Goldbach conjecture (1742)

- We note $\mathbb{P}$ the set of primes.
  $\mathbb{P} = \{2, 3, 5, 7, 11, \ldots\}$

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

- **Statement :**

  Each even number greater than 2 is the sum of two primes :

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

- p and q are called Goldbach components of n.

Recalls

- Primes greater than 3 are of $6k \pm 1$ ($k \geq 1$) form.
- n being an even number greater than 4 can't be an odd prime's square that is odd.
- The Goldbach components of n are invertible elements (units) of $\mathbb{Z}/n\mathbb{Z}$, which are coprime to n. Units are in $\varphi(n)$ quantity and half of them are smaller than or equal to $n/2$.

Recalls

- If a prime $p \leq n/2$ is congruent to n modulo a prime $m_i < \sqrt{n}$ $(n = p + \lambda m_i)$,

  then its complementary q to n is composite because $q = n - p = \lambda m_i$ is congruent to 0 $(mod\ m_i)$.

  In that case, prime p can't be a Goldbach component of n.

An algorithm to obtain an even number's Goldbach components

- It's a process that permits to obtain, among numbers from $6k+1$ and/or $6k-1$ arithmetic progressions, a set of numbers that are Goldbach components of n.
- Let us note m_i $(i = 1, \ldots, j(n))$, primes $3 < m_i \leq \sqrt{n}$.
- The process consists :
  - first in ruling out numbers $p \leq n/2$ congruent to 0 $(mod\ m_i)$
  - then in cancelling numbers p congruent to n $(mod\ m_i)$.
- The sieve of Eratosthenes is used for these eliminations.

A sample study : $n = 500$

- $500 \equiv 2 \ (mod\ 3)$.

- Since $6k - 1 = 3k' + 2$, all primes of the form $6k - 1$ are congruent to 500 $(mod\ 3)$, in such a way that their complementary to 500 is composite.

- We don't have to take those numbers into account.

- So, we only consider numbers of the form $6k + 1$ smaller than or equal to $500/2$. They are between 7 and 247 (first column of the table).

A sample study : $n = 500$

- Since $\lfloor \sqrt{500} \rfloor = 22$, prime moduli m_i different from 2 and 3 to be considerated are $5, 7, 11, 13, 17, 19$. Let us call them m_i where $i = 1, 2, 3, 4, 5, 6$.

- $500 = 2^2.5^3$

- 500 is congruent to :

  $0 \ (mod\ 5)$,
  $3 \ (mod\ 7)$,
  $5 \ (mod\ 11)$,
  $6 \ (mod\ 13)$,
  $7 \ (mod\ 17)$
  and $6 \ (mod\ 19)$.

A sample study : $n = 500$

$a_k = 6k+1$	congruence(s) to 0 cancelling a_k	congruence(s) to r $\neq 0$ cancelling a_k	n-a_k	G.C.
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	

Remarks :

- The first pass of the algorithm cancels numbers p congruent to $0 \ (mod \ m_i)$ for any i.

  Its result consists in ruling out all composite numbers that have some m_i in their euclidean decomposition, n being eventually one of them, in ruling out also all primes smaller than $\sqrt{n}$, but in keeping primes greater than or equal to $\sqrt{n}$ (that is smaller than $n/4+1$).

Remarks :

- The second pass of the algorithm cancels numbers p whose complementary to n is composite because they share a congruence with n ($p \equiv n \ (mod \ m_i)$ for some given i).

  Its result consists in ruling out numbers p of the form $n = p + \lambda m_i$ for any i.

  - If $n = \mu_i m_i$,

    no prime can satisfy the preceding relation.

    Since n is even, $\mu_i = 2\nu_i$, conjecture implies that $\nu_i = 1$.
  - If $n \neq \mu_i m_i$,

    conjecture implies that there exists a prime p such that, for a given i, $n = p + \lambda m_i$ that can be rewritten in

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

Remarks :

- All modules smaller than $\sqrt{n}$ except those of n's euclidean decomposition appear in third column (for modules that divide n, first and second pass eliminate same numbers).
- The same module can't be found on the same line in second and third column.

Gauss's Disquisitiones arithmeticae : Article 127

- **Lemma :**

  "In progression $1, 2, 3, 4, \ldots, n$, there can't be more terms divisibles by any number h, than in progression $a, a+1, a+2, \ldots, a+n-1$ that has the same number of terms."

- "Indeed, we see without pain that
  - if n is divisible by h, there are in each progression $\frac{n}{h}$ terms divisibles by h ;
  - else let $n = he + f$, f being $< h$; there will be in the first serie e terms, and in the second one e or $e + 1$ terms divisibles by h."

Gauss's Disquisitiones arithmeticae : Article 127

- "It follows from this, as a corollary, that $\frac{a(a+1)(a+2)(a+3)...(a+n-1)}{1.2.3...n}$ is always an integer : proposition known by figurated numbers theory, but that was, if I'm right, never demonstrated by no one.

- Finally we could have presented more generally this lemma as following :
  In the progression $a, a+1, a+2 \ldots a+n-1$, there are at least as many terms congruent modulo h to any given number, than there are terms divisibles by h in the progression $1, 2, 3 \ldots n$."

Precisions about lemma's differents cases

- Let us note n mod p the rest of the division of n by p.
- From 1 to n, there are $\left\lfloor \frac{n}{p} \right\rfloor$ numbers congruent to $0\ (mod\ p)$.
- And if $2n \not\equiv 0\ (mod\ p)$, from 1 to n,
  - there are $\left\lfloor \frac{n}{p} \right\rfloor$ numbers congruent to $2n\ (mod\ p)$
    $$\Leftrightarrow\ n \bmod p < 2n \bmod p\ ;$$
  - there are $\left\lfloor \frac{n}{p} \right\rfloor + 1$ numbers congruent to $2n\ (mod\ p)$
    $$\Leftrightarrow\ n \bmod p > 2n \bmod p.$$

How can we generalize article 127 Gauss's lemma ?

- We don't know how to extend this knowledge provided by article 127 lemma (precised or not by the knowledge about n's modular residues) to several modules because we don't know how cases combine themselves.

- However, can we produce a result ?

Computations

- Between 1 and $n/2$, there are less numbers whose complementary to n is prime than there are primes.
- During the second pass, each module that divides n brings no number elimination.
- There are nearly the same quantity of numbers eliminated by second pass of the algorithm than by the first pass.
- There are nearly as many primes of $6k+1$ form than there are of $6k-1$ form (it seems that less than half of them are of $6k+1$ form).
- We should have to be able to compute the quantity of numbers that are eliminated simultaneously by the two passes.