 0$.
Si on remplace n par 8, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8.

Si on remplace n par 10, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

4 Passer d'un degré au degré supérieur

Considérons d'abord les deux premières équations des deux systèmes pour les degrés 4 et 5. On passe de l'équation :

$$x^4 - \sigma_{1,4}x^3 + \sigma_{2,4}x^2 - \sigma_{3,4}x + \sigma_{4,4} = 0$$

à l'équation :

$$x^5 - \sigma_{1,5}x^4 + \sigma_{2,5}x^3 - \sigma_{3,5}x^2 + \sigma_{4,5}x - \sigma_{5,5} = 0$$

Les coefficients de l'équation de degré 5 ont été obtenus ainsi à partir de ceux de l'équation de degré 4.

$$\begin{array}{ll} \sigma_{1,5} = \sigma_{1,4} & +p_5 \\ \sigma_{2,5} = \sigma_{2,4} & +\sigma_{1,4}.p_5 \\ \sigma_{3,5} = \sigma_{3,4} & +\sigma_{2,4}.p_5 \\ \sigma_{4,5} = \sigma_{4,4} & +\sigma_{3,4}.p_5 \\ \sigma_{5,5} = & \sigma_{4,4}.p_5 \end{array}$$

Plus généralement, si p_i désigne le $p^{ième}$ nombre premier impair,

$$\begin{array}{ll} \sigma_{1,i} = \sigma_{1,i-1} & +p_i \\ \sigma_{2,i} = \sigma_{2,i-1} & +\sigma_{1,i-1}.p_i \\ \sigma_{3,i} = \sigma_{3,i-1} & +\sigma_{2,i-1}.p_i \\ \vdots & \\ \sigma_{i-1,i} = \sigma_{i-1,i-1} & +\sigma_{i-2,i-1}.p_i \\ \sigma_{i,i} = & +\sigma_{i-1,i-1}.p_i \end{array}$$

[‡]En annexe, on fournit les équations polynomiales de degré 5 qui permettent laborieusement de trouver les décomposants de Goldbach des nombres 14 et 16 qui ont comme nombres premiers impairs inférieurs à eux les nombres premiers $3, 5, 7, 11$ et 13 (!).

Il faudrait trouver également comment on passe de la deuxième équation du système à deux équations d'un certain degré à la deuxième équation du système de degré immédiatement supérieur.

Peut-être est-ce à cause de ce mécanisme de passage d'un degré au degré immédiatement supérieur que les équations sont toujours résolubles ?...

5 Pgcd des polynomes

Dans la mesure où l'on cherche une racine r qui vérifie et la première et la deuxième équation, le fait que les deux polynômes en question aient un pgcd différent de 1 assurerait l'existence d'une telle racine.

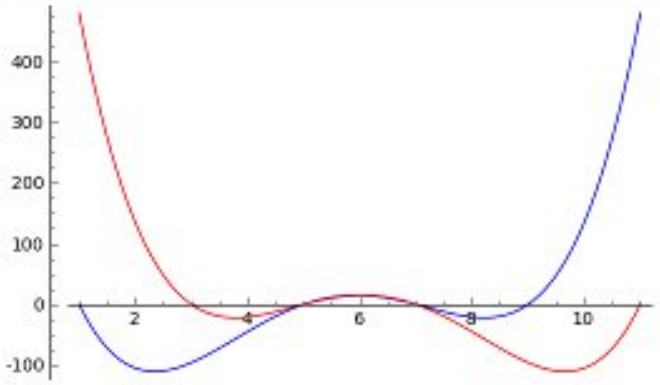
Avec l'outil Sage, on expérimente cette idée à la recherche des décomposants de Goldbach du nombre pair 14.

$$
\begin{aligned}
&Sage : decomp14 = var('x')\\
&Sage : eq1 = x^5 - 39 * x^4 + 574 * x^3 - 3954 * x^2 + 12673 * x - 15015\\
&Sage : eq2 = -x^5 + 31 * x^4 - 350 * x^3 + 1730 * x^2 - 3489 * x + 2079\\
&Sage : eq1.gcd(eq2)\\
&Sage :\ x^3 - 21 * x^2 + 131 * x - 231\\
&Sage : eq4 = x^3 - 21 * x^2 + 131 * x - 231 == 0\\
&Sage : solve([eq4], x)\\
&Sage :\ [x == 7, x == 11, x == 3]
\end{aligned}
$$

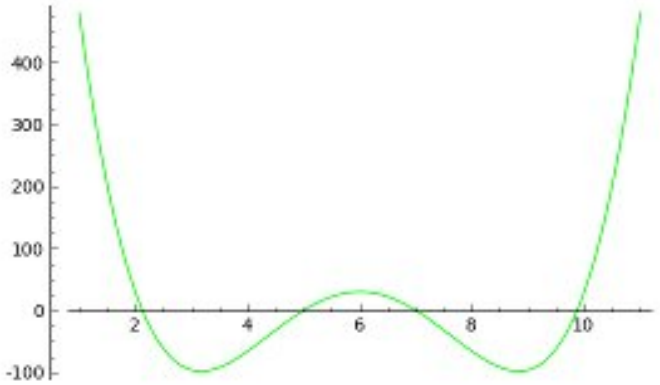
6 Somme des polynômes

Dans la mesure où les deux courbes algébriques sont symétriques l'une de l'autre par rapport à une droite d'ordonnée $n/2$ (puisque $x = n/2 = n - n/2$), on peut voir apparaître directement les décomposants de Goldbach comme racine du polynôme qui est la somme des deux polynômes. On découvre les décomposants de Goldbach sur les visualisations ci-dessous, concernant les nombres pairs 12 et 18. La somme en question est systématiquement une fonction polynomiale paire.

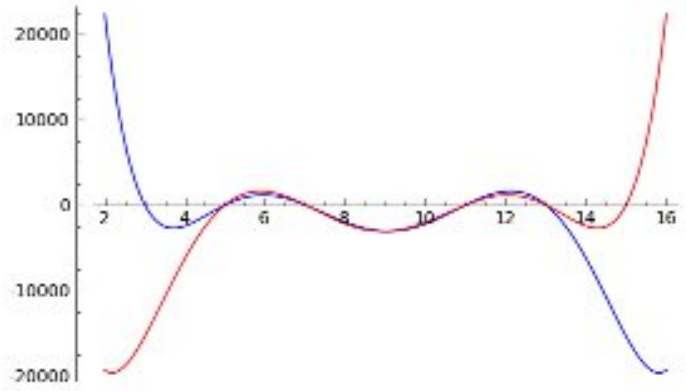
```
f=plot(x^4-22*x^3+164*x^2-458*x+315,(x,1,11),rgbcolor=(0,0,1))
g=plot(x^4-26*x^3+236*x^2-886*x+1155,(x,1,11),rgbcolor=(1,0,0))
show(f+g)
```



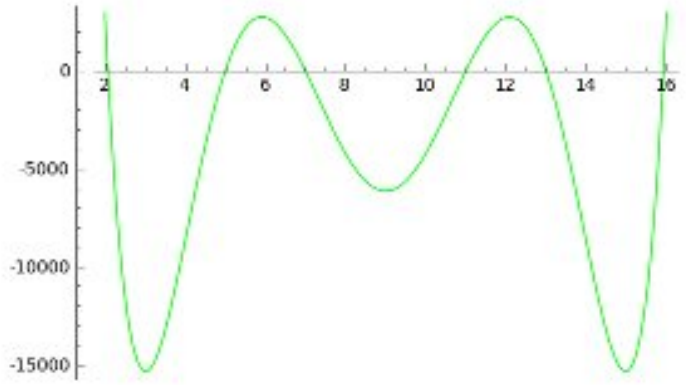

```
h=plot(2*x^4-48*x^3+400*x^2-1344*x+1470,(x,1,11),rgbcolor=(0,1,0))
show(h)
```



```
x=var('decomp18')
f=plot(x^6-56*x^5+1237*x^4-13712*x^3+79891*x^2-230456*x+255255,(x,2,16),rgbcolor=(0,0,1))
g=plot(x^6-52*x^5+1057*x^4-10552*x^3+52891*x^2-118420*x+75075,(x,2,16),rgbcolor=(1,0,0))
show(f+g)
```




```
h=plot(2*x^6-108*x^5+2294*x^4-24264*x^3+132782*x^2-348876*x+330330,(x,2,16),rgbcolor=(0,1,0))
show(h)
```



Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

Annexe : exemples de degrés 4 et 5

Si on résoud les équations dont on a calculé les coefficients en remplaçant n successivement par les valeurs 12 (équations de degré 4 car il y a 4 nombres premiers impairs inférieurs à 12 qui sont $3, 5, 7$ et 11) puis par les valeurs 14 et 16 pour n (équations polynomiales de degré 5 car on a rajouté le nombre premier impair 13) avec un outil tel que l'outil libre Sage qui permet la résolution d'équations polynomiales, on arrive à résoudre les systèmes ci-dessous.

Pour $n = 12$, il faut résoudre le système :

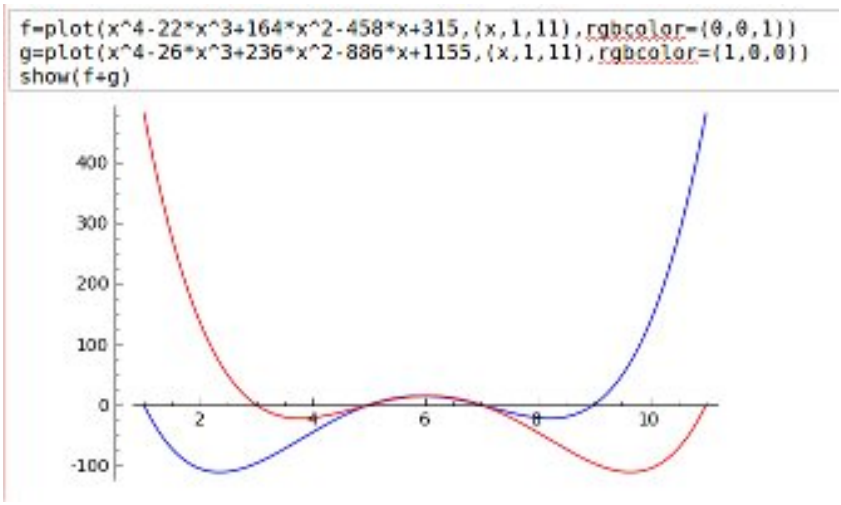
$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 + (26 - 4n)x^3 + (6n^2 - 78n + 236)x^2 + (-4n^3 + 78n^2 - 472n + 886)x + (n^4 - 26n^3 + 236n^2 - 886n + 1155) = 0 \end{cases}$$

qui se ramène au système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont bien 5 et 7 qui sont bien les décomposants de Goldbach de 12.

La visualisation des deux polynômes par l'outil Sage est fournie ci-dessous :



Calculons les équations pour le degré 5 (nombres premiers impairs 3, 5, 7, 11 et 13).

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 10725 = 0$$

avec

$3 + 5 + 7 + 11 + 13 = 39$
$3.5 + 3.7 + 3.11 + 3.13 + 5.7 + 5.11 + 5.13 + 7.11 + 7.13 + 11.13 = 574$
$3.5.7 + 3.5.11 + 3.5.13 + 3.7.11 + 3.7.13 + 3.11.13 + 5.7.11 + 5.7.13 + 5.11.13 + 7.11.13 = 3954$
$3.5.7.11 + 3.5.7.13 + 3.5.11.13 + 3.7.11.13 + 5.7.11.13 = 12673$
$3.5.7.11.13 = 15015.$

En remplaçant x par $n-x$, on obtient le polynôme suivant dont on cherche quelles valeurs de x l'annulent.

$$\begin{array}{rrrrrrr} & & & & & & -x^5 \\ & & & & +(5n & -39) & x^4 \\ & & & +(-10n^2 & +156n & -574) & x^3 \\ & & +(10n^3 & -234n^2 & +1722n & -3954) & x^2 \\ & +(-5n^4 & +156n^3 & -1722n^2 & +7908n & -12673) & x^1 \\ +(n^5 & -39n^4 & +574n^3 & -3954n^2 & +12673n & -15015) & \end{array}$$

Pour $n = 14$ ou $n = 16$, il faut résoudre le système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + (5n-39)x^4 + (-10n^2 + 156n - 574)x^3 + (10n^3 - 234n^2 + 1722n - 3954)x^2 + \\ \qquad (-5n^4 + 156n^3 - 1722n^2 + 7908n - 12673)x + (n^5 - 39n^4 + 574n^3 - 3954n^2 + 12673n - 15015) = 0 \end{cases}$$

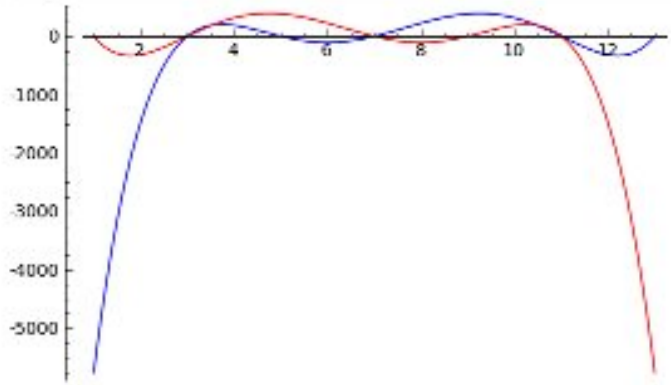
qui se ramène dans le cas de $n = 14$ au système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont $3, 7$ et 11, qui sont bien les décomposants de Goldbach de 14.

