An algorithm to obtain an even number's Goldbach components, décembre 2012.

transparents CG.

english slides, GC.

Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair, décembre 2012.

transparents.

tableaux colorés.

Application double du crible d'Eratosthène pour trouver les décomposants de Goldbach d'un nombre pair.

Minorer le nombre de décomposants de Goldbach, avril 2013.

Théorie des groupes et Conjecture de Goldbach, janvier 2013.

Application double du crible d'Eratosthène pour trouver les décomposants de Goldbach d'un nombre pair, décembre 2012.

C'est extra !, novembre 2012.

Tableaux colorés.

Colored arrays.

Théorie de Galois et Conjecture de Goldbach, février 2013.

Equations polynomiales modulaires et Conjecture de Goldbach.

Expérimentations en GAP.

An algorithm to obtain an even number's Goldbach components, décembre 2012.

slides.

Minorer le nombre de décomposants de Goldbach, mars 2013.

Tentative inaboutie de démonstration par récurrence de la conjecture de Goldbach.

transparents.

bijection de Cantor.

Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair, décembre 2012.

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 $\left\lfloor \frac{500}{12} \right\rfloor$ 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.

Les décomposants de Goldbach d'un nombre pair sont systématiquement indiqués entre parenthèses après ce nombre, précédés des lettres DG.

1 Nombres pairs de forme $6k$ de 144 à 30

L'application du double crible est présentée dans un tableau coupé en deux dans le sens de la hauteur, les nombres de la partie haute du tableau appartenant à la progression $6x-1$ tandis que ceux de la partie basse du tableau appartiennent à la progression $6k+1$.

On note dans la deuxième colonne le ré sultat du passage de la première passe du crible (élimination des nombres congrus à 0 selon un module inférieur ou égal à $\sqrt{x}$).

On note dans la troisième colonne le résultat du passage de la seconde passe du crible en spécifiant la congruence partagée avec x.

On note dans les quatrième et cinquième colonnes les nombres de l'intervalle translaté et leurs congruences à 0 en bijection avec les congruences à $r \neq 0$ de la troisième colonne.

- $x = 144$ $\quad (DG : 5, 7, 13, 17, 31, 37, 41, 43, 47, 61, 71)$

  $x/2 = 72$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 4\ (mod\ 5), x \equiv 4\ (mod\ 7), x \equiv 1\ (mod\ 11)$.

5	$0\ (mod\ 5)$		2171	
11	$0\ (mod\ 11)$	$4\ (mod\ 7)$	2177	$0\ (mod\ 7)$
17			2183	
23		$1\ (mod\ 11)$	2189	$0\ (mod\ 11)$
29		$4\ (mod\ 5)$	2195	$0\ (mod\ 5)$
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		2201	
41			2207	
47			2213	
53		$4\ (mod\ 7)$	2219	$0\ (mod\ 7)$
59		$4\ (mod\ 5)$	2225	$0\ (mod\ 5)$
65	$0\ (mod\ 5)$		2231	
71			2237	
7	$0\ (mod\ 7)$		2173	
13			2179	
19		$4\ (mod\ 5)$	2185	$0\ (mod\ 5)$
25	$0\ (mod\ 5)$	$4\ (mod\ 7)$	2191	$0\ (mod\ 7)$
31			2197	
37			2203	
43			2209	
49	$0\ (mod\ 7)$	$4\ (mod\ 5)$	2215	$0\ (mod\ 5)$
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		222	
61			2227	
67		$4\ (mod\ 7)$ *et* $1\ (mod\ 11)$	2233	$0\ (mod\ 7)$ *et* $0\ (mod\ 11)$

- $x = 138$ $\quad (DG : 7, 11, 29, 31, 37, 41, 59, 67)$

  $x/2 = 69$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 3\ (mod\ 5), x \equiv 5\ (mod\ 7), x \equiv 6\ (mod\ 11)$.

5	$0\ (mod\ 5)$	$5\ (mod\ 7)$	2177	$0\ (mod\ 7)$
11	$0\ (mod\ 11)$		2183	
17		$6\ (mod\ 11)$	2189	$0\ (mod\ 11)$
23		$3\ (mod\ 5)$	2195	$0\ (mod\ 5)$
29			2201	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$	2207		
41			2213	
47		$5\ (mod\ 7)$	2219	$0\ (mod\ 7)$
53		$3\ (mod\ 5)$	2225	$0\ (mod\ 5)$
59			2231	
65	$0\ (mod\ 5)$		2237	
7	$0\ (mod\ 7)$		2179	
13		$3\ (mod\ 5)$	2185	$0\ (mod\ 5)$
19		$5\ (mod\ 7)$	2191	$0\ (mod\ 7)$
25	$0\ (mod\ 5)$		2197	
31			2203	
37			2209	
43		$3\ (mod\ 5)$	2215	$0\ (mod\ 5)$
49	$0\ (mod\ 7)$		2221	
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		2227	
61		$5\ (mod\ 7)$ *et* $6\ (mod\ 11)$	2233	$0\ (mod\ 7)$ *et* $0\ (mod\ 11)$
67			2239	

- $x = 132$ $\quad (DG : 5, 19, 23, 29, 31, 43, 53, 59, 61)$

  $x/2 = 66$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 2\ (mod\ 5), x \equiv 6\ (mod\ 7), x \equiv 0\ (mod\ 11)$.

5	$0\ (mod\ 5)$		83	
11	$0\ (mod\ 11)$		89	
17		$2\ (mod\ 5)$	95	$0\ (mod\ 5)$
23			101	
29			107	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		113	
41		$6\ (mod\ 7)$	119	$0\ (mod\ 7)$
47		$2\ (mod\ 5)$	125	$0\ (mod\ 5)$
53			131	
59			137	
65	$0\ (mod\ 5)$		143	
7	$0\ (mod\ 7)$	$2\ (mod\ 5)$	85	$0\ (mod\ 5)$
13		$6\ (mod\ 7)$	91	$0\ (mod\ 7)$
19			97	
25	$0\ (mod\ 5)$		103	
31			109	
37		$2\ (mod\ 5)$	115	$0\ (mod\ 5)$
43			121	
49	$0\ (mod\ 7)$		127	
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		133	
61			139	

- $x = 126$ $\quad (DG : 13, 17, 19, 23, 29, 37, 43, 47, 53, 59)$

  $x/2 = 63$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers $5,\ 7$ *et* 11.
  $x \equiv 1\ (mod\ 5), x \equiv 0\ (mod\ 7), x \equiv 5\ (mod\ 11)$.

5	$0\ (mod\ 5)$	$5\ (mod\ 11)$	209	$0\ (mod\ 11)$
11	$0\ (mod\ 11)$	$1\ (mod\ 5)$	215	$0\ (mod\ 5)$
17			221	
23			227	
29			233	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		239	
41		$1\ (mod\ 5)$	245	$0\ (mod\ 5)$
47			251	
53			257	
59			263	
7	$0\ (mod\ 7)$		211	
13			217	
19			223	
25	$0\ (mod\ 5)$		229	
31		$1\ (mod\ 5)$	235	$0\ (mod\ 5)$
37			241	
43			247	
49	$0\ (mod\ 7)$	$5\ (mod\ 11)$	253	$0\ (mod\ 11)$
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		259	
61		$1\ (mod\ 5)$	265	$0\ (mod\ 5)$

- $x = 120$ $\quad (DG : 7, 11, 13, 17, 19, 23, 31, 37, 41, 47, 53, 59)$

  $x/2 = 60$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 0\ (mod\ 5), x \equiv 1\ (mod\ 7)$.

5	$0\ (mod\ 5)$		11	
11			17	
17			23	
23			29	
29		$1\ (mod\ 7)$	35	$0\ (mod\ 7)$
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$	41		
41			47	
47			53	
53			59	
59			65	
7	$0\ (mod\ 7)$		-29	
13			-23	
19			-17	
25	$0\ (mod\ 5)$		-11	
31			-5	
37			1	
43		$1\ (mod\ 7)$	7	$0\ (mod\ 7)$
49	$0\ (mod\ 7)$		13	
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		19	

- $x = 114$ $(DG : 5, 7, 11, 13, 17, 31, 41, 43, 47, 53)$

  $x/2 = 57$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 4\ (mod\ 5), x \equiv 2\ (mod\ 7)$.

