Conjecture de Goldbach (1742)

- On note $\mathbb{P}$ l'ensemble des nombres premiers.
  $\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$

- *remarque* : $1 \notin \mathbb{P}$

- **Énoncé :**
  Tout entier pair supérieur à 2 est la somme de deux nombres premiers :

$$\forall n \in 2\mathbb{N}, n > 2, \exists p, q \in \mathbb{P}, n = p + q$$

- p et q sont appelés des *décomposants de Goldbach* de n.

Rappels

- Les nombres premiers plus grands que 3 sont de la forme $6k \pm 1$ ($k \geq 1$).
- n étant un nombre pair plus grand que 4 ne peut être le carré d'un nombre premier impair qui est impair.
- Les décomposants de Goldbach de n sont des éléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$, qui sont premiers à n ; les éléments inversibles sont en nombre $\varphi(n)$ et la moitié d'entre eux sont inférieurs ou égaux à $n/2$.

Rappels

- Si un nombre premier $p \leq n/2$ est congru à n modulo un nombre premier $m_i < \sqrt{n}$ $(n = p + \lambda m_i)$,

  alors son complémentaire q à n est composé parce que $q = n - p = \lambda m_i$ est congru à 0 $(mod\ m_i)$.

  Dans ce cas, le nombre premier p ne peut pas être un décomposant de Goldbach de n.

Algorithme d'obtention des décomposants de Goldbach d'un nombre pair

- C'est une procédure qui permet d'obtenir, parmi les nombres appartenant aux progressions arithmétiques $6k+1$ et/ou $6k-1$, un ensemble de nombres qui sont des décomposants de Goldbach de n.

- Notons m_i $(i = 1, \ldots, j(n))$, les nombres premiers $3 < m_i \leq \sqrt{n}$.

- La procédure consiste :
  - d'abord à éliminer les nombres $p \leq n/2$ congrus à 0 $(mod\ m_i)$
  - puis à éliminer les nombres p congrus à n $(mod\ m_i)$.

- Le crible d'Eratosthène est utilisé pour ces éliminations.

Étude d'un exemple : $n = 500$

- $500 \equiv 2\ (mod\ 3)$.
- Puisque $6k - 1 = 3k' + 2$, tous les nombres premiers de la forme $6k - 1$ sont congrus à $500\ (mod\ 3)$, de telle manière que leur complémentaire à 500 est composé.
- Nous n'avons pas à prendre en compte ces nombres.
- Aussi, nous ne considérons que les nombres de la forme $6k + 1$ inférieurs ou égaux à $500/2$. Ils sont compris entre 7 et 247 (première colonne du tableau).

Étude d'un exemple : $n = 500$

- Puisque $\lfloor \sqrt{500} \rfloor = 22$, les modules premiers m_i différents de 2 et 3 à considérer sont $5, 7, 11, 13, 17, 19$. Appelons-les m_i où $i = 1, 2, 3, 4, 5, 6$.

- $500 = 2^2.5^3$

- 500 est congru à :
  $0 \ (mod\ 5)$,
  $3 \ (mod\ 7)$,
  $5 \ (mod\ 11)$,
  $6 \ (mod\ 13)$,
  $7 \ (mod\ 17)$
  et $6 \ (mod\ 19)$.

Étude de cas : $n = 500$

$a_k = 6k + 1$	*congruence(s)* à 0 *éliminant* a_k	*congruence(s)* à r $\neq 0$ éliminant a_k	n-a_k	*D.G.*
7 (p)	0 (*mod* 7)	7 (*mod* 17)	493	
13 (p)	0 (*mod* 13)		487 (p)	
19 (p)	0 (*mod* 19)	6 (*mod* 13)	481	
25	0 (*mod* 5)	6 (*mod* 19)	475	
31 (p)		3 (*mod* 7)	469	
37 (p)			463 (p)	37
43 (p)			457 (p)	43
49	0 (*mod* 7)	5 (*mod* 11)	451	
55	0 (*mod* 5 *and* 11)		445	
61 (p)			439 (p)	61
67 (p)			433 (p)	67
73 (p)		3 (*mod* 7)	427	
79 (p)			421 (p)	79
85	0 (*mod* 5 *and* 17)		415	
91	0 (*mod* 7 *and* 13)		409 (p)	
97 (p)		6 (*mod* 13)	403	
103 (p)			397 (p)	103
109 (p)		7 (*mod* 17)	391	
115	0 (*mod* 5)	3 (*mod* 7) *and* 5 (*mod* 11)	385	
121	0 (*mod* 11)		379 (p)	
127 (p)			373 (p)	127
133	0 (*mod* 7 *and* 19)		367 (p)	
139 (p)		6 (*mod* 19)	361	
145	0 (*mod* 5)		355	
151 (p)			349 (p)	151
157 (p)		3 (*mod* 7)	343	
163 (p)			337 (p)	163
169	0 (*mod* 13)		331	
175	0 (*mod* 5 *and* 7)	6 (*mod* 13)	325	
181 (p)		5 (*mod* 11)	319	
187	0 (*mod* 11 *and* 17)		313 (p)	
193 (p)			307 (p)	193
199 (p)		3 (*mod* 7)	301	
205	0 (*mod* 5)		295	
211 (p)		7 (*mod* 17)	289	
217	0 (*mod* 7)		283 (p)	
223 (p)			277 (p)	223
229 (p)			271 (p)	229
235	0 (*mod* 5)		265	
241 (p)		3 (*mod* 7)	259	
247	0 (*mod* 13 *and* 19)	5 (*mod* 11)	253	

Remarques :

- La première partie de l'algorithme élimine les nombres p congrus à 0 $(mod\ m_i)$ quelque soit i.