La visualisation des deux polynômes par l'outil Sage est fournie ci-dessous :

```
f=plot(x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015,(x,1,13),rgbcolor=(0,0,1))
g=plot(-x^5+31*x^4-350*x^3+1730*x^2-3489*x+2079,(x,1,13),rgbcolor=(1,0,0))
show(f+g)
```



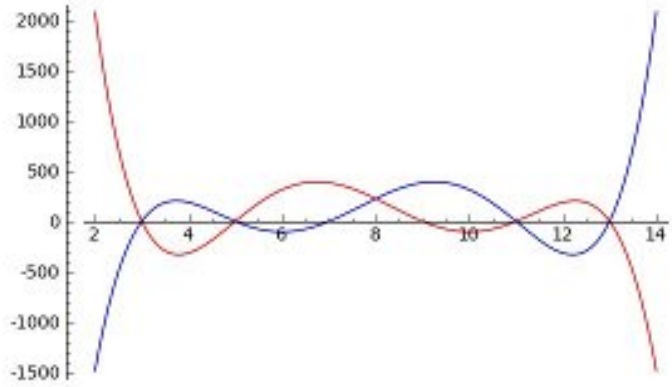
Pour $n = 16$, le système final à résoudre est :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{cases}$$

Le pgcd de ces deux polynômes est $x^4 - 32x^3 + 350x^2 - 1504x + 2145$. Les seules valeurs de x qui conviennent sont $3, 5, 11$ et 13, qui sont bien les décomposants de Goldbach de 16.

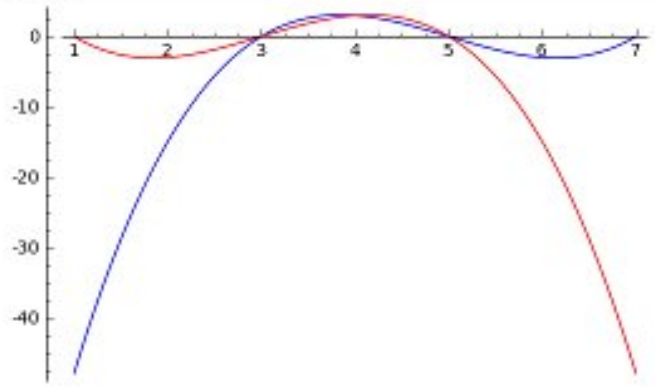
La visualisation des deux polynômes par l'outil Sage est fournie ci-dessous :

```
f=plot(x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015,(x,2,14),rgbcolor=(0,0,1))
g=plot(-x^5+41*x^4-638*x^3+4654*x^2-15681*x+19305,(x,2,14),rgbcolor=(1,0,0))
show(f+g)
```

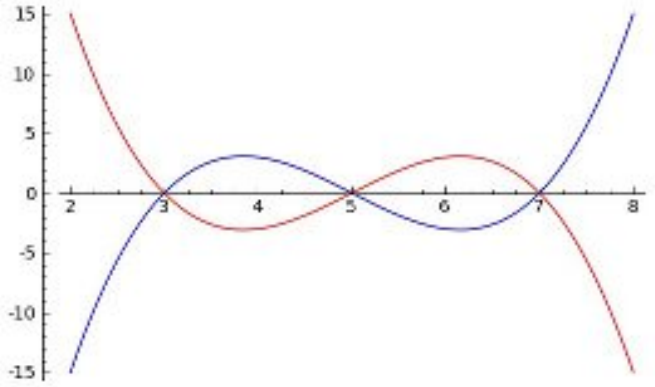


Fournissons enfin les visualisations par l'outil Sage des polynômes permettant de trouver les décomposants de Goldbach des nombres pairs 8, 10 et 18.

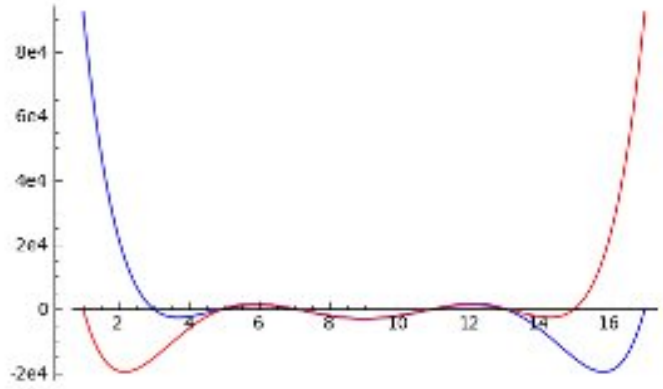
```
f=plot(x^3-15*x^2+71*x-105,(x,1,7),rgbcolor=(0,0,1))
g=plot(-x^3+9*x^2-23*x+15,(x,1,7),rgbcolor=(1,0,0))
show(f+g)
```




```
f=plot(x^3-15*x^2+71*x-105,(x,2,8),rgbcolor=(0,0,1))
g=plot(-x^3+15*x^2-71*x+105,(x,2,8),rgbcolor=(1,0,0))
show(f+g)
```




```
f=plot(x^6-56*x^5+1237*x^4-13712*x^3+79891*x^2-230456*x+255255,(x,1,17),rgbcolor=(0,0,1))
g=plot(x^6-52*x^5+1057*x^4-10552*x^3+52891*x^2-118420*x+75075,(x,1,17),rgbcolor=(1,0,0))
show(f+g)
```



Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p n'est pas congru à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à n est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$"*. Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale. On réalise à ces lectures que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tous racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5+3.7+3.11+5.7+5.11+7.11.$$
$$886 = 3.5.7+3.5.11+3.7.11+5.7.11.$$
$$1155 = 3.5.7.11.$$

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$x^{\pi(n)-1} - \sigma_1.x^{\pi(n)-2} + \sigma_2.x^{\pi(n)-3} - \sigma_3.x^{\pi(n)-1} + \ldots = 0$$

La plus grande puissance de x est $\pi(n) - 1$ où $\pi(n)$ est la notation habituelle pour le nombre de nombres premiers inférieurs à n, le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers impairs considérés. Par exemple, $\sigma_1 = p_1+p_2+p_3+p_4... = 3+5+7+11...$, $\sigma_2 = p_1p_2+p_1p_3+...+p_2p_3+p_2p_4+...$ et le dernier σ est le produit de tous les nombres premiers impairs inférieurs à n.

Pour exprimer que $n - x$, le complémentaire du nombre à chercher doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on utilise la même équation polynomiale en remplaçant x par $n - x$; si l'on considère les 4 premiers nombres premiers impairs seulement, l'équation polynomiale devient :

$$((n-x)-3)((n-x)-5)((n-x)-7)((n-x)-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

L'élévation aux différentes puissances du monôme $n - x$ donne les résultats ci-dessous :

$$\begin{array}{l}(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 = n^2 - 2nx + x^2.\end{array}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n - x$ à la puissance i.

Si on développe et qu'on regroupe ensemble les coefficients concernant une même puissance de x, on obtient :

$$x^4+(-4n+26)x^3+(6n^2-78n+236)x^2+(-4n^3+78n^2-472n+886)x+(n^4-26n^3+236n^2-886n+1155) \;=\; 0$$

On reconnaît dans la dernière parenthèse le polynôme initial dans lequel x a été remplacé par n. Puis pour les coefficients des puissances supérieures de x, on voit qu'on dérive successivement le polynôme initial puis les polynômes obtenus, qu'on prend l'opposé du résultat à chaque fois et qu'on divise successivement les résultats intermédiaires par 2, 3, etc.

Pour le degré 4, le polynôme initial est :

$$n^4 - 26n^3 + 236n^2 - 886n + 1155$$

On le dérive et on en prend l'opposé :

$$-4n^3 + 78n^2 - 472n + 886$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 2 :

$$6n^2 - 78n + 236$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 3 :

$$-4n + 26$$

Les coefficients d'expression $\frac{(-1)^n P^{(n)}(x)}{n!}$ sont appelés coefficients du développement de Taylor.

On est donc systématiquement ramené au système d'équations à deux équations de degré i suivant, dont il faudrait réussir à prouver qu'il admet systématiquement au moins une solution :

$$\begin{cases} P(x) : x^{\pi(n)-1} - \sigma_1.x^{\pi(n)-2} + \sigma_2.x^{\pi(n)-3} - \sigma_3.x^{\pi(n)-1} + \ldots = 0 \\ \sum_{i=0}^{i=\pi(n)-1} \frac{(-1)^i P^{(i)}(n)}{i!} x^i = 0 \end{cases}$$

3 Exemples

Traitons les exemples $n = 8$ et $n = 10$. Il n'y a que trois nombres premiers impairs inférieurs à n, 3, 5 *et* 7.
L'équation polynomiale $(x-3)(x-5)(x-7) = 0$ se développe en $x^3 - 15x^2 + 71x - 105 = 0$.
L'équation polynomiale portant sur $n - x$ se développe quant à elle en :
$-x^3 + (3n-15)x^2 + (-3n^2 + 30n - 71)x + (n^3 - 15n^2 + 71n - 105) = 0$.
Si on remplace n par 8, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8.

Si on remplace n par 10, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

4 Passer d'un degré au degré supérieur

Considérons d'abord les deux premières équations des deux systèmes pour les degrés 4 et 5. On passe de l'équation :

$$x^4 - \sigma_{1,4}x^3 + \sigma_{2,4}x^2 - \sigma_{3,4}x + \sigma_{4,4} = 0$$

à l'équation :

$$x^5 - \sigma_{1,5}x^4 + \sigma_{2,5}x^3 - \sigma_{3,5}x^2 + \sigma_{4,5}x - \sigma_{5,5} = 0$$

Les coefficients de l'équation de degré 5 ont été obtenus ainsi à partir de ceux de l'équation de degré 4.

$$\begin{array}{ll} \sigma_{1,5} = \sigma_{1,4} & +p_5 \\ \sigma_{2,5} = \sigma_{2,4} & +\sigma_{1,4}.p_5 \\ \sigma_{3,5} = \sigma_{3,4} & +\sigma_{2,4}.p_5 \\ \sigma_{4,5} = \sigma_{4,4} & +\sigma_{3,4}.p_5 \\ \sigma_{5,5} = & \sigma_{4,4}.p_5 \end{array}$$

Plus généralement, si p_i désigne le $p^{ième}$ nombre premier impair,

$$\begin{array}{ll} \sigma_{1,i} = \sigma_{1,i-1} & +p_i \\ \sigma_{2,i} = \sigma_{2,i-1} & +\sigma_{1,i-1}.p_i \\ \sigma_{3,i} = \sigma_{3,i-1} & +\sigma_{2,i-1}.p_i \\ \vdots & \\ \sigma_{i-1,i} = \sigma_{i-1,i-1} & +\sigma_{i-2,i-1}.p_i \\ \sigma_{i,i} = & +\sigma_{i-1,i-1}.p_i \end{array}$$

5 Pgcd des polynomes

Dans la mesure où l'on cherche une racine r qui vérifie et la première et la deuxième équation, le fait que les deux polynômes en question aient un pgcd différent de 1 assurerait l'existence d'une telle racine.

Avec l'outil libre Sage, on expérimente cette idée à la recherche des décomposants de Goldbach de 14.

$Sage : decomp14 = var('x')$
$Sage : eq1 = x^5 - 39 * x^4 + 574 * x^3 - 3954 * x^2 + 12673 * x - 15015$
$Sage : eq2 = -x^5 + 31 * x^4 - 350 * x^3 + 1730 * x^2 - 3489 * x + 2079$
$Sage : eq1.gcd(eq2)$
$Sage :\ x^3 - 21 * x^2 + 131 * x - 231$
$Sage : eq4 = x^3 - 21 * x^2 + 131 * x - 231 == 0$
$Sage : solve([eq4], x)$
$Sage :\ [x == 7, x == 11, x == 3]$

En annexe, sont fournis par Sage les polynômes *pgcd* jusqu'au degré 6.

6 Poursuivons

On a bien compris que le coefficient important (directeur en quelque sorte), c'est le deuxième coefficient du second polynôme, car il fournit la somme des complémentaires à n des nombres premiers inférieurs à n et que la somme en question doit être représentable par une partition de $\pi(n) - 1$ entiers impairs compris entre 1 et $n - 3$, cette partition contenant un nombre premier au moins.

Par exemple, pour $n = 14$, le deuxième coefficient du deuxième polynôme est 31. Ce nombre 31 est la somme des complémentaires des nombres premiers impairs inférieurs à 14 que sont $3, 5, 7, 11$ et 13 : $31 = 1 + 3 + 7 + 9 + 11$.

Voyons comment ce 31 est "advenu" par nos coefficients de Taylor successifs.

6.1 Comprenons sur le cas du nombre pair 14

Dans la suite, on n'effectuera pas les calculs, laissant au fur et à mesure apparaître les premiers entiers qui s'élimineront entre eux.

Le premier polynôme à dériver est : $P(x) = x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015$

Il se dérive en : $P'(x) = -5x^4 + (4 \times 39)x^3 - (3 \times 574)x^2 + (2 \times 3954)x - 12673$

Puis,

$$\frac{P''(x)}{2} = \left(\frac{5 \times 4}{2}\right) x^3 - \left(\frac{3 \times 4 \times 39}{2}\right) x^2 + \left(\frac{2 \times 3 \times 574}{2}\right) x + \left(\frac{2 \times 3954}{2}\right)$$

Encore,

$$\frac{P'''(x)}{2 \times 3} = -\left(\frac{3 \times 4 \times 5}{2 \times 3}\right) x^2 + \left(\frac{2 \times 3 \times 4 \times 39}{2 \times 3}\right) x + \left(\frac{2 \times 3 \times 574}{2 \times 3}\right)$$

Enfin,

$$\frac{P''''(x)}{2 \times 3 \times 4} = \left(\frac{2 \times 3 \times 4 \times 5}{2 \times 3 \times 4}\right) x - \left(\frac{2 \times 3 \times 4 \times 39}{2 \times 3 \times 4}\right)$$

Si l'on ne se préoccupe que de la plus haute puissance de x, on a :

$$x^5 \to -5x^4 \to \left(\frac{4 \times 5}{2}\right) x^3 \to -\left(\frac{3 \times 4 \times 5}{2 \times 3}\right) x^2 \to \left(\frac{2 \times 3 \times 4 \times 5}{2 \times 3 \times 4}\right) x$$

Remplaçons x par 14 dans la dernière expression, ce qui nous donne $5 \times 14 = 70$.

Soustrayons de 70 le σ_1 du premier polynôme $39 = 3 + 5 + 7 + 11 + 13$, on obtient 31.
Ce nombre 31 est une somme d'impairs compris entre 1 et $n - 3 = 11$. En l'occurrence, 31 est la somme $1 + 3 + 7 + 9 + 11$. Il y a plusieurs nombres premiers dans cette somme qui sont autant de décomposants de Goldbach de 14.