5	$0\ (mod\ 5)$		101	
11			107	
17			113	
23		$2\ (mod\ 7)$	119	$0\ (mod\ 7)$
29		$4\ (mod\ 5)$	125	$0\ (mod\ 5)$
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		131	
41			137	
47			143	
53			149	
7	$0\ (mod\ 7)$		103	
13			109	
19		$4\ (mod\ 5)$	115	$0\ (mod\ 5)$
25	$0\ (mod\ 5)$		121	
31			127	
37		$2\ (mod\ 7)$	133	$0\ (mod\ 7)$
43			139	
49	$0\ (mod\ 7)$	$4\ (mod\ 5)$	145	$0\ (mod\ 5)$
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		151	

- $x = 108$ $(DG : 5, 7, 11, 19, 29, 37, 41, 47)$

  $x/2 = 54$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 3\ (mod\ 5), x \equiv 3\ (mod\ 7)$.

5	$0\ (mod\ 5)$		107	
11			113	
17		$3\ (mod\ 7)$	119	$0\ (mod\ 7)$
23		$3\ (mod\ 5)$	125	$0\ (mod\ 5)$
29			131	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		137	
41			143	
47			149	
53		$3\ (mod\ 5)$	155	$0\ (mod\ 5)$
7	$0\ (mod\ 7)$		109	
13		$3\ (mod\ 5)$	115	$0\ (mod\ 5)$
19			121	
25	$0\ (mod\ 5)$		127	
31		$3\ (mod\ 7)$	133	$0\ (mod\ 7)$
37			139	
43		$3\ (mod\ 5)$	145	$0\ (mod\ 5)$
49	$0\ (mod\ 7)$		151	

- $x = 102$ $\quad (DG : 5, 13, 19, 23, 29, 31, 41, 43)$

  $x/2 = 51$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 2\ (mod\ 5), x \equiv 4\ (mod\ 7)$.

5	$0\ (mod\ 5)$		113	
11		$4\ (mod\ 7)$	119	$0\ (mod\ 7)$
17		$2\ (mod\ 5)$	125	$0\ (mod\ 5)$
23			131	
29			137	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		143	
41			149	
47		$2\ (mod\ 5)$	155	$0\ (mod\ 5)$
7	$0\ (mod\ 7)$	$2\ (mod\ 5)$	115	$0\ (mod\ 5)$
13			121	
19			127	
25	$0\ (mod\ 5)$	$4\ (mod\ 7)$	133	$0\ (mod\ 7)$
31			139	
37		$2\ (mod\ 5)$	145	$0\ (mod\ 5)$
43			151	
49	$0\ (mod\ 7)$		157	

- $x = 96$ $\quad (DG : 7, 13, 17, 23, 29, 37, 43)$

  $x/2 = 48$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 1\ (mod\ 5), x \equiv 5\ (mod\ 7)$.

5	$0\ (mod\ 5)$	$5\ (mod\ 7)$	119	$0\ (mod\ 7)$
11		$1\ (mod\ 5)$	125	$0\ (mod\ 5)$
17			131	
23			137	
29			143	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		149	
41		$1\ (mod\ 5)$	155	$0\ (mod\ 5)$
47		$5\ (mod\ 7)$	161	$0\ (mod\ 7)$
7	$0\ (mod\ 7)$		121	
13			127	
19		$5\ (mod\ 7)$	133	$0\ (mod\ 7)$
25	$0\ (mod\ 5)$		139	
31		$1\ (mod\ 5)$	145	$0\ (mod\ 5)$
37			151	
43			157	

- $x = 90$ $(DG : 7, 11, 17, 19, 23, 29, 31, 37, 43)$

  $x/2 = 45$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 0\ (mod\ 5), x \equiv 6\ (mod\ 7)$.

5	$0\ (mod\ 5)$		-1	
11			5	
17			11	
23			17	
29			23	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		29	
41		$6\ (mod\ 7)$	35	$0\ (mod\ 7)$
7	$0\ (mod\ 7)$		1	
13		$6\ (mod\ 7)$	7	$0\ (mod\ 7)$
19			13	
25	$0\ (mod\ 5)$		19	
31			25	
37			31	
43			37	

- $x = 84$ $(DG : 5, 11, 13, 17, 23, 31, 37, 41)$

  $x/2 = 42$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 4\ (mod\ 5), x \equiv 0\ (mod\ 7)$.

5	$0\ (mod\ 5)$		-19	
11			-13	
17			-7	
23			-1	
29		$4\ (mod\ 5)$	5	$0\ (mod\ 5)$
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		11	
41			17	
7	$0\ (mod\ 7)$		13	
13			19	
19		$4\ (mod\ 5)$	25	$0\ (mod\ 5)$
25	$0\ (mod\ 5)$		31	
31			37	
37			43	

- $x = 78$ $(DG : 5, 7, 11, 17, 19, 31, 37)$

  $x/2 = 39$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 3\ (mod\ 5), x \equiv 1\ (mod\ 7)$.

5	$0\ (mod\ 5)$		137	
11			143	
17			149	
23		$3\ (mod\ 5)$	155	$0\ (mod\ 5)$
29		$1\ (mod\ 7)$	161	$0\ (mod\ 7)$
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		167	
7	$0\ (mod\ 7)$		19	
13		$3\ (mod\ 5)$	25	$0\ (mod\ 5)$
19			31	
25	$0\ (mod\ 5)$		37	
31			43	
37			49	

- $x = 72$ $(DG : 5, 11, 13, 19, 29, 31)$

  $x/2 = 36$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 2\ (mod\ 5), x \equiv 2\ (mod\ 7)$.

5	$0\ (mod\ 5)$		143	
11			149	
17		$2\ (mod\ 5)$	155	$0\ (mod\ 5)$
23		$2\ (mod\ 7)$	161	$0\ (mod\ 7)$
29			167	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		173	
7	$0\ (mod\ 7)$	$2\ (mod\ 5)$	25	$0\ (mod\ 5)$
13			31	
19			37	
25	$0\ (mod\ 5)$		43	
31			49	

- $x = 66$ $(DG : 5, 7, 13, 19, 23, 29)$

  $x/2 = 33$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 1\ (mod\ 5), x \equiv 3\ (mod\ 7)$.

5	$0\ (mod\ 5)$		149	
11		$1\ (mod\ 5)$	155	$0\ (mod\ 5)$
17		$3\ (mod\ 7)$	161	$0\ (mod\ 7)$
23			167	
29			173	
7	$0\ (mod\ 7)$		151	
13			157	
19			163	
25	$0\ (mod\ 5)$		169	
31		$1\ (mod\ 5)$ *et* $3\ (mod\ 7)$	175	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$

- $x = 60$ $(DG : 7, 13, 17, 19, 23, 29)$

  $x/2 = 30$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 0\ (mod\ 5), x \equiv 4\ (mod\ 7)$.

5	$0\ (mod\ 5)$		29	
11		$4\ (mod\ 7)$	35	$0\ (mod\ 7)$
17			41	
23			47	
29			53	
7	$0\ (mod\ 7)$		-11	
13			-5	
19			1	
25	$0\ (mod\ 5)$	$4\ (mod\ 7)$	7	$0\ (mod\ 7)$

- $x = 54$ $(DG : 7, 11, 13, 17, 23)$

  $x/2 = 27$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 4\ (mod\ 5), x \equiv 5\ (mod\ 7)$.

5	$0\ (mod\ 5)$	$5\ (mod\ 7)$	35	$0\ (mod\ 7)$
11			41	
17			47	
23			53	
7	$0\ (mod\ 7)$		163	
13			169	
19		$4\ (mod\ 5)$ *et* $5\ (mod\ 7)$	175	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$
25	$0\ (mod\ 5)$		181	

- $x = 48$ $(DG : 5, 7, 11, 17, 19)$

  $x/2 = 24$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 3\ (mod\ 5)$.

5	$0\ (mod\ 5)$		-13	
11			-7	
17			-1	
23		$3\ (mod\ 5)$	5	$0\ (mod\ 5)$
7			19	
13		$3\ (mod\ 5)$	25	$0\ (mod\ 5)$
19			31	

- $x = 42$ $(DG : 5, 11, 13, 19)$

  $x/2 = 21$.
  $5 < \sqrt{x} < 5$. On s'intéresse au module premier 5.
  $x \equiv 2\ (mod\ 5)$.

5	$0\ (mod\ 5)$		-7	
11			-1	
17		$2\ (mod\ 5)$	5	$0\ (mod\ 5)$
7		$2\ (mod\ 5)$	25	$0\ (mod\ 5)$
13			31	
19			37	

- $x = 36$ $(DG : 5, 7, 13, 17)$

  $x/2 = 18$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 1\ (mod\ 5)$.

