An algorithm to obtain an even number's Goldbach components

Denise Vella-Chemla

2012, December

1 Preliminaries

Goldbach conjecture states that any even integer n greater than 2 can be expressed as a sum of two prime numbers. These prime numbers p and q are called the Goldbach components of n. We assume here that Goldbach conjecture holds.

Let us remind four facts :

1) Prime numbers greater than 3 are of the form $6k \pm 1$.

2) n being an even number greater than 2 cannot be the square of a prime number which is odd. If $p_1, p_2, \ldots, p_r$ are prime numbers greater than $\sqrt{n}$, one of them at most (perhaps none) belongs to the Euclidean decomposition of n into prime numbers since the product of two of them is greater than n.

3) The n's Goldbach components are to be found among units of the multiplicative group $(\mathbb{Z}/n\mathbb{Z}, \times)$. These units are coprime to n, their quantity is an even number and half of them are smaller than or equal to $n/2$.

4) If a prime number $p \leq n/2$ is congruent to n modulo a prime number $m_i < \sqrt{n}$ $(n = p + \lambda m_i)$, its complementary to n, q, is composite because $q = n - p = \lambda m_i$ is congruent to 0 $(mod\ m_i)$. In that case, the prime number p can't be a Goldbach component of n.

2 Algorithm

Taking into account these elementary facts gives rise to a procedure from which one obtains a set of prime numbers that are Goldbach components of n.

We shall denote m_i $(i = 1, \ldots, j(n))$, the prime numbers $3 < m_i \leq \sqrt{n}$.

The procedure consists in first ruling out numbers $p \leq n/2$ congruent to 0 $(mod\ m_i)$ then in cancelling numbers p congruent to n $(mod\ m_i)$.

For this purpose of elimination, the sieve of Eratosthenes will be used.

3 Case study

Let us apply the procedure to the even number $n = 500$.

Let us first note that $500 \equiv 2$ $(mod\ 3)$. Since $6k - 1 = 3k' + 2$, all prime numbers of the form $6k - 1$ are congruent to 500 $(mod\ 3)$, so that their complementary to 500 is composite. We do not have to take these numbers into account. Thus we only consider $\left\lfloor \dfrac{500}{12} \right\rfloor$ numbers of the form $6k + 1$ smaller than or equal to 500/2. They run from 7 to 247 (first column of the table).

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

The second column of the table provides the result of the sieve's first pass : it cancels numbers congruent to 0 $(mod\ m_i)$ for any i.

The third column of the table provides the result of the sieve's second pass : it cancels numbers congruent to n $(mod\ m_i)$ for any i.

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).

$500 = 2^2.5^3$. Module 5 doesn't appear in third column.

The same module can't be found on the same line in second and third column.

500 is congruent to 0 (mod 5), 3 (mod 7), 5 (mod 11), 6 (mod 13), 7 (mod 17) and 6 (mod 19).

$a_k = 6k+1$	*congruence(s) to 0 eliminating* a_k	*congruence(s) to* r $\neq 0$ *eliminating* a_k (*i.e. congruence(s) to* n)	n-a_k	*remaining numbers*
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	

Remark : let us go back on the first part of the algorithm, to rule out numbers p congruent to 0 (mod m_i) for any i. As a result, it cancels all the composite numbers with any m_i in their Euclidean decomposition, eventually including n, cancels all the prime numbers smaller than $\sqrt{n}$, but keeps all the prime numbers greater than $\sqrt{n}$ which is smaller than $n/4+1$.

The second part of the algorithm rules out the numbers p whose complementary to n is composite because they share a congruence with n ($p \equiv n$ (mod m_i) for any i). The second part of the algorithm rules out the numbers p of the form $n = p + \lambda_i m_i$ for any i. If $n = \mu_i m_i$, no such prime number can satisfy the previous relation. Since n is even, $\mu_i = 2\nu_i$, the conjecture implies $\nu_i = 1$. In case when $n \neq \mu_i m_i$, the conjecture implies that there exists a prime number p such that, for some i, $n = p + \lambda_i m_i$, which can be written as $n \equiv p \ (mod\ m_i)$ *or* $n - p \equiv 0 \ (mod\ m_i)$.

First and second passes can be led independently.

Bibiographie

[1] **C.F. Gauss**, *Recherches arithmétiques*, 1807, Ed. Jacques Gabay, 1989.

[2] **J.F. Gold, D.H. Tucker**, *On A Conjecture of Erdös*, Proceedings-NCUR VIII. (1994), Vol.II, pp.794-798.