6.2 Réappliquons pour le nombre pair 16

Réappliquons la méthode pour le nombre pair 16. Soustrayons de $16 \times 5 = 80$ le même nombre 39 somme des premiers impairs inférieurs à 16. On obtient 41, une somme d'impairs compris entre 1 et 13. La somme en question est $13 + 11 + 9 + 5 + 3$ qui contient les décomposants de Goldbach de 16.

6.3 Résumons avec 18

Notons $\sigma_1(n)$ la somme des nombres premiers impairs inférieurs à $n-1$. En réexpérimentant une dernière fois pour 18, on comprend que prouver la conjecture de Goldbach consiste à prouver que le nombre $n(\pi(n)-1) - \sigma_1(n)$ peut toujours être partitionné en une somme de $\pi(n) - 1$ nombres impairs compris entre 1 et $n-3$ avec l'un des nombres de la partition en question qui est un nombre premier, et de fait un décomposant de Goldbach de n.

7 Démonstration par récurrence

On fournit ici ce qui se passe pour les premiers nombres pairs à des fins pédagogiques.

n	*décomp. de la forme* p+q *avec* p *premier impair*	m ($2^{ème}$ *coeff. du* $2^{ème}$ *polynôme*)	$f(n) = (\pi(n)-1)n - \sigma_1(n)$
6	$3+3, 5+1$	$1+3=4$	$2\times 6 - 8 = 4$
8	$3+5, 5+3, 7+1$	$1+3+5=9$	$3\times 8 - 15 = 9$
10	$3+7, 5+5, 7+3$	$3+5+7=15$	$3\times 10 - 15 = 15$
12	$3+9, 5+7, 7+5, 11+1$	$1+5+7+9=22$	$4\times 12 - 26 = 22$
14	$3+11, 5+9, 7+7, 11+3, 13+1$	$1+3+7+9+11=31$	$5\times 14 - 39 = 31$
16	$3+13, 5+11, 7+9, 11+5, 13+3$	$3+5+9+11+13=41$	$5\times 16 - 39 = 41$
18	$3+15, 5+13, 7+11, 11+7, 13+5, 17+1$	$1+5+7+11+13+15$	$6\times 18 - 56 = 52$
20	$3+17, 5+15, 7+13, 11+9, 13+7, 17+3, 19+1$	$1+3+7+9+13+15+17=65$	$7\times 20 - 75 = 65$
22	$3+19, 5+17, 7+15, 11+11, 13+9, 17+5, 19+3$	$3+5+9+11+15+17+19=79$	$7\times 22 - 75 = 79$
...	...	...	...

On rappelle que $f(n) = \sum_1^{\pi(n)-1} k_i$ est la somme des nombres impairs k_i tels que $n = p_i + k_i$ avec p_i un nombre premier impair compris entre 3 et n.

On voit par le calcul ci-dessous que la différence séparant deux nombres $f(n)$ à partitionner successifs vaut $2(\pi(n)-1)$ si $n-1$ n'est pas un nombre premier et $2\pi(n)-1$ si $n-1$ est un nombre premier.

S'il n'y a pas de nombre premier entre n et $n+2$,

$$\begin{aligned}
\pi(n+2) &= \pi(n)\\
\sigma_1(n+2) &= \sigma_1(n)\\
f(n+2) &= (\pi(n+2)-1)(n+2) - \sigma_1(n+2)\\
&= \pi(n)(n+2) - (n+2) - \sigma_1(n)\\
&= \pi(n)n + 2\pi(n) - (n+2) - \sigma_1(n)\\
f(n) &= (\pi(n)-1)n - \sigma_1(n)\\
f(n+2) - f(n) &= [\pi(n)n - \sigma_1(n) + 2\pi(n) - (n+2)] - [\pi(n)n - n - \sigma_1(n)]\\
&= 2\pi(n) - 2\\
&= 2(\pi(n)-1)
\end{aligned}$$

S'il y a un nombre premier entre n et $n+2$, qui n'est autre que $n+1$,

$$\begin{array}{ll}
\pi(n+2) & = \pi(n)+1. \\
\sigma_1(n+2) & = \sigma_1(n)+p_{\pi(n)-1} \\
 & = \sigma_1(n)+n+1. \\
f(n+2) & = (\pi(n+2)-1)(n+2)-\sigma_1(n+2) \\
 & = \pi(n)(n+2)-\sigma_1(n)-n-1 \\
 & = \pi(n)n-\sigma_1(n)+2\pi(n)-n-1. \\
f(n) & = (\pi(n)-1)n-\sigma_1(n) \\
 & = \pi(n)n-n-\sigma_1(n) \\
f(n+2)-f(n) & = [\pi(n)n+2\pi(n)-\sigma_1(n)-n-1]-[\pi(n)n-n-\sigma_1(n)] \\
 & = 2\pi(n)-1
\end{array}$$

On va démontrer par récurrence que s'il existe une partition du coefficient $f(n)$ associé à n en $d=\pi(n)-1$ nombres impairs différents dont l'un est un nombre premier, alors il existe une partition du coefficient $f(n+2)$ associé à $n'=n+2$ en $d'=\pi(n')-1=\pi(n+2)-1$ nombres impairs différents dont l'un est un nombre premier :
- *initialisation de la récurrence* : il existe une partition du nombre 4 en 2 nombres impairs dont l'un des deux est premier ;
- *passage du nombre pair n au nombre pair suivant $n+2$:* supposons la conjecture de Goldbach vérifiée jusqu'à n, il existe une partition de $(\pi(n)-1)n-\sigma_1(n)$ en $\pi(n)-1$ nombres impairs différents dont l'un au moins est premier.
Ecrivons la partition de $f(n)$: $f(n)=\alpha_1+\alpha_2+\ldots+\alpha_{\pi(n)-1}$ dans laquelle les α_i sont indifféremment des nombres impairs premiers ou composés.
Pour trouver $f(n+2)$ le nombre à partitionner correspondant à $n+2$, on a vu qu'il faut distinguer deux cas :

- soit $n+1$ n'est pas premier ; pour obtenir $f(n+2)$, on doit alors ajouter à $f(n)$ le nombre $2(\pi(n)-1)$. On peut écrire :

  $$f(n+2)=f(n)+2(\pi(n)-1)=\alpha_1+\alpha_2+\ldots+\alpha_{\pi(n)-1}+q_1+q_2$$

  avec q_1 et q_2 deux nombres premiers impairs, puisque la conjecture de Goldbach est en particulier vérifiée pour le nombre pair $2(\pi(n)-1)$ car il est inférieur à n (de l'ordre de $\frac{n}{ln(n)}$ selon le théorème des nombres premiers d'Hadamard)*.
  Mais on peut aussi écrire :

  $$f(n+2)=change(f(n))=(\alpha_1+2)+(\alpha_2+2)+\ldots+(\alpha_{\pi(n)-1}+2)$$

  ~~On a ajouté 2 sommants à la partition de $f(n)$: q_1 et q_2. Or la partition de $f(n+2)$ doit contenir autant de sommants que celle de $f(n)$. Il faut éliminer deux signes +. L'élimination des deux signes + doit se faire en regroupant 3 nombres en un seul, pour préserver l'imparité des sommants de la partition. Ce regroupement de 3 nombres de la partition de $f(n)$ ne peut faire disparaître simultanément les 3 nombres premiers impairs qui étaient présents (p_1, q_1 et q_2) dans la partition de $f(n)$. Il reste un nombre premier au moins dans la partition de $f(n+2)$ qui est un décomposant de Goldbach de $n+2$.~~

- soit $n+1$ est premier ; on doit alors ajouter à $f(n)$ le nombre $2\pi(n)-1$. On peut écrire :

  $$f(n+2)=f(n)+2\pi(n)-1=\alpha_1+\alpha_2+\ldots+\alpha_{\pi(n)-1}+q_1+q_2+(-1)$$

  avec p_1, q_1 et q_2 trois nombres premiers impairs, puisque la conjecture de Goldbach est en particulier vérifiée pour le nombre pair $2\pi(n)$ car il est inférieur à n (de l'ordre de $\frac{n}{ln(n)}$ selon le théorème des nombres premiers d'Hadamard), et les α_i des nombres impairs indifféremment premiers ou composés.
  Mais on peut aussi écrire :

  $$f(n+2)=change(f(n))=1+(\alpha_1+2)+(\alpha_2+2)+\ldots+(\alpha_{\pi(n)-1}+2)$$

*1 appartient à la partition de $f(n)$ tandis qu'il n'appartient pas à celle de $f(n+2)$ et les deux partitions de $f(n)$ et $f(n+2)$ ont en commun les deux plus grands nombres de la partition de $f(n)$.

~~On a ajouté 3 sommants à la partition de $f(n)$: q_1, q_2 et -1. Or la partition de $f(n+2)$ contient seulement un sommant de plus que celle de $f(n)$. Il faut éliminer là-encore deux signes $+$. Le nombre -1 doit forcément faire partie d'un regroupement de 3 nombres car d'une part, il doit disparaître dans la mesure où la partition de $f(n+2)$ ne doit contenir que des nombres impairs positifs, et d'autre part, il est nécessaire de le regrouper avec 2 autres nombres impairs pour que la somme obtenue soit comme tous les autres sommants un nombre impair positif. Le regroupement de -1 avec deux autres nombres de la partition de $f(n)$ ne peut faire disparaître simultanément les 3 nombres premiers qui étaient présents (p_1, q_1 et q_2). Il reste un nombre premier au moins dans la partition de $f(n+2)$ qui est un décomposant de Goldbach de $n+2$.~~

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

[3], **Léonard Euler**, *Démonstration sur le nombre de points où deux lignes des ordres quelconques peuvent se couper*, Mémoires de l'Académie des Sciences et belles lettres de Berlin [4], Berlin, 1750, p.234-248.

[4], **Léonard Euler**, *Nouvelle méthode d'éliminer les quantités inconnues des équations*, Mémoires de l'Académie des Sciences et belles lettres de Berlin [20], Berlin, 1764, p.91-104.

Annexe 1 : exemples des degrés 2 à 6

Si on résoud les équations dont on a calculé les coefficients en remplaçant n successivement par les valeurs 12 (équations de degré 4 car il y a 4 nombres premiers impairs inférieurs à 12 qui sont $3, 5, 7$ et 11) puis par les valeurs 14 et 16 pour n (équations polynomiales de degré 5 car on a rajouté le nombre premier impair 13), et enfin 18 (degré 6) avec un outil tel que l'outil libre Sage qui permet la résolution d'équations polynomiales, on arrive à résoudre les systèmes ci-dessous.

Pour $n = 12$, il faut résoudre le système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 + (26-4n)x^3 + (6n^2 - 78n + 236)x^2 + (-4n^3 + 78n^2 - 472n + 886)x + (n^4 - 26n^3 + 236n^2 - 886n + 1155) = 0 \end{cases}$$

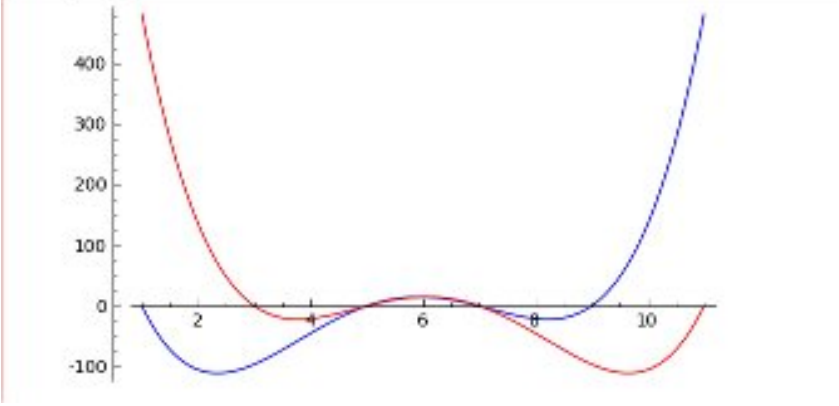
qui se ramène au système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont bien 5 et 7 qui sont bien les décomposants de Goldbach de 12.

La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :

```
f=plot(x^4-22*x^3+164*x^2-458*x+315,(x,1,11),rgbcolor=(0,0,1))
g=plot(x^4-26*x^3+236*x^2-886*x+1155,(x,1,11),rgbcolor=(1,0,0))
show(f+g)
```



Calculons les équations pour le degré 5 (nombres premiers impairs 3, 5, 7, 11 et 13).

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 10725 = 0$$

avec

$3 + 5 + 7 + 11 + 13 = 39$
$3.5 + 3.7 + 3.11 + 3.13 + 5.7 + 5.11 + 5.13 + 7.11 + 7.13 + 11.13 = 574$
$3.5.7 + 3.5.11 + 3.5.13 + 3.7.11 + 3.7.13 + 3.11.13 + 5.7.11 + 5.7.13 + 5.11.13 + 7.11.13 = 3954$
$3.5.7.11 + 3.5.7.13 + 3.5.11.13 + 3.7.11.13 + 5.7.11.13 = 12673$
$3.5.7.11.13 = 15015.$

En remplaçant x par $n-x$, on obtient le polynôme suivant dont on cherche quelles valeurs de x l'annulent.

$$\begin{array}{rrrrrrr}
 & & & & & & -x^5 \\
 & & & & +(5n & -39) & x^4 \\
 & & & +(-10n^2 & +156n & -574) & x^3 \\
 & & +(10n^3 & -234n^2 & +1722n & -3954) & x^2 \\
 & +(-5n^4 & +156n^3 & -1722n^2 & +7908n & -12673) & x^1 \\
+(n^5 & -39n^4 & +574n^3 & -3954n^2 & +12673n & -15015) &
\end{array}$$

Pour $n = 14$ ou $n = 16$, il faut résoudre le système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + (5n - 39)x^4 + (-10n^2 + 156n - 574)x^3 + (10n^3 - 234n^2 + 1722n - 3954)x^2 + \\ \qquad (-5n^4 + 156n^3 - 1722n^2 + 7908n - 12673)x + (n^5 - 39n^4 + 574n^3 - 3954n^2 + 12673n - 15015) = 0 \end{cases}$$

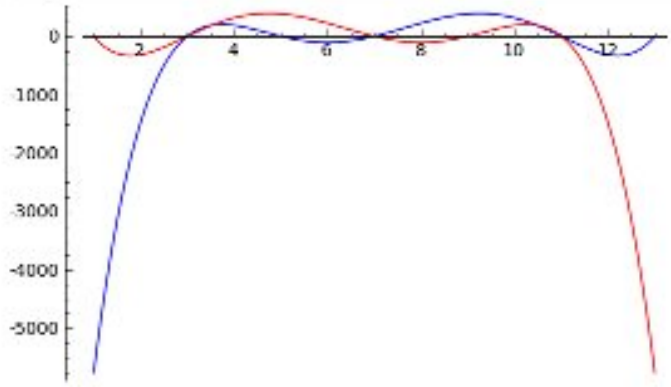
qui se ramène dans le cas de $n = 14$ au système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont $3, 7$ et 11, qui sont bien les décomposants de Goldbach de 14.