5	$0\ (mod\ 5)$		-1	
11		$1\ (mod\ 5)$	5	$0\ (mod\ 5)$
17			11	
7				
13				

- $x = 30$ $(DG : 7, 11, 13)$

  $x/2 = 15$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 0\ (mod\ 5)$.

5	$0\ (mod\ 5)$			
11				
7				
13				

2 Nombres pairs de forme $6k + 4$ de 142 à 28

L'application du double crible est présentée dans un tableau ne contenant que des nombres appartenant à la progression $6x - 1$.

- $x = 142$ $(DG : 3, 5, 11, 29, 41, 53, 59, 71)$

  $x/2 = 71$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 2\ (mod\ 5), x \equiv 2\ (mod\ 7), x \equiv 10\ (mod\ 11)$.

5	$0\ (mod\ 5)$		1403	
11	$0\ (mod\ 11)$		1409	
17		$2\ (mod\ 5)$	1415	$0\ (mod\ 5)$
23		$2\ (mod\ 7)$	1421	$0\ (mod\ 7)$
29			1427	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		1433	
41			1439	
47		$2\ (mod\ 5)$	1445	$0\ (mod\ 5)$
53			1451	
59			1457	
65	$0\ (mod\ 5)$	$2\ (mod\ 7)$ *et* $10\ (mod\ 11)$	1463	$0\ (mod\ 7)$ *et* $0\ (mod\ 11)$
71			1469	

- $x = 136$ $(DG : 5, 23, 29, 47, 53)$

  $x/2 = 68$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 1\ (mod\ 5), x \equiv 3\ (mod\ 7), x \equiv 4\ (mod\ 11)$.

5	$0\ (mod\ 5)$		1409	
11	$0\ (mod\ 11)$	$1\ (mod\ 5)$	1415	$0\ (mod\ 5)$
17		$3\ (mod\ 7)$	1421	$0\ (mod\ 7)$
23			1427	
29			1433	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		1439	
41		$1\ (mod\ 5)$	1445	$0\ (mod\ 5)$
47			1451	
53			1457	
59		$3\ (mod\ 7)$ *et* $4\ (mod\ 11)$	1463	$0\ (mod\ 7)$ *et* $0\ (mod\ 11)$
65	$0\ (mod\ 5)$		1469	

- $x = 130$ $(DG : 3, 17, 23, 29, 41, 47, 59)$

  $x/2 = 65$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 0\ (mod\ 5), x \equiv 4\ (mod\ 7), x \equiv 9\ (mod\ 11)$.

5	$0\ (mod\ 5)$		29	
11	$0\ (mod\ 11)$	$4\ (mod\ 7)$	35	$0\ (mod\ 7)$
17			41	
23			47	
29			53	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		59	
41			65	
47			71	
53		$4\ (mod\ 7)$ *et* $9\ (mod\ 11)$	77	$0\ (mod\ 7)$ *et* $0\ (mod\ 11)$
59			83	
65	$0\ (mod\ 5)$		89	

- $x = 124$ $(DG : 11, 17, 23, 41, 53)$

  $x/2 = 62$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 4\ (mod\ 5), x \equiv 5\ (mod\ 7), x \equiv 3\ (mod\ 11)$.

5	$0\ (mod\ 5)$	$5\ (mod\ 7)$	1421	$0\ (mod\ 7)$
11	$0\ (mod\ 11)$		1427	
17			1433	
23			1439	
29		$4\ (mod\ 5)$	1445	$0\ (mod\ 5)$
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		1451	
41			1457	
47		$5\ (mod\ 7)$ *et* $3\ (mod\ 11)$	1463	$0\ (mod\ 7)$ *et* $0\ (mod\ 11)$
53			1469	
59		$4\ (mod\ 5)$	1475	$0\ (mod\ 5)$

- $x = 118$ $(DG : 5, 11, 17, 29, 47, 59)$

  $x/2 = 99$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 3\ (mod\ 5), x \equiv 6\ (mod\ 7)$.

5	$0\ (mod\ 5)$		167	
11			173	
17			179	
23		$3\ (mod\ 5)$	185	$0\ (mod\ 5)$
29			191	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		197	
41		$6\ (mod\ 7)$	203	$0\ (mod\ 7)$
47			209	
53		$3\ (mod\ 5)$	215	$0\ (mod\ 5)$
59			221	

- $x = 112$ $(DG : 3, 5, 11, 23, 29, 41, 53)$

  $x/2 = 56$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 2\ (mod\ 5), x \equiv 0\ (mod\ 7)$.

5	$0\ (mod\ 5)$		-7	
11			-1	
17		$2\ (mod\ 5)$	5	$0\ (mod\ 5)$
23			11	
29			17	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		23	
41			29	
47		$2\ (mod\ 5)$	35	$0\ (mod\ 5)$
53			41	

- $x = 106$ $(DG : 3, 5, 17, 23, 47, 53)$

  $x/2 = 53$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 1\ (mod\ 5), x \equiv 1\ (mod\ 7)$.

5	$0\ (mod\ 5)$		179	
11		$1\ (mod\ 5)$	185	$0\ (mod\ 5)$
17			191	
23			197	
29		$1\ (mod\ 7)$	203	$0\ (mod\ 7)$
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		209	
41		$1\ (mod\ 5)$	215	$0\ (mod\ 5)$
47			221	
53			227	

- $x = 100$ $(DG : 3, 11, 17, 29, 41, 47)$

  $x/2 = 50$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 0\ (mod\ 5), x \equiv 2\ (mod\ 7)$.

5	$0\ (mod\ 5)$		17	
11			23	
17			29	
23		$2\ (mod\ 7)$	35	$0\ (mod\ 7)$
29			41	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		47	
41			53	
47			59	

- $x = 94$ $(DG : 5, 11, 23, 41, 47)$

  $x/2 = 47$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 4\ (mod\ 5), x \equiv 3\ (mod\ 7)$.

5	$0\ (mod\ 5)$		191	
11			197	
17		$3\ (mod\ 7)$	203	$0\ (mod\ 7)$
23			209	
29		$4\ (mod\ 5)$	215	$0\ (mod\ 5)$
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		221	
41			227	
47			233	

- $x = 88$ $(DG : 5, 17, 29, 41)$

  $x/2 = 44$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 3\ (mod\ 5), x \equiv 4\ (mod\ 7)$.

5	$0\ (mod\ 5)$		197	
11		$4\ (mod\ 7)$	203	$0\ (mod\ 7)$
17			209	
23		$3\ (mod\ 5)$	215	$0\ (mod\ 5)$
29			221	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		227	
41			233	

- $x = 82$ $(DG : 3, 11, 23, 29, 41)$

  $x/2 = 41$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 2\ (mod\ 5), x \equiv 5\ (mod\ 7)$.

5	$0\ (mod\ 5)$	$5\ (mod\ 7)$	203	$0\ (mod\ 7)$
11			209	
17		$2\ (mod\ 5)$	215	$0\ (mod\ 5)$
23			221	
29			227	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		233	
41			239	

- $x = 76$ $(DG : 3, 5, 17, 23, 29)$

  $x/2 = 38$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 1\ (mod\ 5), x \equiv 6\ (mod\ 7)$.

5	$0\ (mod\ 5)$		-1	
11		$1\ (mod\ 5)$	5	$0\ (mod\ 5)$
17			11	
23			17	
29			23	
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$		29	

- $x = 70$ $(DG : 3, 11, 17, 23, 29)$

  $x/2 = 35$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 0\ (mod\ 5), x \equiv 0\ (mod\ 7)$.

5	$0\ (mod\ 5)$			
11				
17				
23				
29				
35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$			

- $x = 64$ $(DG : 3, 5, 11, 17, 23)$

  $x/2 = 32$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 4\ (mod\ 5), x \equiv 1\ (mod\ 7)$.

5	$0\ (mod\ 5)$		11	
11			17	
17			23	
23			29	
29		$4\ (mod\ 5)$ *et* $1\ (mod\ 7)$	35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$

- $x = 58$ $(DG : 5, 11, 17, 29)$

  $x/2 = 29$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 3\ (mod\ 5), x \equiv 2\ (mod\ 7)$.