  Son résultat consiste à éliminer tous les nombres composés qui ont un quelconque m_i dans leur décomposition euclidienne, n en faisant éventuellement partie, à éliminer également tous les nombres premiers plus petits que $\sqrt{n}$, mais à conserver tous les nombres premiers supérieurs ou égaux à $\sqrt{n}$ qui est plus petit que $n/4 + 1$.

Remarques :

- La seconde partie de l'algorithme élimine les nombres p dont le complémentaire à n est composé parce qu'ils partagent une congruence avec n ($p \equiv n\ (mod\ m_i)$ pour un i donné).

  Son résultat consiste à éliminer les nombres p de la forme $n = p + \lambda m_i$ quelque soit i.

  - Si $n = \mu_i m_i$,

    aucun nombre premier ne peut satisfaire la relation précédente.

    Puisque n est pair, $\mu_i = 2\nu_i$, la conjecture implique $\nu_i = 1$.
  - Si $n \neq \mu_i m_i$,

    la conjecture implique qu'il existe un nombre premier p tel que, pour un i donné, $n = p + \lambda m_i$ qui peut être réécrit en

    $$n \equiv p\ (mod\ m_i)\ ou\ n - p \equiv 0\ (mod\ m_i).$$

Remarques :

- Tous les modules inférieurs à $\sqrt{n}$ sauf ceux de la factorisation de n apparaissent en troisième colonne (pour les modules qui divisent n, la première et la deuxième passe éliminent les mêmes nombres).

- Un même module ne peut apparaître sur la même ligne en deuxième et troisième colonne.

Article 127 des Recherches arithmétiques de Gauss

Lemme :

- *"Dans la progression* $a, a+1, a+2, \ldots, a+n-1$*, il ne peut y avoir plus de termes divisibles par un nombre quelconque* h *que dans la progression* $1, 2, 3, \ldots, n$ *qui a le même nombre de termes."*

- "En effet, on voit sans peine que
  - si n est divisible par h, il y a dans chaque progression $\frac{n}{h}$ termes divisibles par h ;
  - sinon soit $n = he + f$, f étant $< h$; il y aura dans la première série e termes, et dans la seconde e ou $e+1$ termes divisibles par h."

Article 127 des Recherches arithmétiques de Gauss

- "Il suit de là, comme corollaire, que $\frac{a(a+1)(a+2)(a+3)...(a+n-1)}{1.2.3...n}$ est toujours un nombre entier : proposition connue par la théorie des nombres figurés, mais qui, si je ne me trompe, n'a encore été démontrée directement par personne.
- Enfin on aurait pu présenter plus généralement ce lemme comme il suit :
  Dans la progression $a, a+1, a+2 \ldots a+n-1$, *il y a au moins autant de termes congrus suivant le module h à un nombre donné quelconque, qu'il y a de termes divisibles par h dans la progression* $1, 2, 3 \ldots n$."

Précisions sur les différents cas du lemme

- On note n mod p le reste de la division de n par p.
- De 1 à n, il y a $\left\lfloor \frac{n}{p} \right\rfloor$ nombres congrus à 0 $(mod\ p)$.
- Et si $2n \not\equiv 0\ (mod\ p)$, de 1 à n,
  - il y a $\left\lfloor \frac{n}{p} \right\rfloor$ nombres congrus à $2n\ (mod\ p)$
    $\Leftrightarrow\ n \bmod p < 2n \bmod p$;
  - il y a $\left\lfloor \frac{n}{p} \right\rfloor + 1$ nombres congrus à $2n\ (mod\ p)$
    $\Leftrightarrow\ n \bmod p > 2n \bmod p$.

Comment généraliser le lemme de l'article 127 ?

- On ne sait pas étendre cette connaissance fournie par le lemme (précisée ou pas par la connaissance des restes modulaires de n) à plusieurs modules car on ne sait pas comment les cas se combinent entre eux.

- Peut-on aboutir tout de même à un résultat ?

Comptages

- Entre 1 et $n/2$, il y a moins de nombres dont le complémentaire à n est premier que de nombres premiers.
- Lors de la deuxième passe, tout module diviseur de n n'entraîne l'élimination d'aucun nombre.
- Il y a sensiblement autant de nombres éliminés par la deuxième passe de l'algorithme que par la première passe.
- Il y a sensiblement autant de nombres premiers de la forme $6k + 1$ qu'il y en a de la forme $6k - 1$ (il semblerait que moins de la moitié soit de la forme $6k + 1$).
- Il faudrait être capable de calculer le cardinal de l'intersection des ensembles de nombres éliminés par les deux passes.