La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :

```
f=plot(x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015,(x,1,13),rgbcolor=(0,0,1))
g=plot(-x^5+31*x^4-350*x^3+1730*x^2-3489*x+2079,(x,1,13),rgbcolor=(1,0,0))
show(f+g)
```



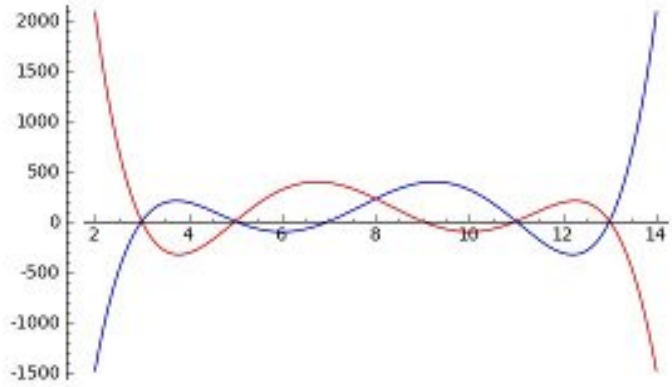
Pour $n = 16$, le système final à résoudre est :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{cases}$$

Le pgcd de ces deux polynômes est $x^4 - 32x^3 + 350x^2 - 1504x + 2145$. Les seules valeurs de x qui conviennent sont $3, 5, 11$ et 13, qui sont bien les décomposants de Goldbach de 16.

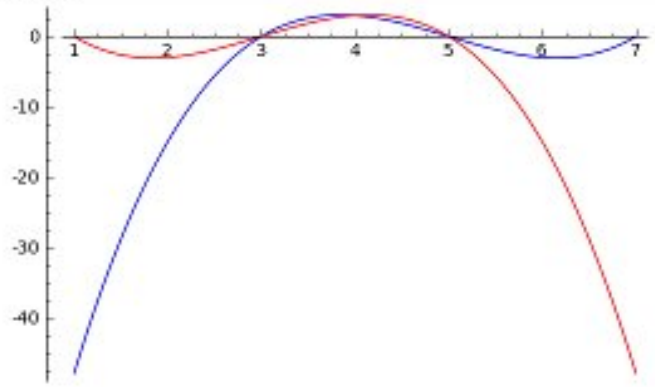
La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :

```
f=plot(x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015,(x,2,14),rgbcolor=(0,0,1))
g=plot(-x^5+41*x^4-638*x^3+4654*x^2-15681*x+19305,(x,2,14),rgbcolor=(1,0,0))
show(f+g)
```

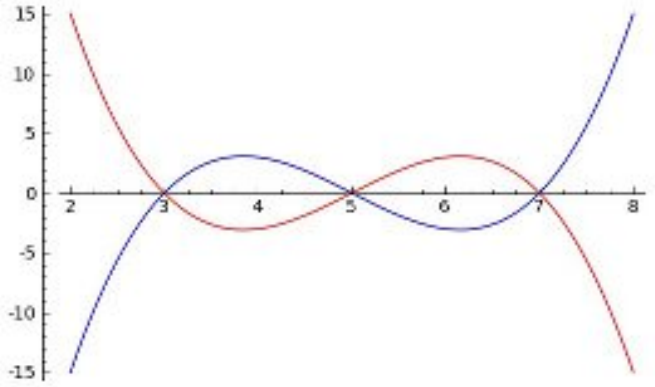


Fournissons enfin les visualisations par l'outil libre Sage des polynômes permettant de trouver les décomposants de Goldbach des nombres pairs 6, 8, 10 et 18.

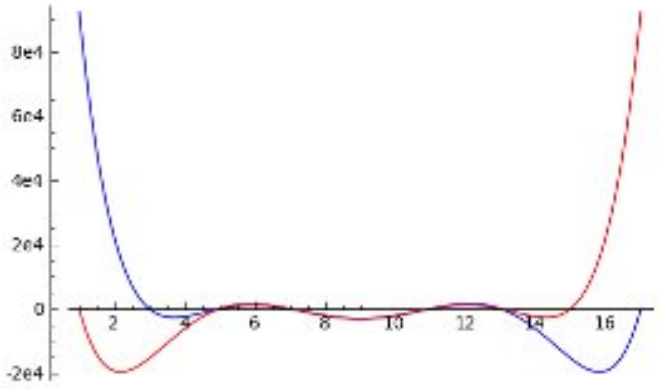
```
f=plot(x^3-15*x^2+71*x-105,(x,1,7),rgbcolor=(0,0,1))
g=plot(-x^3+9*x^2-23*x+15,(x,1,7),rgbcolor=(1,0,0))
show(f+g)
```




```
f=plot(x^3-15*x^2+71*x-105,(x,2,8),rgbcolor=(0,0,1))
g=plot(-x^3+15*x^2-71*x+105,(x,2,8),rgbcolor=(1,0,0))
show(f+g)
```




```
f=plot(x^6-56*x^5+1237*x^4-13712*x^3+79891*x^2-230456*x+255255,(x,1,17),rgbcolor=(0,0,1))
g=plot(x^6-52*x^5+1057*x^4-10552*x^3+52891*x^2-118420*x+75075,(x,1,17),rgbcolor=(1,0,0))
show(f+g)
```



Ci-dessous la copie d'écran du calcul des *pgcd* par Sage (on rappelle que les racines du *pgcd* des deux polynômes de variable x et $n-x$ sont les décomposants de Goldbach de n) :

```
p=x^2-8*x+15
q=p.substitute(x=6-x).expand()
q.gcd(p)
```

```
x - 3
```

```
p=x^3-15*x^2+71*x-105
q=p.substitute(x=8-x).expand()
q.gcd(p)
```

```
x^2 - 8*x + 15
```

```
p=x^3-15*x^2+71*x-105
q=p.substitute(x=10-x).expand()
q.gcd(p)
```

```
x^3 - 15*x^2 + 71*x - 105
```

```
p=x^4-22*x^3+164*x^2-458*x+315
q=p.substitute(x=12-x).expand()
q.gcd(p)
```

```
x^2 - 12*x + 35
```

```
p=x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015
q=p.substitute(x=14-x).expand()
q.gcd(p)
```

```
x^3 - 21*x^2 + 131*x - 231
```

```
p=x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015
q=p.substitute(x=16-x).expand()
q.gcd(p)
```

```
x^4 - 32*x^3 + 350*x^2 - 1504*x + 2145
```

```
p=x^6-56*x^5+1237*x^4-13712*x^3+79891*x^2-230456*x+255255
q=p.substitute(x=18-x).expand()
q.gcd(p)
```

```
x^4 - 36*x^3 + 466*x^2 - 2556*x + 5005
```

Annexe 2 : complémentaires des nombres premiers impairs inférieurs à n pour n compris entre 8 et 100

Il faut démontrer le théorème suivant : *"Si la suite $i_1, i_2, \ldots, i_{\pi(n)-1}$ de $\pi(n)-1$ nombres impairs différents, compris entre 1 et $n-3$ contient un nombre premier alors la suite $i_1+2, i_2+2, \ldots, i_k+2$ contient elle-aussi un nombre premier.*

Le nombre d'impairs compris entre 1 et $n-3$ est $\frac{n-2}{2}$.

$n =$ 8
$\pi(n) - 1 =$ 3
nombre d'impairs compris entre 1 *et* n-3 : 3
$p(f(n)) =$ $1 + 3 + 5$
$f(n) =$ 9

$n =$ 10
$\pi(n) - 1 =$ 3
nombre d'impairs compris entre 1 *et* n-3 : 4
$p(f(n)) =$ $3 + 5 + 7$
$f(n) =$ 15

$n =$ 12
$\pi(n) - 1 =$ 4
nombre d'impairs compris entre 1 *et* n-3 : 5
$p(f(n)) =$ $1 + 5 + 7 + 9$
$f(n) =$ 22

$n =$ 14
$\pi(n) - 1 =$ 5
nombre d'impairs compris entre 1 *et* n-3 : 6
$p(f(n)) =$ $1 + 3 + 7 + 9 + 11$
$f(n) =$ 31

$n =$ 16
$\pi(n) - 1 =$ 5
nombre d'impairs compris entre 1 *et* n-3 : 7
$p(f(n)) =$ $3 + 5 + 9 + 11 + 13$
$f(n) =$ 41

$n =$ 18
$\pi(n) - 1 =$ 6
nombre d'impairs compris entre 1 *et* n-3 : 8
$p(f(n)) =$ $1 + 5 + 7 + 11 + 13 + 15$
$f(n) =$ 52

$n =$ 20
$\pi(n) - 1 =$ 7
nombre d'impairs compris entre 1 *et* n-3 : 9
$p(f(n)) =$ $1 + 3 + 7 + 9 + 13 + 15 + 17$
$f(n) =$ 65

$n =$ 22
$\pi(n) - 1 =$ 7
nombre d'impairs compris entre 1 *et* n-3 : 10
$p(f(n)) =$ $3 + 5 + 9 + 11 + 15 + 17 + 19$
$f(n) =$ 79

$n =$ 24
$\pi(n) - 1 =$ 8
nombre d'impairs compris entre 1 *et* n-3 : 11
$p(f(n)) =$ $1 + 5 + 7 + 11 + 13 + 17 + 19 + 21$
$f(n) =$ 94

$n =$ 26
$\pi(n) - 1 =$ 8
nombre d'impairs compris entre 1 *et* n-3 : 12
$p(f(n)) =$ $3 + 7 + 9 + 13 + 15 + 19 + 21 + 23$
$f(n) =$ 110

$n =$ 28
$\pi(n) - 1 =$ 8
nombre d'impairs compris entre 1 *et* n-3 : 13
$p(f(n)) =$ $5 + 9 + 11 + 15 + 17 + 21 + 23 + 25$
$f(n) =$ 126

$n =$ 30
$\pi(n) - 1 =$ 9
nombre d'impairs compris entre 1 *et* n-3 : 14
$p(f(n)) =$ $1 + 7 + 11 + 13 + 17 + 19 + 23 + 25 + 27$
$f(n) =$ 143

$n =$ 32
$\pi(n) - 1 =$ 10
nombre d'impairs compris entre 1 *et* n-3 : 15
$p(f(n)) =$ $1 + 3 + 9 + 13 + 15 + 19 + 21 + 25 + 27 + 29$
$f(n) =$ 162

$n =$ 34
$\pi(n) - 1 =$ 10
nombre d'impairs compris entre 1 *et* n-3 : 16
$p(f(n)) =$ $3 + 5 + 11 + 15 + 17 + 21 + 23 + 27 + 29 + 31$
$f(n) =$ 182

$n =$ 36
$\pi(n) - 1 =$ 10
nombre d'impairs compris entre 1 *et* n-3 : 17
$p(f(n)) =$ $5 + 7 + 13 + 17 + 19 + 23 + 25 + 29 + 31 + 33$
$f(n) =$ 202

$n =$ 38
$\pi(n) - 1 =$ 11
nombre d'impairs compris entre 1 *et* n-3 : 18
$p(f(n)) =$ $1 + 7 + 9 + 15 + 19 + 21 + 25 + 27 + 31 + 33 + 35$
$f(n) =$ 223

$n =$ 40
$\pi(n) - 1 =$ 11
nombre d'impairs compris entre 1 *et* n-3 : 19
$p(f(n)) =$ $3 + 9 + 11 + 17 + 21 + 23 + 27 + 29 + 33 + 35 + 37$
$f(n) =$ 245

$n =$ 42
$\pi(n) - 1 =$ 12
nombre d'impairs compris entre 1 *et* n-3 : 20
$p(f(n)) =$ $1 + 5 + 11 + 13 + 19 + 23 + 25 + 29 + 31 + 35 + 37 + 39$
$f(n) =$ 268

$n =$ 44
$\pi(n) - 1 =$ 13
nombre d'impairs compris entre 1 *et* n-3 : 21
$p(f(n)) =$ $1 + 3 + 7 + 13 + 15 + 21 + 25 + 27 + 31 + 33 + 37 + 39 + 41$
$f(n) =$ 293

$n =$ 46
$\pi(n) - 1 =$ 13
nombre d'impairs compris entre 1 *et* n-3 : 22
$p(f(n)) =$ $3 + 5 + 9 + 15 + 17 + 23 + 27 + 29 + 33 + 35 + 39 + 41 + 43$
$f(n) =$ 319

$n =$ 48
$\pi(n) - 1 =$ 14
nombre d'impairs compris entre 1 *et* n-3 : 23
$p(f(n)) =$ $1 + 5 + 7 + 11 + 17 + 19 + 25 + 29 + 31 + 35 + 37 + 41 + 43 + 45$
$f(n) =$ 346

$n =$ 50
$\pi(n) - 1 =$ 14
nombre d'impairs compris entre 1 *et* n-3 : 24
$p(f(n)) =$ $3 + 7 + 9 + 13 + 19 + 21 + 27 + 31 + 33 + 37 + 39 + 43 + 45 + 47$
$f(n) =$ 374