5	$0\ (mod\ 5)$		17	
11			23	
17			29	
23		$3\ (mod\ 5)$ *et* $2\ (mod\ 7)$	35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$
29			41	

- $x = 52$ $(DG : 5, 11, 23)$

  $x/2 = 26$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 2\ (mod\ 5), x \equiv 3\ (mod\ 7)$.

5	$0\ (mod\ 5)$		23	
11			29	
17		$2\ (mod\ 5)$ *et* $3\ (mod\ 7)$	35	$0\ (mod\ 5)$ *et* $0\ (mod\ 7)$
23			41	

- $x = 46$ $(DG : 3, 5, 17, 23)$

  $x/2 = 23$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 1\ (mod\ 5)$.

5	$0\ (mod\ 5)$		-1	
11		$1\ (mod\ 5)$	5	$0\ (mod\ 5)$
17			11	
23			17	

- $x = 40$ $(DG : 3, 11, 17)$

  $x/2 = 20$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 0\ (mod\ 5)$.

5	$0\ (mod\ 5)$			
11				
17				

- $x = 34$ $(DG : 3, 5, 11, 17)$

  $x/2 = 17$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 4\ (mod\ 5)$.

5	$0\ (mod\ 5)$			
11				
17				

- $x = 28$ $(DG : 5, 11)$

  $x/2 = 14$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 3\ (mod\ 5)$.

5	$0\ (mod\ 5)$			
11				

3 Nombres pairs de forme $6k + 2$ de 140 à 26

L'application du double crible est présentée dans un tableau ne contenant que des nombres appartenant à la progression $6k + 1$.

- $x = 140$ $(DG : 3, 13, 31, 37, 43, 61, 67)$

  $x/2 = 70$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 0\ (mod\ 5), x \equiv 0\ (mod\ 7), x \equiv 8\ (mod\ 11)$.

7	$0\ (mod\ 7)$		43	
13			49	
19		$8\ (mod\ 11)$	55	$0\ (mod\ 11)$
25	$0\ (mod\ 5)$		61	
31			67	
37			73	
43			79	
49	$0\ (mod\ 7)$		85	
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		91	
61			97	
67			103	

- $x = 134$ $(DG : 3, 7, 31, 37, 61, 67)$

  $x/2 = 67$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 4\ (mod\ 5), x \equiv 1\ (mod\ 7), x \equiv 2\ (mod\ 11)$.

7	$0\ (mod\ 7)$		643	
13		$2\ (mod\ 11)$	649	$0\ (mod\ 11)$
19		$4\ (mod\ 5)$	655	$0\ (mod\ 5)$
25	$0\ (mod\ 5)$		661	
31			667	
37			673	
43		$1\ (mod\ 7)$	679	$0\ (mod\ 7)$
49	$0\ (mod\ 7)$	$4\ (mod\ 5)$	685	$0\ (mod\ 5)$
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		691	
61			697	
67			703	

- $x = 128$ $\quad (DG : 19, 31, 61)$

  $x/2 = 64$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 3\ (mod\ 5), x \equiv 2\ (mod\ 7), x \equiv 7\ (mod\ 11)$.

7	$0\ (mod\ 7)$	$7\ (mod\ 11)$	649	$0\ (mod\ 11)$
13		$3\ (mod\ 5)$	655	$3\ (mod\ 5)$
19			661	
25	$0\ (mod\ 5)$		667	
31			673	
37		$2\ (mod\ 7)$	679	$0\ (mod\ 7)$
43		$3\ (mod\ 5)$	685	$0\ (mod\ 5)$
49	$0\ (mod\ 7)$		691	
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		697	
61			703	

- $x = 122$ $\quad (DG : 13, 19, 43, 61)$

  $x/2 = 61$.
  $11 < \sqrt{x} < 13$. On s'intéresse aux modules premiers 5, 7 *et* 11.
  $x \equiv 2\ (mod\ 5), x \equiv 3\ (mod\ 7), x \equiv 1\ (mod\ 11)$.

7	$0\ (mod\ 7)$	$2\ (mod\ 5)$	25	$0\ (mod\ 5)$
13			31	
19			37	
25	$0\ (mod\ 5)$		43	
31		$3\ (mod\ 7)$	49	$0\ (mod\ 7)$
37		$2\ (mod\ 5)$	55	$0\ (mod\ 5)$
43			61	
49	$0\ (mod\ 7)$		67	
55	$0\ (mod\ 5)$		73	
61			79	

- $x = 116$ $\quad (DG : 3, 7, 13, 19, 37, 43)$

  $x/2 = 58$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 1\ (mod\ 5), x \equiv 4\ (mod\ 7)$.

7	$0\ (mod\ 7)$		31	
13			37	
19			43	
25	$0\ (mod\ 5)$	$4\ (mod\ 7)$	49	$0\ (mod\ 7)$
31		$1\ (mod\ 5)$	55	$0\ (mod\ 5)$
37			61	
43			67	
49	$0\ (mod\ 7)$		73	
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		79	

- $x = 110$ $(DG : 3, 7, 13, 31, 37, 43)$

  $x/2 = 55$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 0\ (mod\ 5), x \equiv 5\ (mod\ 7)$.

7	$0\ (mod\ 7)$		-5	
13			1	
19		$5\ (mod\ 7)$	7	$0\ (mod\ 7)$
25	$0\ (mod\ 5)$		13	
31			19	
37			25	
43			31	
49	$0\ (mod\ 7)$		37	
55	$0\ (mod\ 5)$ *et* $0\ (mod\ 11)$		43	

- $x = 104$ $(DG : 3, 7, 31, 37, 43)$

  $x/2 = 52$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 4\ (mod\ 5), x \equiv 6\ (mod\ 7)$.

7	$0\ (mod\ 7)$		43	
13		$6\ (mod\ 7)$	49	$0\ (mod\ 7)$
19		$4\ (mod\ 5)$	55	$0\ (mod\ 5)$
25	$0\ (mod\ 5)$		61	
31			67	
37			73	
43			79	
49	$0\ (mod\ 7)$	$4\ (mod\ 5)$	85	$4\ (mod\ 5)$

- $x = 98$ $(DG : 19, 31, 37)$

  $x/2 = 49$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 3\ (mod\ 5), x \equiv 0\ (mod\ 7)$.

7	$0\ (mod\ 7)$		19	
13		$3\ (mod\ 5)$	25	$0\ (mod\ 5)$
19			31	
25	$0\ (mod\ 5)$		37	
31			43	
37			49	
43		$3\ (mod\ 5)$	55	$0\ (mod\ 5)$
49	$0\ (mod\ 7)$		61	

- $x = 92$ $(DG : 3, 13, 19, 31)$

  $x/2 = 46$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 2\ (mod\ 5), x \equiv 1\ (mod\ 7)$.

7	$0\ (mod\ 7)$	$2\ (mod\ 5)$	55	$0\ (mod\ 5)$
13			61	
19			67	
25	$0\ (mod\ 5)$		73	
31			79	
37		$2\ (mod\ 5)$	85	$0\ (mod\ 5)$
43		$1\ (mod\ 7)$	91	$0\ (mod\ 7)$

- $x = 86$ $(DG : 3, 7, 13, 19, 43)$

  $x/2 = 43$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 1\ (mod\ 5), x \equiv 2\ (mod\ 7)$.

7	$0\ (mod\ 7)$		61	
13			67	
19			73	
25	$0\ (mod\ 5)$		79	
31		$1\ (mod\ 5)$	85	$0\ (mod\ 5)$
37		$2\ (mod\ 7)$	91	$0\ (mod\ 7)$
43			97	

- $x = 80$ $(DG : 7, 13, 19, 37)$

  $x/2 = 40$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 0\ (mod\ 5), x \equiv 3\ (mod\ 7)$.

7	$0\ (mod\ 7)$		-17	
13			-11	
19			-5	
25	$0\ (mod\ 5)$		1	
31		$3\ (mod\ 7)$	7	$0\ (mod\ 7)$
37			13	

- $x = 74$ $(DG : 3, 7, 13, 31, 37)$

  $x/2 = 37$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 4\ (mod\ 5), x \equiv 4\ (mod\ 7)$.

7	$0\ (mod\ 7)$		73	
13			79	
19		$4\ (mod\ 5)$	85	$0\ (mod\ 5)$
25	$0\ (mod\ 5)$	$4\ (mod\ 7)$	91	$0\ (mod\ 7)$
31			97	
37			103	

- $x = 68$ $(DG : 7, 31)$

  $x/2 = 34$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 3\ (mod\ 5), x \equiv 5\ (mod\ 7)$.

