Goldbach conjecture (1742, june, the 7^{th})

- We note $\mathbb{P}$ the prime numbers set.
  $\mathbb{P} = \{p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots\}$
- *remark* : $1 \notin \mathbb{P}$

Statement :

- Each even number greater than 2 is the sum of two prime numbers.
  $\forall n \in 2\mathbb{N}, n > 2, \exists p, q \in \mathbb{P}, n = p + q$

- p and q are called *n's Goldbach components*.

Recalls

- Prime numbers greater than 3 are of $6k \pm 1$ form.
- n being an even number greater than 2 can't be a prime number square that is odd.
- n's Goldbach components n are to be found among multiplicative group $(\mathbb{Z}/n\mathbb{Z}, \times)$ units. These units are coprime to n, they are in even quantity and half of them are smaller than or equal to $n/2$.

Recalls

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

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

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

An algorithm to obtain an even number's Goldbach components

- It's a process that permits to obtain a set of numbers that are n's Goldbach components.
- Let us note m_i $(i = 1, \ldots, j(n))$, prime numbers $3 < m_i \leq \sqrt{n}$.
- 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 prime numbers 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 prime numbers smaller than $\sqrt{n}$, but in keeping prime numbers 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 number 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 number 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.

Using Gold and Tucker notation in their article "On a conjecture of Erdös" about covering system of congruences

- Proving that n allways admits a Goldbach component consists in proving that :

$$\left\{ \bigcup_{m_i\ prime,\ m_i=2}^{m_i<\sqrt{n}} [0, r_i]\ mod\ m_i \right\} \text{doesn't cover interval } [3, n/2].$$