$n =$ 52
$\pi(n) - 1 =$ 14
nombre d'impairs compris entre 1 *et* n-3 : 25
$p(f(n)) =$ $5 + 9 + 11 + 15 + 21 + 23 + 29 + 33 + 35 + 39 + 41 + 45 + 47 + 49$
$f(n) =$ 402

$n =$ 54
$\pi(n) - 1 =$ 15
nombre d'impairs compris entre 1 *et* n-3 : 26
$p(f(n)) =$ $1 + 7 + 11 + 13 + 17 + 23 + 25 + 31 + 35 + 37 + 41 + 43 + 47 + 49 + 51$
$f(n) =$ 431

$n =$ 56
$\pi(n) - 1 =$ 15
nombre d'impairs compris entre 1 *et* n-3 : 27
$p(f(n)) =$ $3 + 9 + 13 + 15 + 19 + 25 + 27 + 33 + 37 + 39 + 43 + 45 + 49 + 51 + 53$
$f(n) =$ 461

$n =$ 58
$\pi(n) - 1 =$ 15
nombre d'impairs compris entre 1 *et* n-3 : 28
$p(f(n)) =$ $5 + 11 + 15 + 17 + 21 + 27 + 29 + 35 + 39 + 41 + 45 + 47 + 51 + 53 + 55$
$f(n) =$ 491

$n =$ 60
$\pi(n) - 1 =$ 16
nombre d'impairs compris entre 1 *et* n-3 : 29
$p(f(n)) =$ $1 + 7 + 13 + 17 + 19 + 23 + 29 + 31 + 37 + 41 + 43 + 47 + 49 + 53 + 55$
$+57$
$f(n) =$ 522

$n =$ 62
$\pi(n) - 1 =$ 17
nombre d'impairs compris entre 1 *et* n-3 : 30
$p(f(n)) =$ $1 + 3 + 9 + 15 + 19 + 21 + 25 + 31 + 33 + 39 + 43 + 45 + 49 + 51 + 55$
$+57 + 59$
$f(n) =$ 555

$n =$ 64
$\pi(n) - 1 =$ 17
nombre d'impairs compris entre 1 *et* n-3 : 31
$p(f(n)) =$ $3 + 5 + 11 + 17 + 21 + 23 + 27 + 33 + 35 + 41 + 45 + 47 + 51 + 53$
$+57 + 59 + 61$
$f(n) =$ 589

$n =$ 66
$\pi(n) - 1 =$ 17
nombre d'impairs compris entre 1 *et* n-3 : 32
$p(f(n)) =$ $5 + 7 + 13 + 19 + 23 + 25 + 29 + 35 + 37 + 43 + 47 + 49 + 53 + 55$
$+59 + 61 + 63$
$f(n) =$ 623

$n =$ 68
$\pi(n) - 1 =$ 18
nombre d'impairs compris entre 1 *et* n-3 : 33
$p(f(n)) =$ $1 + 7 + 9 + 15 + 21 + 25 + 27 + 31 + 37 + 39 + 45 + 49 + 51 + 55$
$+57 + 61 + 63 + 65$
$f(n) =$ 658

$n =$ 70
$\pi(n) - 1 =$ 18
nombre d'impairs compris entre 1 *et* n-3 : 34
$p(f(n)) =$ $3 + 9 + 11 + 17 + 23 + 27 + 29 + 33 + 39 + 41 + 47 + 51 + 53 + 57$
$+59 + 63 + 65 + 67$
$f(n) =$ 694

$n =$ 72
$\pi(n) - 1 =$ 19
nombre d'impairs compris entre 1 *et* n-3 : 35
$p(f(n)) =$ $1 + 5 + 11 + 13 + 19 + 25 + 29 + 31 + 35 + 41 + 43 + 49 + 53 + 55$
$+59 + 61 + 65 + 67 + 69$
$f(n) =$ 731

$n =$ 74
$\pi(n) - 1 =$ 20
nombre d'impairs compris entre 1 *et* n-3 : 36
$p(f(n)) =$ $1 + 3 + 7 + 13 + 15 + 21 + 27 + 31 + 33 + 37 + 43 + 45 + 51 + 55$
$+57 + 61 + 63 + 67 + 69 + 71$
$f(n) =$ 770

$n =$ 76
$\pi(n) - 1 =$ 20
nombre d'impairs compris entre 1 *et* n-3 : 37
$p(f(n)) =$ $3 + 5 + 9 + 15 + 17 + 23 + 29 + 33 + 35 + 39 + 45 + 47 + 53 + 57$
$+59 + 63 + 65 + 69 + 71 + 73$
$f(n) =$ 810

$n =$ 78
$\pi(n) - 1 =$ 20
nombre d'impairs compris entre 1 *et* n-3 : 38
$p(f(n)) =$ $5 + 7 + 11 + 17 + 19 + 25 + 31 + 35 + 37 + 41 + 47 + 49 + 55 + 59$
$+61 + 65 + 67 + 71 + 73 + 75$
$f(n) =$ 850

$n =$ 80
$\pi(n) - 1 =$ 21
nombre d'impairs compris entre 1 *et* n-3 : 39
$p(f(n)) =$ $1 + 7 + 9 + 13 + 19 + 21 + 27 + 33 + 37 + 39 + 43 + 49 + 51 + 57$
$+61 + 63 + 67 + 69 + 73 + 75 + 77$
$f(n) =$ 891

$n =$ 82
$\pi(n) - 1 =$ 21
nombre d'impairs compris entre 1 *et* n-3 : 40
$p(f(n)) =$ $3 + 9 + 11 + 15 + 21 + 23 + 29 + 35 + 39 + 41 + 45 + 51 + 53$
$+59 + 63 + 65 + 69 + 71 + 75 + 77 + 79$
$f(n) =$ 933

$n =$ 84
$\pi(n) - 1 =$ 22
nombre d'impairs compris entre 1 *et* n-3 : 41
$p(f(n)) =$ $1 + 5 + 11 + 13 + 17 + 23 + 25 + 31 + 37 + 41 + 43 + 47 + 53$
$+55 + 61 + 65 + 67 + 71 + 73 + 77 + 79 + 81$
$f(n) =$ 976

$n =$ 86
$\pi(n) - 1 =$ 22
nombre d'impairs compris entre 1 *et* n-3 : 42
$p(f(n)) =$ $3 + 7 + 13 + 15 + 19 + 25 + 27 + 33 + 39 + 43 + 45 + 49 + 55$
$+57 + 63 + 67 + 69 + 73 + 75 + 79 + 81 + 83$
$f(n) = 1020$

$n =$ 88
$\pi(n) - 1 =$ 22
nombre d'impairs compris entre 1 *et* n-3 : 43
$p(f(n)) =$ $5 + 9 + 15 + 17 + 21 + 27 + 29 + 35 + 41 + 45 + 47 + 51 + 57$
$+59 + 65 + 69 + 71 + 75 + 77 + 81 + 83 + 85$
$f(n) =$ 1064

$n =$ 90
$\pi(n) - 1 =$ 23
nombre d'impairs compris entre 1 *et* n-3 : 44
$p(f(n)) =$ $1 + 7 + 11 + 17 + 19 + 23 + 29 + 31 + 37 + 43 + 47 + 49 + 53$
$+59 + 61 + 67 + 71 + 73 + 77 + 79 + 83 + 85 + 87$
$f(n) =$ 1109

$n =$ 92
$\pi(n) - 1 =$ 23
nombre d'impairs compris entre 1 *et* n-3 : 45
$p(f(n)) =$ $3 + 9 + 13 + 19 + 21 + 25 + 31 + 33 + 39 + 45 + 49 + 51 + 55$
$+61 + 63 + 69 + 73 + 75 + 79 + 81 + 85 + 87 + 89$
$f(n) =$ 1155

$n =$ 94
$\pi(n) - 1 =$ 23
nombre d'impairs compris entre 1 *et* n-3 : 46
$p(f(n)) =$ $5 + 11 + 15 + 21 + 23 + 27 + 33 + 35 + 41 + 47 + 51 + 53 + 57$
$+63 + 65 + 71 + 75 + 77 + 81 + 83 + 87 + 89 + 91$
$f(n) =$ 1201

$n =$ 96
$\pi(n) - 1 =$ 23
nombre d'impairs compris entre 1 *et* n-3 : 47
$p(f(n)) =$ $7 + 13 + 17 + 23 + 25 + 29 + 35 + 37 + 43 + 49 + 53 + 55 + 59$
$+65 + 67 + 73 + 77 + 79 + 83 + 85 + 89 + 91 + 93$
$f(n) =$ 1247

$n =$	98
$\pi(n) - 1 =$	24
nombre d'impairs compris entre 1 *et* n-3 :	48
$p(f(n)) =$	$1 + 9 + 15 + 19 + 25 + 27 + 31 + 37 + 39 + 45 + 51 + 55 + 57$ $+61 + 67 + 69 + 75 + 79 + 81 + 85 + 87 + 91 + 93 + 95$
$f(n) =$	1294
$n =$	100
$\pi(n) - 1 =$	24
nombre d'impairs compris entre 1 *et* n-3 :	49
$p(f(n)) =$	$3 + 11 + 17 + 21 + 27 + 29 + 33 + 39 + 41 + 47 + 53 + 57 + 59$ $+63 + 69 + 71 + 77 + 81 + 83 + 87 + 89 + 93 + 95 + 97$
$f(n) =$	1342

Annexe 3 : trouver des éléments par rapport au $3^{ème}$ coefficient de la deuxième équation

Le troisième coefficient représente la somme des produits de 2 nombres premiers parmi ceux considérés.

Quand on passe de n à $n + 2$, on ajoute 2 à chaque racine de la $2^{ème}$ équation et on ne change pas de nombre de racines (de degré) si $n+1$ n'est pas premier tandis qu'on ajoute la racine 1 si $n+1$ est premier (1 devient complémentaire à n d'un nombre premier et est donc racine de la seconde équation qui recense tous les complémentaires à n de premiers impairs).

Donnons un exemple : passons de $p_1p_2 + p_1p_3 + p_2p_3$ à $(p_1 + 2)(p_2 + 2) + (p_1 + 2)(p_3 + 2) + (p_2 + 2)(p_3 + 2)$. On voit qu'on passe du $3^{ème}$ coefficient de la deuxième équation associée n à celui de la deuxième équation associée à $n + 2$ en effectuant le calcul suivant si $n + 1$ n'est pas premier :

$$g(n + 2) = g(n) + 4\sigma_1(n) + 4(\pi(n) - 1)$$

On doit faire le calcul suivant si $n + 1$ est premier :

$$g(n + 2) = g(n) + 4\sigma_1(n) + 4(\pi(n) - 1) + \sigma_1(n + 2).$$

Tous ces calculs sont beaucoup trop laborieux pour que l'on puisse les mener à bien. Cependant, un théorème exprime que toute fonction rationnelle des lettres a, b, c, etc, invariante par permutation de ces lettres s'exprime en fonction des fonctions symétriques de ces lettres. En raison des relations entre les racines et les coefficients d'un polynôme, on en déduit que toute fonction rationnelle des racines d'une équation s'exprime rationnellement en fonction des coefficients de cette équation. Les solutions de la deuxième équation sont donc calculables et si on connaissait la façon de calculer ces racines, on arriverait peut-être à prouver que l'une de ces solutions est un nombre premier.

Résoudre un système d'équations algébriques pour trouver un décomposant de Goldbach d'un nombre pair

Denise Vella-Chemla

27/10/2011

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. On rappelle qu'un nombre premier impair p est un décomposant de Goldbach de n un nombre pair supérieur ou égal à 6 si p n'est pas congru à n selon tout module premier impair p' inférieur à $\sqrt{n}$. En effet, dans le cas contraire, le complémentaire à n de p est composé.

Exemple : 19 est un décomposant de Goldbach de 98 car 19 est incongru à 98 selon 3, 5 et 7. Par contre, 3 n'est pas un décomposant de Goldbach de 98 car $3 \equiv 98$ (mod 5) (ce qui correspond au fait que 5 divise $98-3$). 5 n'est pas un décomposant de Goldbach de 98 car $5 \equiv 98$ (mod 3). 7 n'est pas un décomposant de Goldbach de 98 car $7 \equiv 98$ (mod 7) (ce qui correspond au fait que 7 divise $98-7$, 7 est diviseur de 98). 11 n'est pas un décomposant de Goldbach de 98 car $11 \equiv 98$ (mod 3). 13 n'est pas un décomposant de Goldbach de 98 car $13 \equiv 98$ (mod 5). 17 n'est pas un décomposant de Goldbach de 98 car $17 \equiv 98$ (mod 3).

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n revient donc simplement à chercher un nombre qui vérifie les conditions suivantes : d'une part, il est premier et d'autre part, son complémentaire à n est premier.

Lors de ces recherches autour de la conjecture de Goldbach, comme il s'agit de trouver les solutions entières d'équations, on a longuement buté sur un extrait de Galois qui écrit : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$"*. Récemment, on a pu trouver sur la toile la référence [2] dans laquelle Libri explique sa méthode simple pour trouver les solutions entières d'une équation polynomiale. On réalise à ces lectures que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tous racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$26 = 3+5+7+11.$$
$$236 = 3.5+3.7+3.11+5.7+5.11+7.11.$$
$$886 = 3.5.7+3.5.11+3.7.11+5.7.11.$$
$$1155 = 3.5.7.11.$$

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme suivante :

$$x^{\pi(n)-1} - \sigma_1.x^{\pi(n)-2} + \sigma_2.x^{\pi(n)-3} - \sigma_3.x^{\pi(n)-1} + \ldots = 0$$

La plus grande puissance de x est $\pi(n) - 1$ où $\pi(n)$ est la notation habituelle pour le nombre de nombres premiers inférieurs à n, le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers impairs considérés. Par exemple, $\sigma_1 = p_1+p_2+p_3+p_4... = 3+5+7+11...$, $\sigma_2 = p_1p_2+p_1p_3+...+p_2p_3+p_2p_4+...$ et le dernier σ est le produit de tous les nombres premiers impairs inférieurs à n.