7	$0\ (mod\ 7)$		79	
13		$3\ (mod\ 5)$	85	$0\ (mod\ 5)$
19		$5\ (mod\ 7)$	91	$0\ (mod\ 7)$
25	$0\ (mod\ 5)$		97	
31			103	

- $x = 62$ $(DG : 3, 19, 31)$

  $x/2 = 31$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 2\ (mod\ 5), x \equiv 6\ (mod\ 7)$.

7	$0\ (mod\ 7)$	$2\ (mod\ 5)$	85	$0\ (mod\ 5)$
13		$6\ (mod\ 7)$	91	$0\ (mod\ 7)$
19			97	
25	$0\ (mod\ 5)$		103	
31			109	

- $x = 56$ $(DG : 3, 13, 19)$

  $x/2 = 28$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 1\ (mod\ 5), x \equiv 0\ (mod\ 7)$.

7	$0\ (mod\ 7)$			
13				
19				
25	$0\ (mod\ 5)$			

- $x = 50$ $(DG : 3, 7, 13, 19)$

  $x/2 = 25$.
  $7 < \sqrt{x} < 11$. On s'intéresse aux modules premiers 5 *et* 7.
  $x \equiv 0\ (mod\ 5), x \equiv 1\ (mod\ 7)$.

7	$0\ (mod\ 7)$			
13				
19				
25	$0\ (mod\ 5)$			

- $x = 44$ $(DG : 3, 7, 13)$

  $x/2 = 22$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 4\ (mod\ 5)$.

7	$0\ (mod\ 7)$		13	
13			19	
19		$4\ (mod\ 5)$	25	$0\ (mod\ 5)$

- $x = 38$ $(DG : 7, 19)$

  $x/2 = 19$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 3\ (mod\ 5)$.

7	$0\ (mod\ 7)$		19	
13		$3\ (mod\ 5)$	25	$0\ (mod\ 5)$
19			31	

- $x = 32$ $(DG : 3, 13)$

  $x/2 = 16$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 2\ (mod\ 5)$.

7	$0\ (mod\ 7)$	$2\ (mod\ 5)$	25	$0\ (mod\ 5)$
13			31	

- $x = 26$ $(DG : 3, 7, 13)$

  $x/2 = 13$.
  $5 < \sqrt{x} < 7$. On s'intéresse au module premier 5.
  $x \equiv 1\ (mod\ 5)$.

7	$0\ (mod\ 7)$			
13				

Conjecture de Goldbach (7 juin 1742)

- On note $\mathbb{P}$ l'ensemble des nombres premiers.
  $\mathbb{P} = \{p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots\}$
- *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 dits *décomposants de Goldbach* de n.

Rappels

- Les nombres premiers plus grands que 3 sont de la forme $6k \pm 1$.
- n étant un nombre pair plus grand que 2 ne peut être le carré d'un nombre premier qui est impair.
- Les décomposants de Goldbach de n sont à trouver parmi les unités du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z}, \times)$. Ces unités sont premières à n, elles sont en nombre pair et la moitié d'entre elles sont inférieures ou égales 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 à n, q, 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 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 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
    $n \equiv p \ (mod \ m_i)$ *or* $n - p \equiv 0 \ (mod \ m_i)$.

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.

Utiliser la notation de l'article de Gold and Tucker "On a conjecture of Erdös" traitant de systèmes couvrant de congruences

- Prouver que n admet toujours un décomposant de Goldbach consiste à prouver que :

$$\left\{ \bigcup_{m_i \text{ prime},\ m_i=2}^{m_i<\sqrt{n}} [0, r_i] \ mod\ m_i \right\} \text{ ne couvre pas l'intervalle } [3, \mathrm{n}/2].$$

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 :

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

Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair

Denise Vella-Chemla

Décembre 2012

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair n plus grand que 2 est la somme de deux nombres premiers. Ces nombres premiers p et q sont appelés décomposants de Goldbach de n. Assumons ici que la conjecture de Goldbach est vraie.

Rappelons quatre faits :

1) Les nombres premiers plus grands que 3 sont de la forme $6k \pm 1$ ($k \geq 1$).

2) n étant un nombre pair plus grand que 4 ne peut être le carré d'un nombre premier impair qui est impair. Si $p_1, p_2, \ldots, p_r$ sont des nombres premiers plus grands que $\sqrt{n}$, l'un d'entre eux au plus (peut-être aucun) appartient à la décomposition euclidienne de n en facteurs premiers puisque le produit de deux d'entre eux est supérieur à n.

3) Les décomposants de Goldbach de n sont des éléments inversibles (ou unités) de $\mathbb{Z}/n\mathbb{Z}$, qui sont premiers à n ; les unités sont en nombre $\varphi(n)$ et la moitié d'entre elles sont inférieures ou égales à $n/2$.

4) Si un nombre premier $p \leq n/2$ est congru à n modulo un nombre premier $m_i < \sqrt{n}$ ($n = p + \lambda m_i$), son complémentaire à n, q, 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 être un décomposant de Goldbach de n.

2 Algorithme

Prendre en compte ces faits élémentaires amène une procédure qui permet d'obtenir 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.

3 Etude d'un exemple

Appliquons la procédure au nombre pair $n = 500$.

Notons d'abord que $500 \equiv 2\ (mod\ 3)$. 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 $\left\lfloor \frac{500}{12} \right\rfloor$ nombres de la forme $6k+1$ inférieurs ou égaux à 500/2. Ils sont compris entre 7 et 247 (première colonne du tableau).

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

La seconde colonne du tableau fournit le résultat de la première passe du crible : elle élimine les nombres congrus à 0 ($mod\ m_i$) quelque soit i.

La troisième colonne du tableau fournit le résultat de la deuxième passe du crible : elle élimine les nombres congrus à n $(mod\ m_i)$ quelque soit i.

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).

$500 = 2^2.5^3$. Le module 5 n'apparaît pas en troisième colonne.

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

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

$a_k = 6k+1$	*congruence(s) à 0 éliminant* a_k	*congruence(s) à* r $\neq 0$ *éliminant* a_k (*i.e. congruence(s) à* n)	n-a_k	*nombres restants*
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	

Remarque : revenons sur la première partie de l'algorithme, qui 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 $n/4+1$.

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). La seconde partie de l'algorithme élimine 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 $n \equiv p \ (mod\ m_i)$ *or* $n - p \equiv 0 \ (mod\ m_i)$.

Les deux passes de l'algorithme peuvent être menées indépendamment l'une de l'autre.

4 Le lemme de l'article 127 des Recherches arithmétiques de Gauss

Gauss, dans l'article 127 des Recherches arithmétiques, fournit le lemme suivant :

"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."

Il en donne ensuite la démonstration suivante :

"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."

Il suit de là, comme corollaire, que $\frac{a(a+1)(a+2)(a+3)\ldots(a+n-1)}{1.2.3\ldots n}$ est toujours un nombre entier : proposition connue par la théorie des nombres figurés mais qui, si je ne me trompe, n'a jamais été démontrée par personne.

Enfin, nous aurions pu présenter plus généralement ce lemme de la façon suivante :
"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."

On peut préciser les différents cas du lemme : si on note $n \bmod p$ 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 $2n$ ($mod\ p$) $\Leftrightarrow$ $n \bmod p > 2n \bmod p$.

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

5 Calculs

Même si on ne sait pas étendre le lemme de l'article 127 de Gauss aux cas faisant intervenir plusieurs modules au lieu d'un, on peut cependant effectuer certains calculs.

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.

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.

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 $\frac{a(a+1)(a+2)(a+3)\ldots(a+n-1)}{1.2.3\ldots n}$ 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 mod $p < 2n$ mod p ;
  - il y a $\left\lfloor \frac{n}{p} \right\rfloor + 1$ nombres congrus à $2n$ ($mod\ p$)
    $\Leftrightarrow$ n mod $p > 2n$ mod 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.

