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 primes. These primes p and q are called the Goldbach components of n. We assume here that Goldbach conjecture holds.

Let us remind four facts :

1) Primes greater than 3 are of the form $6k \pm 1$ ($k \geq 1$).

2) n being an even number greater than 4 cannot be the square of an odd prime which is odd. If $p_1, p_2, \ldots, p_r$ are primes greater than $\sqrt{n}$, one of them at most (perhaps none) belongs to the Euclidean decomposition of n into primes since the product of two of them is greater than n.

3) The n's Goldbach components 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 $n/2$.

4) If a prime $p \leq n/2$ is congruent to n modulo a prime $m_i < \sqrt{n}$ ($n = p + \lambda m_i$), 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 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 primes that are Goldbach components of n.

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

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 primes 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 primes smaller than $\sqrt{n}$, but keeps all the primes 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 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 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.

4 Gauss's Disquisitiones arithmeticae : Article 127's lemma

In article 127 of Disquisitiones arithmeticae, one can find the following lemma :

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

Gauss gives after the following demonstration :

"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."

"It follows from this, as a corollary, that $\frac{a(a+1)(a+2)(a+3)\dots(a+n-1)}{1.2.3\dots n}$ 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 $a, a+1, a+2 \dots a+n-1$, there are at least as many terms congruent modulo h to any given number, than there are terms divisibles by h in the progression $1, 2, 3 \dots n$."

We can give some precisions about Gauss article 127 lemma's differents cases.

Let us note $n \bmod p$ 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 $2n \ (mod\ p) \Leftrightarrow\ n \bmod p > 2n \bmod p$.

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

5 Computations

Even if we don't know how to extend article 127 Gauss's lemma in more than one modulo cases, we can however make some computations :

Between 1 and $n/2$, there are less numbers whose complementary to n is prime than 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.

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.