Pour exprimer que $n - x$, le complémentaire du nombre à chercher doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on utilise la même équation polynomiale en remplaçant x par $n - x$; si l'on considère les 4 premiers nombres premiers impairs seulement, l'équation polynomiale devient :

$$((n-x)-3)((n-x)-5)((n-x)-7)((n-x)-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

L'élévation aux différentes puissances du monôme $n - x$ donne les résultats ci-dessous :

$$\begin{array}{l}(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 = n^2 - 2nx + x^2.\end{array}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n - x$ à la puissance i.

Si on développe et qu'on regroupe ensemble les coefficients concernant une même puissance de x, on obtient :

$$x^4+(-4n+26)x^3+(6n^2-78n+236)x^2+(-4n^3+78n^2-472n+886)x+(n^4-26n^3+236n^2-886n+1155) \;=\; 0$$

On reconnaît dans la dernière parenthèse le polynôme initial dans lequel x a été remplacé par n. Puis pour les coefficients des puissances supérieures de x, on voit qu'on dérive successivement le polynôme initial puis les polynômes obtenus, qu'on prend l'opposé du résultat à chaque fois et qu'on divise successivement les résultats intermédiaires par 2, 3, etc.

Pour le degré 4, le polynôme initial est :

$$n^4 - 26n^3 + 236n^2 - 886n + 1155$$

On le dérive et on en prend l'opposé :

$$-4n^3 + 78n^2 - 472n + 886$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 2 :

$$6n^2 - 78n + 236$$

On dérive ce dernier, on en prend l'opposé et on divise le résultat par 3 :

$$-4n + 26$$

Les coefficients d'expression $\frac{(-1)^n P^{(n)}(x)}{n!}$ sont appelés coefficients du développement de Taylor.

On est donc systématiquement ramené au système d'équations à deux équations de degré i suivant, dont il faudrait réussir à prouver qu'il admet systématiquement au moins une solution :

$$\begin{cases} P(x) : x^{\pi(n)-1} - \sigma_1.x^{\pi(n)-2} + \sigma_2.x^{\pi(n)-3} - \sigma_3.x^{\pi(n)-1} + \ldots = 0 \\ \sum_{i=0}^{i=\pi(n)-1} \frac{(-1)^i P^{(i)}(n)}{i!} x^i = 0 \end{cases}$$

3 Exemples

Traitons les exemples $n = 8$ et $n = 10$. Il n'y a que trois nombres premiers impairs inférieurs à n, 3, 5 *et* 7.
L'équation polynomiale $(x-3)(x-5)(x-7) = 0$ se développe en $x^3 - 15x^2 + 71x - 105 = 0$.
L'équation polynomiale portant sur $n - x$ se développe quant à elle en :
$-x^3 + (3n-15)x^2 + (-3n^2 + 30n - 71)x + (n^3 - 15n^2 + 71n - 105) = 0$.
Si on remplace n par 8, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases}$$

3 et 5 sont les seules solutions de ce système. Ce sont les décomposants de Goldbach de 8.

Si on remplace n par 10, on aboutit au système :

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases}$$

Les deux équations sont équivalentes, 3 et 5 et 7 sont solutions de ce système, et sont décomposants de Goldbach de 10.

4 Démonstration graphique

On comprend aisément, puisque c'est ainsi qu'on les a construites, que les courbes des deux équations identifiées sont verticalement symétriques l'une de l'autre par rapport à un axe vertical d'équation $x = n/2$.

Imaginons deux points se déplaçant à même vitesse sur ces deux courbes, depuis le point d'ordonnée $x = n/2$, l'un vers la droite sur la première courbe, l'autre vers la gauche sur la deuxième courbe.

Premier cas, le point en question est sur l'axe des abscisses, il annule les deux courbes, $n/2$ est un nombre premier ; un nombre pair double d'un nombre premier vérifie trivialement la conjecture.

Deuxième cas, le point en question n'annule pas les courbes, elles s'intersectent en lui, au-dessus ou bien au-dessous de l'axe des abscisses. Puis plusieurs fois, elles vont ainsi se croiser. A chaque fois qu'elles se croisent, les deux polynômes coïncident, n'en sont qu'un.

Prenons l'exemple du nombre pair 8 dont on a vu que les deux polynômes représentant ses décomposants de Goldbach sont les polynômes suivants :

$$x^3 - 15x^2 + 71x - 105 = 0$$
$$x^3 - 9x^2 + 23x - 15 = 0$$

$n/2$ vaut 4. L'une des solutions de Goldbach est la solution $3 + 5$, 3 et 5 sont séparés de 4, le milieu, par $\Delta = 1$. Voyons ce qu'il advient de nos deux polynômes lorsqu'on remplace x par $x - 1$ dans le premier et x par $x + 1$ dans le second.

$$(x+1)^3 - 15(x+1)^2 + 71(x+1) - 105 = x^3 - 12x^2 + 44x - 48 = 0$$
$$(x-1)^3 - 9(x-1)^2 + 23(x-1) - 15 = x^3 - 12x^2 + 44x - 48 = 0$$

Si par contre on fait la même chose avec $x - 3$ et $x + 3$, on n'obtient pas du tout les mêmes polynômes, ceci est dû au fait que $1 + 7$ n'est pas une décomposition de Goldbach :

$$(x+3)^3 - 15(x+3)^2 + 71(x+3) - 105 = x^3 - 6x^2 + 8x = 0$$
$$(x-3)^3 - 9(x-3)^2 + 23(x-3) - 15 = x^3 - 18x^2 + 104x - 192 = 0$$

Dans le cas du nombre pair 12 dont on sait que $5 + 7$ est une décomposition située à un Δ de 1 de la moitié de 12 qu'est 6, on obtient les transformations de polynômes suivantes avec Sage :

$$p = x^4 - 22 * x^3 + 164 * x^2 - 458 * x + 315$$
$$p.substitute(x = x - 1).expand()$$
$$>> x^4 - 26 * x^3 + 236 * x^2 - 856 * x + 960$$
$$p = x^4 - 26 * x^3 + 236 * x^2 - 886 * x + 1155$$
$$p.substitute(x = x + 1).expand()$$
$$>> x^4 - 22 * x^3 + 164 * x^2 - 488 * x + 480$$

Le polynôme obtenu par changement de variable dans le premier polynôme fournit un polynôme qui a le même début que le second polynôme et inversement, ce qui permet d'abaisser le degré des équations à résoudre. Malheureusement, on n'arrive pas du tout à obtenir des résultats semblables dès le degré 5.

C'est bien à cause de la Théorie de Galois que la conjecture de Goldbach est vraie : il y a un changement de la variable dans les deux polynômes par $x-\Delta$ et $x+\Delta$ qui fait que les deux polynômes n'en deviennent plus qu'un. Le changement en question fournit la décomposition de Goldbach du nombre pair considéré en $(x-\Delta)+(x+\Delta)$.

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 428, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

[3], **Léonard Euler**, *Démonstration sur le nombre de points où deux lignes des ordres quelconques peuvent se couper*, Mémoires de l'Académie des Sciences et belles lettres de Berlin [4], Berlin, 1750, p.234-248.

[4], **Léonard Euler**, *Nouvelle méthode d'éliminer les quantités inconnues des équations*, Mémoires de l'Académie des Sciences et belles lettres de Berlin [20], Berlin, 1764, p.91-104.

Annexe 1 : exemples des degrés 2 à 6

Si on résoud les équations dont on a calculé les coefficients en remplaçant n successivement par les valeurs 12 (équations de degré 4 car il y a 4 nombres premiers impairs inférieurs à 12 qui sont $3, 5, 7$ et 11) puis par les valeurs 14 et 16 pour n (équations polynomiales de degré 5 car on a rajouté le nombre premier impair 13), et enfin 18 (degré 6) avec un outil tel que l'outil libre Sage qui permet la résolution d'équations polynomiales, on arrive à résoudre les systèmes ci-dessous.

Pour $n = 12$, il faut résoudre le système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 + (26-4n)x^3 + (6n^2 - 78n + 236)x^2 + (-4n^3 + 78n^2 - 472n + 886)x + (n^4 - 26n^3 + 236n^2 - 886n + 1155) = 0 \end{cases}$$

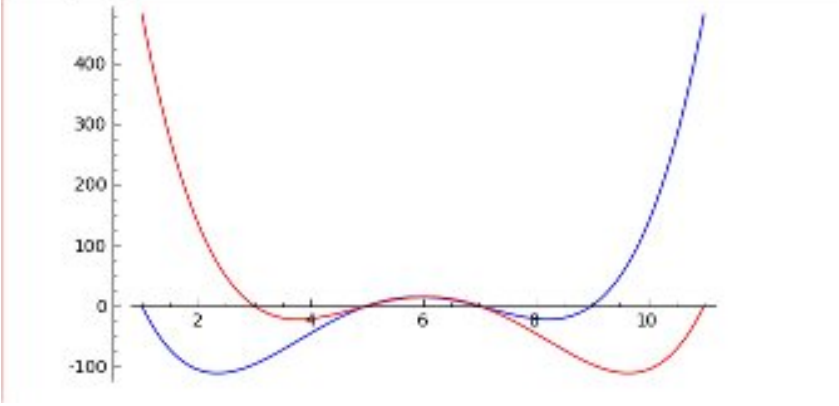
qui se ramène au système :

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont bien 5 et 7 qui sont bien les décomposants de Goldbach de 12.

La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :

```
f=plot(x^4-22*x^3+164*x^2-458*x+315,(x,1,11),rgbcolor=(0,0,1))
g=plot(x^4-26*x^3+236*x^2-886*x+1155,(x,1,11),rgbcolor=(1,0,0))
show(f+g)
```



Calculons les équations pour le degré 5 (nombres premiers impairs 3, 5, 7, 11 et 13).

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 10725 = 0$$

avec

$3 + 5 + 7 + 11 + 13 = 39$
$3.5 + 3.7 + 3.11 + 3.13 + 5.7 + 5.11 + 5.13 + 7.11 + 7.13 + 11.13 = 574$
$3.5.7 + 3.5.11 + 3.5.13 + 3.7.11 + 3.7.13 + 3.11.13 + 5.7.11 + 5.7.13 + 5.11.13 + 7.11.13 = 3954$
$3.5.7.11 + 3.5.7.13 + 3.5.11.13 + 3.7.11.13 + 5.7.11.13 = 12673$
$3.5.7.11.13 = 15015.$

En remplaçant x par $n-x$, on obtient le polynôme suivant dont on cherche quelles valeurs de x l'annulent.

$$\begin{array}{rrrrrrr}
 & & & & & & -x^5 \\
 & & & & +(5n & -39) & x^4 \\
 & & & +(-10n^2 & +156n & -574) & x^3 \\
 & & +(10n^3 & -234n^2 & +1722n & -3954) & x^2 \\
 & +(-5n^4 & +156n^3 & -1722n^2 & +7908n & -12673) & x^1 \\
+(n^5 & -39n^4 & +574n^3 & -3954n^2 & +12673n & -15015) &
\end{array}$$

Pour $n = 14$ ou $n = 16$, il faut résoudre le système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + (5n-39)x^4 + (-10n^2 + 156n - 574)x^3 + (10n^3 - 234n^2 + 1722n - 3954)x^2 + \\ \qquad (-5n^4 + 156n^3 - 1722n^2 + 7908n - 12673)x + (n^5 - 39n^4 + 574n^3 - 3954n^2 + 12673n - 15015) = 0 \end{cases}$$

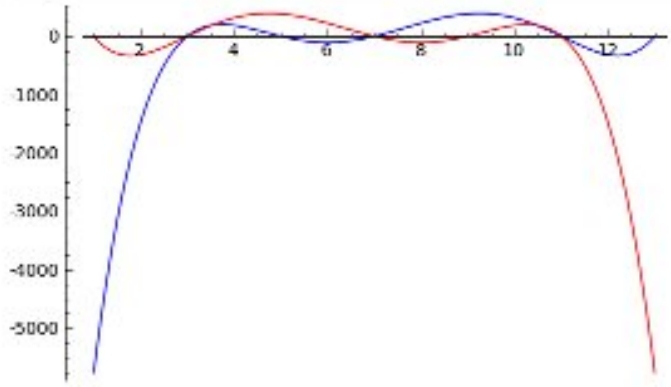
qui se ramène dans le cas de $n = 14$ au système :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0 \end{cases}$$

Les seules valeurs de x qui conviennent sont $3, 7$ et 11, qui sont bien les décomposants de Goldbach de 14.

La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :

```
f=plot(x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015,(x,1,13),rgbcolor=(0,0,1))
g=plot(-x^5+31*x^4-350*x^3+1730*x^2-3489*x+2079,(x,1,13),rgbcolor=(1,0,0))
show(f+g)
```



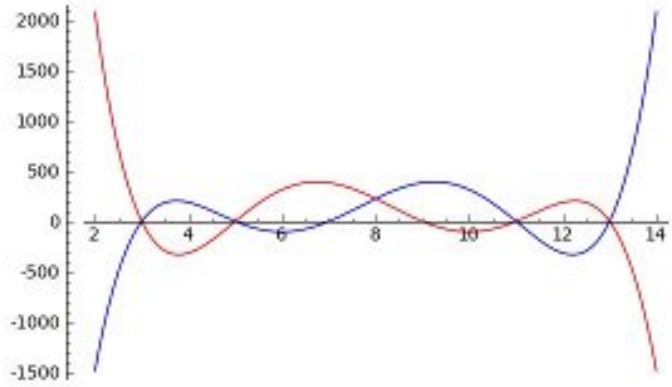
Pour $n = 16$, le système final à résoudre est :

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{cases}$$

Le pgcd de ces deux polynômes est $x^4 - 32x^3 + 350x^2 - 1504x + 2145$. Les seules valeurs de x qui conviennent sont $3, 5, 11$ et 13, qui sont bien les décomposants de Goldbach de 16.