Minoration du nombre de décomposants de Goldbach

$n = 2p$	$G(n)$	$n = 10^k$	$G(n)$
202	9	10^2	8
2 018	28	10^3	28
20 014	174	10^4	127
200 006	1 071	10^5	810
2 000 006	7 336	10^6	5 402
20 000 038	53 269	10^7	38 807

- $$8 > \frac{2}{3} \cdot 9$$
  $$28 > \frac{2}{3} \cdot 28$$
  $$127 > \frac{2}{3} \cdot 174$$
  $$810 > \frac{2}{3} \cdot 1\,071$$
  $$5\,402 > \frac{2}{3} \cdot 7\,336$$
  $$38\,807 > \frac{2}{3} \cdot 53\,269$$

- $n = 144$ $(DG : 5, 7, 13, 17, 31, 37, 41, 43, 47, 61, 71)$

  $n = 2^4.3^2$.
  $n/2 = 72$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		139 (p)	
11 (p)	0 $(mod\ 11)$	4 $(mod\ 7)$	133	
17 (p)			127 (p)	$17 + 127$
23 (p)		1 $(mod\ 11)$	121	
29 (p)		4 $(mod\ 5)$	115	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		109 (p)	
41 (p)			103 (p)	$41 + 103$
47 (p)			97 (p)	$47 + 97$
53 (p)		4 $(mod\ 7)$	91	
59 (p)		4 $(mod\ 5)$	85	
65	0 $(mod\ 5)$		79 (p)	
71 (p)			73 (p)	$71 + 73$

7 (p)	0 $(mod\ 7)$		137 (p)	
13 (p)			131 (p)	$13 + 131$
19 (p)		4 $(mod\ 5)$	125	
25	0 $(mod\ 5)$	4 $(mod\ 7)$	119	
31 (p)			113 (p)	$31 + 113$
37 (p)			107 (p)	$37 + 107$
43 (p)			101 (p)	$43 + 101$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	95	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		89 (p)	
61 (p)			83 (p)	$61 + 83$
67 (p)		4 $(mod\ 7)$ et 1 $(mod\ 11)$	77	

- $n = 142$ $(DG : 3, 5, 11, 29, 41, 53, 59, 71)$

  $n = 2.71$.
  $n/2 = 71$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 10\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		137 (p)	
11 (p)	0 $(mod\ 11)$		131 (p)	
17 (p)		2 $(mod\ 5)$	125	
23 (p)		2 $(mod\ 7)$	119	
29 (p)			113 (p)	$29 + 113$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		107 (p)	
41 (p)			101 (p)	$41 + 101$
47 (p)		2 $(mod\ 5)$	95	
53 (p)			89 (p)	$53 + 89$
59 (p)			83 (p)	$59 + 83$
65	0 $(mod\ 5)$	2 $(mod\ 7)$ et 10 $(mod\ 11)$	77	
71 (p)			71 (p)	$71 + 71$

- $n = 140$ $(DG : 3, 13, 31, 37, 43, 61, 67)$

  $n = 2^2.5.7.$
  $n/2 = 70.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 8\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	133	
13 (p)			127 (p)	$13 + 127$
19 (p)		8 $(mod\ 11)$	121	
25	0 $(mod\ 5)$	0 $(mod\ 5)$	115	
31 (p)			109 (p)	$31 + 109$
37 (p)			103 (p)	$37 + 103$
43 (p)			97 (p)	$43 + 97$
49	0 $(mod\ 7)$	0 $(mod\ 7)$	91	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	85	
61 (p)			79 (p)	$61 + 79$
67 (p)			73 (p)	$67 + 73$

- $n = 138$ $(DG : 7, 11, 29, 31, 37, 41, 59, 67)$

  $n = 2.3.23.$
  $n/2 = 69.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 6\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	133	
11 (p)	0 $(mod\ 11)$		127 (p)	
17 (p)		6 $(mod\ 11)$	121	
23 (p)		3 $(mod\ 5)$	115	
29 (p)			109 (p)	$29 + 109$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		103 (p)	
41 (p)			97 (p)	$41 + 97$
47 (p)		5 $(mod\ 7)$	91	
53 (p)		3 $(mod\ 5)$	85	
59			79 (p)	$59 + 79$
65	0 $(mod\ 5)$		73 (p)	

7 (p)	0 $(mod\ 7)$		131 (p)	
13 (p)		3 $(mod\ 5)$	125	
19 (p)		5 $(mod\ 7)$	119	
25	0 $(mod\ 5)$		113 (p)	
31 (p)			107 (p)	$31 + 107$
37 (p)			101 (p)	$37 + 101$
43 (p)		3 $(mod\ 5)$	95	
49	0 $(mod\ 7)$		89 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		83 (p)	
61 (p)		5 $(mod\ 7)$ et 6 $(mod\ 11)$	77	
67			71 (p)	$67 + 71$

- $n = 136$ $(DG : 5, 23, 29, 47, 53)$

  $n = 2^3.17.$
  $n/2 = 68.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 4\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$		131 (p)	
11 (p)	0 $(mod\ 11)$	1 $(mod\ 5)$	125	
17 (p)		3 $(mod\ 7)$	119	
23 (p)			113 (p)	$23 + 113$
29 (p)			107 (p)	$29 + 107$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		101 (p)	
41 (p)		1 $(mod\ 5)$	95	
47 (p)			89 (p)	$47 + 89$
53 (p)			83 (p)	$53 + 83$
59 (p)		3 $(mod\ 7)$ et 4 $(mod\ 11)$	77	
65	0 $(mod\ 5)$		71 (p)	

- $n = 134$ $(DG : 3, 7, 31, 37, 61, 67)$

  $n = 2.67$.
  $n/2 = 67$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7), n \equiv 2\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$		127 (p)	
13 (p)		2 $(mod\ 11)$	121	
19 (p)		4 $(mod\ 5)$	115	
25	0 $(mod\ 5)$		109 (p)	
31 (p)			103 (p)	$31 + 103$
37 (p)			97 (p)	$37 + 97$
43 (p)		1 $(mod\ 7)$	91	
49	0 $(mod\ 7)$	4 $(mod\ 5)$	85	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		79 (p)	
61 (p)			73 (p)	$61 + 73$
67 (p)			67 (p)	$67 + 67$

- $n = 132$ $(DG : 5, 19, 23, 29, 31, 43, 53, 59, 61)$

  $n = 2^2.3.11$.
  $n/2 = 66$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7), n \equiv 0\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		127 (p)	
11 (p)	0 $(mod\ 11)$	0 $(mod\ 11)$	121	
17 (p)		2 $(mod\ 5)$	115	
23 (p)			109 (p)	$23 + 109$
29 (p)			103 (p)	$29 + 103$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		97 (p)	
41 (p)		6 $(mod\ 7)$	91	
47 (p)		2 $(mod\ 5)$	85	
53 (p)			79 (p)	$53 + 79$
59 (p)			73 (p)	$59 + 73$
65	0 $(mod\ 5)$		67 (p)	

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	125	
13 (p)		6 $(mod\ 7)$	119	
19 (p)			113 (p)	$19 + 113$
25	0 $(mod\ 5)$		107 (p)	
31 (p)			101 (p)	$31 + 101$
37 (p)		2 $(mod\ 5)$	95	
43 (p)			89 (p)	$43 + 89$
49	0 $(mod\ 7)$		83 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	6 $(mod\ 7)$ et 0 $(mod\ 11)$	77	
61 (p)			71 (p)	$61 + 71$

- $n = 130$ $(DG : 3, 17, 23, 29, 41, 47, 59)$

  $n = 2.5.13$.
  $n/2 = 65$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 9\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	125	
11 (p)	0 $(mod\ 11)$	4 $(mod\ 7)$	119	
17 (p)			113 (p)	$17 + 113$
23 (p)			107 (p)	$23 + 107$
29 (p)			101 (p)	$29 + 101$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	95	
41 (p)			89 (p)	$41 + 89$
47 (p)			83 (p)	$47 + 83$
53 (p)		4 $(mod\ 7)$ et 9 $(mod\ 11)$	77	
59 (p)			71 (p)	$59 + 71$
65	0 $(mod\ 5)$	0 $(mod\ 5)$	65	

- $n = 128$ $(DG : 19, 31, 61)$

  $n = 2^7$.
  $n/2 = 64$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 7\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$	7 $(mod\ 11)$	121	
13 (p)		3 $(mod\ 5)$	115	
19 (p)			109 (p)	$19 + 109$
25	0 $(mod\ 5)$		103 (p)	
31 (p)			97 (p)	$31 + 97$
37 (p)		2 $(mod\ 7)$	93	
43 (p)		3 $(mod\ 5)$	87	
49	0 $(mod\ 7)$		81	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		75	
61			69 (p)	$61 + 69$