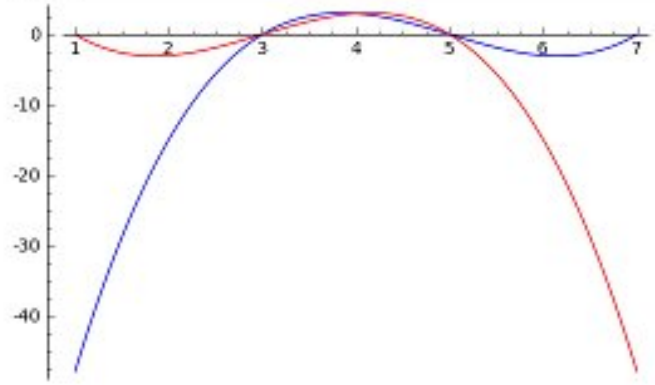
La visualisation des deux polynômes par l'outil libre Sage est fournie ci-dessous :

```
f=plot(x^5-39*x^4+574*x^3-3954*x^2+12673*x-15015,(x,2,14),rgbcolor=(0,0,1))
g=plot(-x^5+41*x^4-638*x^3+4654*x^2-15681*x+19305,(x,2,14),rgbcolor=(1,0,0))
show(f+g)
```

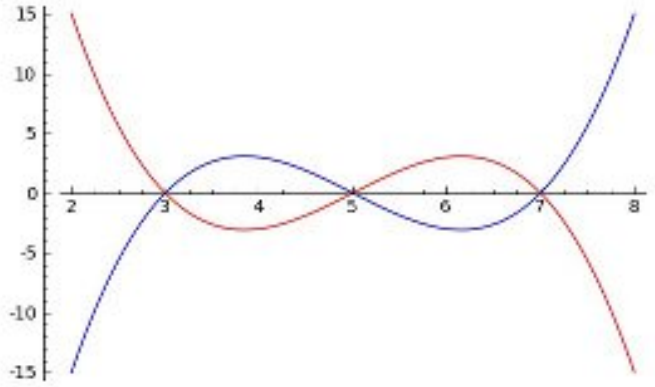


Fournissons enfin les visualisations par l'outil libre Sage des polynômes permettant de trouver les décomposants de Goldbach des nombres pairs 6, 8, 10 et 18.

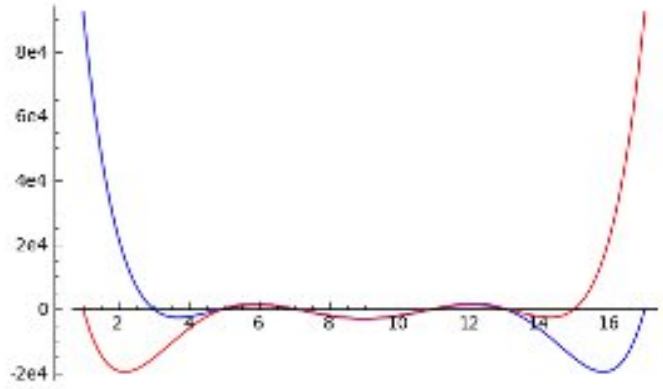
```
f=plot(x^3-15*x^2+71*x-105,(x,1,7),rgbcolor=(0,0,1))
g=plot(-x^3+9*x^2-23*x+15,(x,1,7),rgbcolor=(1,0,0))
show(f+g)
```




```
f=plot(x^3-15*x^2+71*x-105,(x,2,8),rgbcolor=(0,0,1))
g=plot(-x^3+15*x^2-71*x+105,(x,2,8),rgbcolor=(1,0,0))
show(f+g)
```




```
f=plot(x^6-56*x^5+1237*x^4-13712*x^3+79891*x^2-230456*x+255255,(x,1,17),rgbcolor=(0,0,1))
g=plot(x^6-52*x^5+1057*x^4-10552*x^3+52891*x^2-118420*x+75075,(x,1,17),rgbcolor=(1,0,0))
show(f+g)
```



S'amuser avec les nombres

Denise Vella-Chemla

20/11/2011

On peut trouver sur la toile un article concernant les identités de Newton*, dont on recopie un extrait : *En algèbre, les identités de Newton fournissent, dans les espaces de polynômes en plusieurs variables, un lien entre les polynômes symétriques élémentaires et les sommes de Newton, c'est-à-dire les sommes de puissances des indéterminées.*

On pose $s_k = r_1^k + \cdots + r_n^k$, *où les* r_i *sont les racines de* $P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$. *On peut démontrer :*

$$\begin{aligned}
&a_n s_1 {+1} a_{n-1} = 0,\\
&a_n s_2 + a_{n-1}s_1 {+2} a_{n-2} = 0,\\
&a_n s_3 + a_{n-1}s_2 + a_{n-2}s_1 {+3} a_{n-3} = 0,\\
&\vdots\\
&a_n s_d + a_{n-1}s_{d-1} + \ldots + a_{n-d+1}s_1 {+d} a_{n-d} = 0.
\end{aligned}$$

On va l'appliquer à un polynôme pour montrer l'aspect magique de ces résultats.

Les nombres $1, 3, 7, 9$ et 11 sont tous solutions de l'équation :

$$x^5 - 31x^4 + 350x^3 - 1730x^2 + 3489x - 2079 = 0$$

On a :

$$\begin{aligned}
s_1 &= 1 + 3 + 7 + 9 + 11 = 31\\
s_2 &= 1^2 + 3^2 + 7^2 + 9^2 + 11^2\\
&= 1 + 9 + 49 + 81 + 121\\
&= 261\\
s_3 &= 1^3 + 3^3 + 7^3 + 9^3 + 11^3\\
&= 1 + 27 + 343 + 729 + 1331\\
&= 2431\\
s_4 &= 1^4 + 3^4 + 7^4 + 9^4 + 11^4\\
&= 1 + 81 + 2401 + 6561 + 14641\\
&= 23685\\
s_5 &= 1^5 + 3^5 + 7^5 + 9^5 + 11^5\\
&= 1 + 243 + 16807 + 59049 + 161051\\
&= 237151
\end{aligned}$$

*http://fr.wikipedia.org/wiki/Identités_de_Newton

Ecrivons les identités de Newton et vérifions-les.

$s_1+1.(-31) = 0$
$31 - 31 = 0$

$s_2 - 31s_1+2.(350) = 0$
$261 - 31.31 + 700 = 0$
$961 - 961 = 0$

$s_3 - 31s_2 + 350s_1+3.(-1730) = 0$
$2431 - 31.(261) + 350.(31) + 3.(-1730) = 0$
$2431 - 8091 + 10850 - 5190 = 0$

$s_4 - 31s_3 + 350s_2 - 1730s_1+4.(3489) = 0$
$23685 - 31.(2431) + 350.(261) - 1730.(31) + 4.(3489) = 0$
$23685 - 75361 + 91350 - 53630 + 13956 = 0$

$s_5 - 31s_4 + 350s_3 - 1730s_2 + 3489s_1+5.(-2079) = 0$
$237151 - 31.(23685) + 350.(2431) - 1730.(261) + 3489.(31) + 5.(-2079) = 0$
$237151 - 734235 + 850850 - 451530 + 108159 - 10395 = 0$

On pourrait inversement exprimer les nombres entiers successifs $1, 2, 3, 4$ et 5 en fonction des sommes de puissances des indéterminées et des coefficients du polynôme, de la façon suivante :

$$+1 = -\frac{a_n s_1}{a_{n-1}}$$

$$+2 = -\frac{a_n s_2 + a_{n-1} s_1}{a_{n-2}}$$

$$+3 = -\frac{a_n s_3 + a_{n-1} s_2 + a_{n-2} s_1}{a_{n-3}}$$

$$\vdots$$

$$+d = -\frac{a_n s_d + a_{n-1} s_{d-1} + \ldots + a_{n-d+1} s_1}{a_{n-d}}$$

Vision algorithmique de la Conjecture de Goldbach

Denise Vella-Chemla

23/11/2011

On appelle séquence d'entiers une suite finie ordonnée d'entiers. La fonction concaténation prend en argument deux séquences $s1$ et $s2$ et retourne la séquence constituée des éléments de $s1$ suivis des éléments de $s2$.

Considérons les séquences d'entiers suivantes :

$$s_0 = \{1, 3\}$$
$$s_1 = \{1, 3, 5\}$$
$$s_2 = \{3, 5, 7\}.$$

Définissons la fonction $f(S)$ qui associe à la séquence d'entiers S une séquence d'entiers contenant tous les éléments de S auxquels on a ajouté 2.
Définissons alors s_{i+1} de la façon suivante : $s_{i+1} = f(s_i)$ si et seulement si le dernier élément de s_i augmenté de 4 n'est pas un nombre premier et $s_{i+1} = concat(\{1\}, f(s_i))$ sinon.

Démontrer la conjecture de Goldbach équivaut à démontrer que toutes les séquences engendrées par l'algorithme ainsi défini contiennent un nombre premier.
Les séquences pour les nombres pairs de 6 à 100 sont fournies ci-dessous. Les nombres premiers sont bleus.

6 :	1	3																					
8 :	1	3	5																				
10 :	3	5	7																				
12 :	1	5	7	9																			
14 :	1	3	7	9	11																		
16 :	3	5	9	11	13																		
18 :	1	5	7	11	13	15																	
20 :	1	3	7	9	13	15	17																
22 :	3	5	9	11	15	17	19																
24 :	1	5	7	11	13	17	19	21															
26 :	3	7	9	13	15	19	21	23															
28 :	5	9	11	15	17	21	23	25															
30 :	1	7	11	13	17	19	23	25	27														
32 :	1	3	9	13	15	19	21	25	27	29													
34 :	3	5	11	15	17	21	23	27	29	31													
36 :	5	7	13	17	19	23	25	29	31	33													
38 :	1	7	9	15	19	21	25	27	31	33	35												
40 :	3	9	11	17	21	23	27	29	33	35	37												
42 :	1	5	11	13	19	23	25	29	31	35	37	39											
44 :	1	3	7	13	15	21	25	27	31	33	37	39	41										
46 :	3	5	9	15	17	23	27	29	33	35	39	41	43										
48 :	1	5	7	11	17	19	25	29	31	35	37	41	43	45									
50 :	3	7	9	13	19	21	27	31	33	37	39	43	45	47									
52 :	5	9	11	15	21	23	29	33	35	39	41	45	47	49									
54 :	1	7	11	13	17	23	25	31	35	37	41	43	47	49	51								
56 :	3	9	13	15	19	25	27	33	37	39	43	45	49	51	53								
58 :	5	11	15	17	21	27	29	35	39	41	45	47	51	53	55								
60 :	1	7	13	17	19	23	29	31	37	41	43	47	49	53	55	57							
62 :	1	3	9	15	19	21	25	31	33	39	43	45	49	51	55	57	59						
64 :	3	5	11	17	21	23	27	33	35	41	45	47	51	53	57	59	61						
66 :	5	7	13	19	23	25	29	35	37	43	47	49	53	55	59	61	63						
68 :	1	7	9	15	21	25	27	31	37	39	45	49	51	55	57	61	63	65					
70 :	3	9	11	17	23	27	29	33	39	41	47	51	53	57	59	63	65	67					
72 :	1	5	11	13	19	25	29	31	35	41	43	49	53	55	59	61	65	67	69				
74 :	1	3	7	13	15	21	27	31	33	37	43	45	51	55	57	61	63	67	69	71			
76 :	3	5	9	15	17	23	29	33	35	39	45	47	53	57	59	63	65	69	71	73			
78 :	5	7	11	17	19	25	31	35	37	41	47	49	55	59	61	65	67	71	73	75			
80 :	1	7	9	13	19	21	27	33	37	39	43	49	51	57	61	63	67	69	73	75	77		
82 :	3	9	11	15	21	23	29	35	39	41	45	51	53	59	63	65	69	71	75	77	79		
84 :	1	5	11	13	17	23	25	31	37	41	43	47	53	55	61	65	67	71	73	77	79	81	
86 :	3	7	13	15	19	25	27	33	39	43	45	49	55	57	63	67	69	73	75	79	81	83	
88 :	5	9	15	17	21	27	29	35	41	45	47	51	57	59	65	69	71	75	77	81	83	85	
90 :	1	7	11	17	19	23	29	31	37	43	47	49	53	59	61	67	71	73	77	79	83	85	87
92 :	3	9	13	19	21	25	31	33	39	45	49	51	55	61	63	69	73	75	79	81	85	87	89
94 :	5	11	15	21	23	27	33	35	41	47	51	53	57	63	65	71	75	77	81	83	87	89	91
96 :	7	13	17	23	25	29	35	37	43	49	53	55	59	65	67	73	77	79	83	85	89	91	93
98 :	1	9	15	19	25	27	31	37	39	45	51	55	57	61	67	69	75	79	81	85	87	91	93	95
100 :	3	11	17	21	27	29	33	39	41	47	53	57	59	63	69	71	77	81	83	87	89	93	95	97

Vision algorithmique de la Conjecture de Goldbach

Denise Vella-Chemla

23/11/2011

On appelle séquence d'entiers une suite finie ordonnée d'entiers. La fonction concaténation prend en argument deux séquences $s1$ et $s2$ et retourne la séquence constituée des éléments de $s1$ suivis des éléments de $s2$.

Considérons les séquences d'entiers suivantes :

$$s_0 = \{1, 3\}$$
$$s_1 = \{1, 3, 5\}$$
$$s_2 = \{3, 5, 7\}$$

Définissons la fonction $f(S)$ qui associe à la séquence d'entiers S une séquence d'entiers contenant tous les éléments de S auxquels on a ajouté 2.
Définissons alors s_{i+1} de la façon suivante : $s_{i+1} = f(s_i)$ si et seulement si le dernier élément de s_i augmenté de 4 n'est pas un nombre premier et $s_{i+1} = concat(\{1\}, f(s_i))$ sinon.

Démontrer la conjecture de Goldbach équivaut à démontrer que toutes les séquences engendrées par l'algorithme ainsi défini contiennent un nombre premier.
Les séquences pour les nombres pairs de 6 à 100 sont fournies ci-dessous. Les nombres premiers sont bleus.

Essayons d'imaginer une récurrence : admettons que la conjecture de Goldbach soit vraie jusqu'à $n-2$, i.e. pour chaque nombre k inférieur ou égal à $n-2$, on a trouvé un nombre premier (au moins) dans la séquence de nombres associée à k. Par définition, la séquence de nombres à associer à n est totalement déterminée par celle associée à $n-2$ et par la valeur de $n-2$. Mais imaginons que cela ne soit pas le cas, imaginons que ces nombres soient en quelque sorte choisis au hasard : la séquence associée à n contient $B = \pi(n) - 1$ nombres choisis au pire parmi $A = \frac{n-2}{2}$ nombres (voire donc parmi moins). Il y a C_A^B combinaisons de nombres possibles.