- $n = 126$ $(DG : 13, 17, 19, 23, 29, 37, 43, 47, 53, 59)$

  $n = 2.3^2.7$.
  $n/2 = 63$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 5\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 11)$	121	
11 (p)	0 $(mod\ 11)$	1 $(mod\ 5)$	115	
17 (p)			109 (p)	$17 + 109$
23 (p)			103 (p)	$23 + 103$
29 (p)			97 (p)	$29 + 97$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	91	
41 (p)		1 $(mod\ 5)$	85	
47 (p)			79 (p)	$47 + 79$
53 (p)			73 (p)	$53 + 73$
59 (p)			67 (p)	$59 + 67$
7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	119	
13 (p)			113 (p)	$13 + 113$
19 (p)			107 (p)	$19 + 107$
25	0 $(mod\ 5)$		101 (p)	
31 (p)		1 $(mod\ 5)$	95	
37 (p)			89 (p)	$37 + 89$
43 (p)			83 (p)	$43 + 83$
49	0 $(mod\ 7)$	0 $(mod\ 7)$ et 5 $(mod\ 11)$	77	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		71 (p)	
61 (p)		1 $(mod\ 5)$	65	

- $n = 124$ $(DG : 11, 17, 23, 41, 53)$

  $n = 2^2.31$.
  $n/2 = 62$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 3\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	119	
11 (p)	0 $(mod\ 11)$		113 (p)	
17 (p)			107 (p)	$17 + 107$
23 (p)			101 (p)	$23 + 101$
29 (p)		4 $(mod\ 5)$	95	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		89 (p)	
41 (p)			83 (p)	$41 + 83$
47 (p)		5 $(mod\ 7)$ *et* 3 $(mod\ 11)$	77	
53 (p)			71 (p)	$53 + 71$
59 (p)		4 $(mod\ 5)$	65	

- $n = 122$ $(DG : 13, 19, 43, 61)$

  $n = 2.61$.
  $n/2 = 61$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	115	
13 (p)			109 (p)	$13 + 109$
19 (p)			103 (p)	$19 + 103$
25	0 $(mod\ 5)$		97 (p)	
31 (p)		3 $(mod\ 7)$	91	
37 (p)		2 $(mod\ 5)$	85	
43 (p)			79 (p)	$43 + 79$
49	0 $(mod\ 7)$		73 (p)	
55	0 $(mod\ 5)$		67 (p)	
61 (p)			61 (p)	$61 + 61$

- $n = 120$ $(DG : 7, 11, 13, 17, 19, 23, 31, 37, 41, 47, 53, 59)$

  $n = 2^3.3.5$.
  $n/2 = 60$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	115	
11 (p)			109 (p)	$11 + 109$
17 (p)			103 (p)	$17 + 103$
23 (p)			97 (p)	$23 + 97$
29 (p)		1 $(mod\ 7)$	91	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	85	
41 (p)			79 (p)	$41 + 79$
47 (p)			73 (p)	$47 + 73$
53 (p)			67 (p)	$53 + 67$
59 (p)			61 (p)	$59 + 61$

7 (p)	0 $(mod\ 7)$		103 (p)	
13 (p)			97 (p)	$13 + 97$
19 (p)			91 (p)	$19 + 91$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	85	
31 (p)			79 (p)	$31 + 79$
37 (p)			73 (p)	$37 + 73$
43 (p)		1 $(mod\ 7)$	67 (p)	
49	0 $(mod\ 7)$		61 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	55	

- $n = 118$ $(DG : 5, 11, 17, 29, 47, 59)$

  $n = 2.59$.
  $n/2 = 59$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		113 (p)	
11 (p)			107 (p)	$11 + 107$
17 (p)			101 (p)	$17 + 101$
23 (p)		3 $(mod\ 5)$	95	
29 (p)			89 (p)	$29 + 89$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		83 (p)	
41 (p)		6 $(mod\ 7)$	77	
47 (p)			71 (p)	$47 + 71$
53 (p)		3 $(mod\ 5)$	65	
59 (p)			59 (p)	$59 + 59$

- $n = 116$ $(DG : 3, 7, 13, 19, 37, 43)$

  $n = 2^2.29$.
  $n/2 = 58$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		109 (p)	
13 (p)			103 (p)	$13 + 103$
19 (p)			97 (p)	$19 + 97$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	91	
31 (p)		1 $(mod\ 5)$	85	
37 (p)			79 (p)	$37 + 79$
43 (p)			73 (p)	$43 + 73$
49	0 $(mod\ 7)$		67	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		61 (p)	

- $n = 114$ $(DG : 5, 7, 11, 13, 17, 31, 41, 43, 47, 53)$

  $n = 2.3.19$.
  $n/2 = 57$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		109 (p)	
11 (p)			103 (p)	$11 + 103$
17 (p)			97 (p)	$17 + 97$
23 (p)		2 $(mod\ 7)$	91	
29 (p)		4 $(mod\ 5)$	85	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		79 (p)	
41 (p)			73 (p)	$41 + 73$
47 (p)			67 (p)	$47 + 67$
53 (p)			61 (p)	$53 + 61$

7 (p)	0 $(mod\ 7)$		107 (p)	
13 (p)			101 (p)	$13 + 101$
19 (p)		4 $(mod\ 5)$	95	
25	0 $(mod\ 5)$		89 (p)	
31 (p)			83 (p)	$31 + 83$
37 (p)		2 $(mod\ 7)$	77	
43 (p)			71 (p)	$43 + 71$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	65	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		59 (p)	

- $n = 112$ $(DG : 3, 5, 11, 23, 29, 41, 53)$

  $n = 2^4.7$.
  $n/2 = 56$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		107 (p)	
11 (p)			101 (p)	$11 + 101$
17 (p)		2 $(mod\ 5)$	95	
23 (p)			89 (p)	$23 + 89$
29 (p)			83 (p)	$29 + 83$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	77	
41 (p)			71 (p)	$41 + 71$
47 (p)		2 $(mod\ 5)$	65	
53 (p)			59 (p)	$53 + 59$

- $n = 110$ $(DG : 3, 7, 13, 31, 37, 43)$

  $n = 2.5.11$.
  $n/2 = 55$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		103 (p)	
13 (p)			97 (p)	$13 + 97$
19 (p)		5 $(mod\ 7)$	91	
25	0 $(mod\ 5)$	0 $(mod\ 5)$	85	
31 (p)			79 (p)	$31 + 79$
37 (p)			73 (p)	$37 + 73$
43 (p)			67 (p)	$43 + 67$
49	0 $(mod\ 7)$		61 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	55	

- $n = 108$ $(DG : 5, 7, 11, 19, 29, 37, 41, 47)$

  $n = 2^2.3^3$.
  $n/2 = 54$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		103 (p)	
11 (p)			97 (p)	$11 + 97$
17 (p)		3 $(mod\ 7)$	91	
23 (p)		3 $(mod\ 5)$	85	
29 (p)			79 (p)	$29 + 79$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		73 (p)	
41 (p)			67 (p)	$41 + 67$
47 (p)			61 (p)	$47 + 61$
53 (p)		3 $(mod\ 5)$	55	

7 (p)	0 $(mod\ 7)$		101 (p)	
13 (p)		3 $(mod\ 5)$	95	
19 (p)			89 (p)	$19 + 89$
25	0 $(mod\ 5)$		83 (p)	
31 (p)		3 $(mod\ 7)$	77	
37 (p)			71 (p)	$37 + 71$
43 (p)		3 $(mod\ 5)$	65	
49	0 $(mod\ 7)$		59 (p)	

- $n = 106$ $(DG : 3, 5, 17, 23, 47, 53)$

  $n = 2.53$.
  $n/2 = 53$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		101 (p)	
11 (p)		1 $(mod\ 5)$	95	
17 (p)			89 (p)	$17 + 89$
23 (p)			83 (p)	$23 + 83$
29 (p)		1 $(mod\ 7)$	77	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		71 (p)	
41 (p)		1 $(mod\ 5)$	65	
47 (p)			59 (p)	$47 + 59$
53 (p)			53 (p)	$53 + 53$

- $n = 104$ $(DG : 3, 7, 31, 37, 43)$

  $n = 2^3.13$.
  $n/2 = 52$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		97 (p)	
13 (p)		6 $(mod\ 7)$	91	
19 (p)		4 $(mod\ 5)$	85	
25	0 $(mod\ 5)$		79 (p)	
31 (p)			73 (p)	$31 + 73$
37 (p)			67 (p)	$37 + 67$
43 (p)			61 (p)	$43 + 61$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	55	