Calculons :

$$C_A^B = \frac{\left(\frac{n-2}{2}\right)!}{(\pi(n)-1)!\left(\frac{n-2}{2} - \pi(n) + 1\right)!}$$

$\pi(n)$ tend vers $n/ln(n)$ selon le théorème des nombres premiers de Hadamard et La Vallée-Poussin. Le dénominateur se simplifie en $n/2$ si l'on assimile $ln(n) - 2$ à $ln(n)$.
C_A^B devient $\frac{n}{2}\left(\frac{n}{2}-1\right)\left(\frac{n}{2}-2\right)\ldots\left(\frac{n}{ln(n)}\right)$

Le fait que ce nombre soit supérieur à $n/ln(n)$ le nombre de nombres premiers inférieurs ou égaux à n garantirait-il par le principe des tiroirs que la nouvelle ligne contient forcément elle-aussi un nombre premier au moins ?

Autre possibilité : par l'hypothèse de récurrence, toutes les lignes pour les nombres inférieurs à n contiennent un nombre premier. Mais on peut "étendre" ces lignes de multiples manières, en leur adjoignant des nombres quelconques, et en obtenant de la sorte des multitudes de lignes (à dénombrer) qui "couvrent" peut-être toutes ces combinaisons que l'on peut obtenir pour n.

6 :	1	3																					
8 :	1	3	5																				
10 :	3	5	7																				
12 :	1	5	7	9																			
14 :	1	3	7	9	11																		
16 :	3	5	9	11	13																		
18 :	1	5	7	11	13	15																	
20 :	1	3	7	9	13	15	17																
22 :	3	5	9	11	15	17	19																
24 :	1	5	7	11	13	17	19	21															
26 :	3	7	9	13	15	19	21	23															
28 :	5	9	11	15	17	21	23	25															
30 :	1	7	11	13	17	19	23	25	27														
32 :	1	3	9	13	15	19	21	25	27	29													
34 :	3	5	11	15	17	21	23	27	29	31													
36 :	5	7	13	17	19	23	25	29	31	33													
38 :	1	7	9	15	19	21	25	27	31	33	35												
40 :	3	9	11	17	21	23	27	29	33	35	37												
42 :	1	5	11	13	19	23	25	29	31	35	37	39											
44 :	1	3	7	13	15	21	25	27	31	33	37	39	41										
46 :	3	5	9	15	17	23	27	29	33	35	39	41	43										
48 :	1	5	7	11	17	19	25	29	31	35	37	41	43	45									
50 :	3	7	9	13	19	21	27	31	33	37	39	43	45	47									
52 :	5	9	11	15	21	23	29	33	35	39	41	45	47	49									
54 :	1	7	11	13	17	23	25	31	35	37	41	43	47	49	51								
56 :	3	9	13	15	19	25	27	33	37	39	43	45	49	51	53								
58 :	5	11	15	17	21	27	29	35	39	41	45	47	51	53	55								
60 :	1	7	13	17	19	23	29	31	37	41	43	47	49	53	55	57							
62 :	1	3	9	15	19	21	25	31	33	39	43	45	49	51	55	57	59						
64 :	3	5	11	17	21	23	27	33	35	41	45	47	51	53	57	59	61						
66 :	5	7	13	19	23	25	29	35	37	43	47	49	53	55	59	61	63						
68 :	1	7	9	15	21	25	27	31	37	39	45	49	51	55	57	61	63	65					
70 :	3	9	11	17	23	27	29	33	39	41	47	51	53	57	59	63	65	67					
72 :	1	5	11	13	19	25	29	31	35	41	43	49	53	55	59	61	65	67	69				
74 :	1	3	7	13	15	21	27	31	33	37	43	45	51	55	57	61	63	67	69	71			
76 :	3	5	9	15	17	23	29	33	35	39	45	47	53	57	59	63	65	69	71	73			
78 :	5	7	11	17	19	25	31	35	37	41	47	49	55	59	61	65	67	71	73	75			
80 :	1	7	9	13	19	21	27	33	37	39	43	49	51	57	61	63	67	69	73	75	77		
82 :	3	9	11	15	21	23	29	35	39	41	45	51	53	59	63	65	69	71	75	77	79		
84 :	1	5	11	13	17	23	25	31	37	41	43	47	53	55	61	65	67	71	73	77	79	81	
86 :	3	7	13	15	19	25	27	33	39	43	45	49	55	57	63	67	69	73	75	79	81	83	
88 :	5	9	15	17	21	27	29	35	41	45	47	51	57	59	65	69	71	75	77	81	83	85	
90 :	1	7	11	17	19	23	29	31	37	43	47	49	53	59	61	67	71	73	77	79	83	85	87
92 :	3	9	13	19	21	25	31	33	39	45	49	51	55	61	63	69	73	75	79	81	85	87	89
94 :	5	11	15	21	23	27	33	35	41	47	51	53	57	63	65	71	75	77	81	83	87	89	91
96 :	7	13	17	23	25	29	35	37	43	49	53	55	59	65	67	73	77	79	83	85	89	91	93
98 :	1	9	15	19	25	27	31	37	39	45	51	55	57	61	67	69	75	79	81	85	87	91	93	95
100 :	3	11	17	21	27	29	33	39	41	47	53	57	59	63	69	71	77	81	83	87	89	93	95	97

On a une première équation polynomiale qui a pour racines les nombres premiers impairs inférieurs à n. On remplace x par $n-x$ dans cette équation pour obtenir une nouvelle équation polynomiale qui a pour racines les complémentaires des nombres premiers impairs inférieurs à n. Lorsque les racines de la deuxième équation polynomiale sont des nombres premiers impairs, ce sont des décomposants de Goldbach de n.

1 Degré 3 : nombres premiers 3, 5, 7

$$x^3 - 15x^2 + 71x - 105 = 0$$

$$(n-x)^3 - 15(n-x)^2 + 71(n-x) - 105 = 0$$

$$x^3 - (3n-15)x^2 + (3n^2 - 30n + 71)x - (n^3 - 15n^2 + 71n - 105) = 0$$

$$(x^3 - n^3) - (3nx^2 - 3n^2x) + (15x^2 + 15n^2) + (71x - 71n) - 30nx + 105 = 0$$

Il y a invariance de l'équation par permutation de n et x.

2 Degré 4 : nombres premiers 3, 5, 7, 11

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0$$

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0$$

$$x^4 - (4n-26)x^3 + (6n^2 - 78n + 886)x^2 - (4n^3 - 78n^2 + 886n - 236)x \\ +(n^4 - 26n^3 + 886n^2 - 236n + 1155) = 0$$

$$(x^4 + n^4) - (4nx^4 + 4n^3x + (26x^3 - 26n^3) - (78nx^2 - 78n^2x) + (886x^2 + 886n^2) \\ -(236x + 236n) + (6n^2x^2 + 886nx + 1155) = 0$$

Il y a invariance de l'équation par permutation de n et x.

3 Degré 5 : nombres premiers 3, 5, 7, 11, 13

$$x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0$$

$$(n-x)^5 - 39(n-x)^4 + 574(n-x)^3 - 3954(n-x)^2 + 12673(n-x) - 15015 = 0$$

$$x^5 - (5n-39)x^4 + (10n^2 - 156n + 574)x^3 - (10n^3 - 234n^2 + 1722n - 3954)x^2 + \\ (5n^4 - 156n^3 + 1722n^2 - 7908n + 12673)x - (n^5 - 39n^4 + 574n^3 - 3954n^2 + 12673n - 15015) = 0$$

$$(x^5 - n^5) - (5nx^4 - 5n^4x) - (39x^4 - 39n^4) + (10n^2x^3 - 10n^3x^2) - (156nx^3 + 156n^3x) \\ +(574x^3 - 574n^3) - (1722nx^2 - 1722n^2x) - (3954x^2 - 3954n^2) + (12673x - 12673n) \\ -(234n^2x^2 + 7908nx - 15015) = 0$$

Il y a invariance de l'équation par permutation de n et x.

4 Degré 6 : nombres premiers 3, 5, 7, 11, 13, 17

$$x^6 - 56x^5 + 1237x^4 - 13712x^3 + 79891x^2 - 230456x + 255255 = 0$$

$$(n-x)^6 - 56(n-x)^5 + 1237(n-x)^4 - 13712(n-x)^3 + 79891(n-x)^2 - 230456(n-x) + 255255 = 0$$

$$\begin{aligned} x^6 &- (6n-56)x^5 + (15n^2 - 280n + 1237)x^4 - (20n^3 - 560n^2 + 4948n - 13712)x^3 + \\ &(15n^4 - 560n^3 + 7422n^2 - 41136n + 79891)x^2 \\ &-(6n^5 - 280n^4 + 4948n^3 - 41136n^2 - 159782n - 230456)x \\ &+(n^6 - 56n^5 + 1237n^4 - 13712n^3 + 79891n^2 - 230456n + 255255) = 0 \end{aligned}$$

$$\begin{aligned} &(x^6 + n^6) - (6nx^5 + 6n^5x) - (56x^5 + 56n^5) + (15n^2x^4 + 15n^4x^2) - (280nx^4 - 280n^4x) \\ &+(1237x^4 + 1237n^4) + (560n^2x^3 - 560n^3x^2) - (4948nx^3 + 4948n^3x) + (13712x^3 - 13712n^3) \\ &-(41136nx^2 - 41136n^2x) - (79891x^2 - 79891n^2) - (230456x + 230456n) \\ &-(20n^3x^3 - 7422n^2x^2 - 159782nx - 255255) = 0 \end{aligned}$$

Il y a invariance de l'équation par permutation de n et x.

Les équations polynomiales obtenues semblent toujours être des fonctions invariantes par permutation de n et x. Il faut trouver pourquoi ces équations ont toujours l'une de leurs racines au moins qui est un nombre premier impair.

Conjecture de Goldbach et nullité du déterminant d'une matrice de Sylvester

Denise Vella-Chemla

25/12/2011

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. Trouver les décomposants de Goldbach d'un nombre pair n équivaut à trouver les racines communes de deux polynômes : le premier polynôme a pour seules racines les nombres premiers impairs inférieurs ou égaux à n ; le second polynôme a pour seules racines leur complémentaire à n. Par exemple, trouver les décomposants de Goldbach de 6 consiste à trouver les racines communes des polynômes $x^2 - 8x + 15 = (x-3)(x-5)$, et $x^2 - 4x + 3 = (x-1)(x-3)$.

Les coefficients et les racines des deux polynômes vérifient les équations de Viète : dans le cas général d'un polynôme unitaire $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_o$:

$x_1 + x_2 + ... + x_n = -a_{n-1}$
$x_1x_2 + x_1x_3 + ... + x_{n-1}x_n = a_{n-2}$ (*somme de tous les produits* 2 à 2)
$x_1x_2x_3 + x_1x_2x_4 + ... + x_{n-2}x_{n-1}x_n = -a_{n-3}$ (*somme de tous les produits* 3 à 3)
...
$x_1x_2...x_k + x_1x_2...x_{k+1} + ... + x_{n-k}x_{n-k+1}...x_n = (-1)^k a_{n-k}$ (*somme de tous les produits k à k*)
...
$x_1x_2...x_n = (-1)^n a_o$.

Les coefficients du deuxième polynôme sont les coefficients du développement de Taylor du premier polynôme. Dans le cas du nombre pair $n = 6$, les coefficients du premier polynôme sont $a_1 = 1, a_2 = -8, a_3 = 15$. Les coefficients du deuxième polynôme sont :

$$\begin{aligned} b_1 &= a_1, \\ b_2 &= -2a_1n - a_2, \\ b_3 &= a_1n^2 + a_2n + a_3. \end{aligned}$$

Deux polynômes ont des racines communes si leur résultant (le déterminant de leur matrice de Sylvester) est nul.

On rappelle que la matrice de Sylvester de $P(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$ et $Q(x) = x^n + b_1x^{n-1} + b_2x^{n-2} + \ldots + b_{n-1}x + b_n$ est :

$$\begin{pmatrix} a_0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\ a_1 & a_0 & \ddots & 0 & b_1 & b_0 & \ddots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \ddots & a_0 & \vdots & \vdots & \ddots & b_0 \\ a_n & \vdots & \ddots & \vdots & b_n & \vdots & \ddots & \vdots \\ 0 & a_n & \vdots & \vdots & 0 & b_n & \vdots & \vdots \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & a_n & 0 & \ldots & 0 & b_n \end{pmatrix}$$

Dans le cas $n = 6$, exprimons le résultant uniquement en fonction des coefficients du premier polynôme. Peut-être cela nous permettra-t-il de comprendre pourquoi il est nul.

Le résultant des deux polynômes dans le cas où $n = 6$ est égal à :

$$n^4a_1^4 + 4n^3a_1^3a_2 + 4n^2a_1^3a_3 + 5n^2a_1^2a_2^2 + 8na_1^2a_2a_3 + 2na_1a_2^3 + 4a_1a_2^2a_3$$

Si l'on remplace n par 6, a_1 par 1, a_2 par -8 et a_3 par 15, on obtient :

$$6^4 + 4.6^3.(-8) + 4.6^2.15 + 5.6^2.(-8)^2 + 8.6.(-8).15 + 2.6.(-8)^3 + 4.(-8)^2.15$$

qui est égal à :

$$1296 - 6912 + 2160 + 11520 - 5760 - 6144 + 3840$$

qui est bien nul.

Qu'est-ce qui se joue entre les différents nombres pour que le résultant soit finalement nul ? Voyons si en écrivant les factorisations des nombres intervenant dans la somme, cela s'éclaire ?

$$2^4.3^4 - 2^8.3^3 + 2^4.3^3.5 + 2^8.3^2.5 - 2^7.3^2.5 - 2^{11}.3 + 2^8.3.5$$

On se demande si une telle modélisation de la Conjecture de Goldbach peut améliorer sa compréhension.