- $n = 102$ $(DG : 5, 13, 19, 23, 29, 31, 41, 43)$

  $n = 2.3.17$.
  $n/2 = 51$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		97 (p)	
11 (p)		4 $(mod\ 7)$	91	
17 (p)		2 $(mod\ 5)$	85	
23 (p)			79 (p)	$23 + 79$
29 (p)			73 (p)	$29 + 73$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		67 (p)	
41 (p)			61 (p)	$41 + 61$
47 (p)		2 $(mod\ 5)$	55	

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	95	
13 (p)			89 (p)	$13 + 89$
19 (p)			83 (p)	$19 + 83$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	77	
31 (p)			71 (p)	$31 + 71$
37 (p)		2 $(mod\ 5)$	65	
43 (p)			59 (p)	$43 + 59$
49	0 $(mod\ 7)$		53 (p)	

- $n = 100$ $(DG : 3, 11, 17, 29, 41, 47)$

  $n = 2^2.5^2$.
  $n/2 = 50$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	95	
11 (p)			89 (p)	$11 + 89$
17 (p)			83 (p)	$17 + 83$
23 (p)		2 $(mod\ 7)$	77	
29 (p)			71 (p)	$29 + 71$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	65	
41 (p)			59 (p)	$41 + 59$
47 (p)			53 (p)	$47 + 53$

- $n = 98$ $(DG : 19, 31, 37)$

  $n = 2.7^2$.
  $n/2 = 49$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	91	
13 (p)		3 $(mod\ 5)$	85	
19 (p)			79 (p)	$19 + 79$
25	0 $(mod\ 5)$		73	
31 (p)			67 (p)	$31 + 67$
37 (p)			61 (p)	$37 + 61$
43 (p)		3 $(mod\ 5)$	55	
49	0 $(mod\ 7)$	0 $(mod\ 7)$	49	

- $n = 96$ $(DG : 7, 13, 17, 23, 29, 37, 43)$

  $n = 2^5.3$.
  $n/2 = 48$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	91	
11 (p)		1 $(mod\ 5)$	85	
17 (p)			79 (p)	$17 + 79$
23 (p)			73 (p)	$23 + 73$
29 (p)			67 (p)	$29 + 67$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		61 (p)	
41 (p)		1 $(mod\ 5)$	55	
47 (p)		5 $(mod\ 7)$	49	

7 (p)	0 $(mod\ 7)$		89 (p)	
13 (p)			83 (p)	$13 + 83$
19 (p)		5 $(mod\ 7)$	77	
25	0 $(mod\ 5)$		71 (p)	
31 (p)		1 $(mod\ 5)$	65	
37 (p)			59 (p)	$37 + 59$
43 (p)			53 (p)	$43 + 53$

- $n = 94$ $(DG : 5, 11, 23, 41, 47)$

  $n = 2.47$.
  $n/2 = 47$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		89 (p)	
11 (p)			83 (p)	$11 + 83$
17 (p)		3 $(mod\ 7)$	77	
23 (p)			71 (p)	$23 + 71$
29 (p)		4 $(mod\ 5)$	65	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		59 (p)	
41 (p)			53 (p)	$41 + 53$
47 (p)			47 (p)	$47 + 47$

- $n = 92$ $(DG : 3, 13, 19, 31)$

  $n = 2^2.23$.
  $n/2 = 46$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	87	
13 (p)			81 (p)	$13 + 81$
19 (p)			75 (p)	$19 + 75$
25	0 $(mod\ 5)$		69	
31 (p)			63 (p)	$31 + 63$
37 (p)		2 $(mod\ 5)$	57 (p)	
43 (p)		1 $(mod\ 7)$	51	

- $n = 90$ $(DG : 7, 11, 17, 19, 23, 29, 31, 37, 43)$

  $n = 2.3^2.5$.
  $n/2 = 45$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	85	
11 (p)			79 (p)	$11 + 79$
17 (p)			73 (p)	$17 + 73$
23 (p)			67 (p)	$23 + 67$
29 (p)			61 (p)	$29 + 61$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	55	
41 (p)		6 $(mod\ 7)$	49	

7 (p)	0 $(mod\ 7)$		83 (p)	
13 (p)		6 $(mod\ 7)$	77	
19 (p)			71 (p)	$19 + 71$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	65	
31 (p)			59 (p)	$31 + 59$
37 (p)			53 (p)	$37 + 53$
43 (p)			47 (p)	$43 + 47$

- $n = 88$ $(DG : 5, 17, 29, 41)$

  $n = 2^3.11$.
  $n/2 = 44$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		83 (p)	
11 (p)		4 $(mod\ 7)$	77	
17 (p)			71 (p)	$17 + 71$
23 (p)		3 $(mod\ 5)$	65	
29 (p)			59 (p)	$29 + 59$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		53 (p)	
41 (p)			47 (p)	$41 + 47$

- $n = 86$ $(DG : 3, 7, 13, 19, 43)$

  $n = 2.43$.
  $n/2 = 43$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		79 (p)	
13 (p)			73 (p)	$13 + 73$
19 (p)			67 (p)	$19 + 67$
25	0 $(mod\ 5)$		61 (p)	
31 (p)		1 $(mod\ 5)$	55	
37 (p)		2 $(mod\ 7)$	49	
43 (p)			43 (p)	$43 + 43$

- $n = 84$ $(DG : 5, 11, 13, 17, 23, 31, 37, 41)$

  $n = 2^2.3.7$.
  $n/2 = 42$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		79 (p)	
11 (p)			73 (p)	$11 + 73$
17 (p)			67 (p)	$17 + 67$
23 (p)			61 (p)	$23 + 61$
29 (p)		4 $(mod\ 5)$	55	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	49	
41 (p)			43 (p)	$41 + 43$

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	77	
13 (p)			71 (p)	$13 + 71$
19 (p)		4 $(mod\ 5)$	65	
25	0 $(mod\ 5)$		59 (p)	
31 (p)			53 (p)	$31 + 53$
37 (p)			47 (p)	$37 + 47$

- $n = 82$ $(DG : 3, 11, 23, 29, 41)$

  $n = 2.41$.
  $n/2 = 41$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	77	
11 (p)			71 (p)	$11 + 71$
17 (p)		2 $(mod\ 5)$	65	
23 (p)			59 (p)	$23 + 59$
29 (p)			53 (p)	$29 + 53$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		47 (p)	
41 (p)			41 (p)	$41 + 41$

- $n = 80$ $(DG : 7, 13, 19, 37)$

  $n = 2^4.5$.
  $n/2 = 40$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		73 (p)	
13 (p)			67 (p)	$13 + 67$
19 (p)			61 (p)	$19 + 61$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	55	
31 (p)		3 $(mod\ 7)$	49	
37 (p)			43 (p)	$37 + 43$

- $n = 78$ $(DG : 5, 7, 11, 17, 19, 31, 37)$

  $n = 2.3.13$.
  $n/2 = 39$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		73 (p)	
11 (p)			67 (p)	$11 + 67$
17 (p)			61 (p)	$17 + 61$
23 (p)		3 $(mod\ 5)$	55	
29 (p)		1 $(mod\ 7)$	49	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		43 (p)	

7 (p)	0 $(mod\ 7)$		71 (p)	
13 (p)		3 $(mod\ 5)$	65	
19 (p)			59 (p)	$19 + 59$
25	0 $(mod\ 5)$		53 (p)	
31 (p)			47 (p)	$31 + 47$
37 (p)			41 (p)	$37 + 41$

- $n = 76$ $(DG : 3, 5, 17, 23, 29)$

  $n = 2^2.19$.
  $n/2 = 38$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		71 (p)	
11 (p)		1 $(mod\ 5)$	65	
17 (p)			59 (p)	$17 + 59$
23 (p)			53 (p)	$23 + 53$
29 (p)			47 (p)	$29 + 47$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		41 (p)	

- $n = 74$ $(DG : 3, 7, 13, 31, 37)$

  $n = 2.37$.
  $n/2 = 37$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		67 (p)	
13 (p)			61 (p)	$13 + 61$
19 (p)		4 $(mod\ 5)$	55	
25	0 $(mod\ 5)$	4 $(mod\ 7)$	49	
31 (p)			43 (p)	$31 + 43$
37 (p)			37 (p)	$37 + 37$

- $n = 72$ $(DG : 5, 11, 13, 19, 29, 31)$

  $n = 2^3.3^2$.
  $n/2 = 36$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		67 (p)	
11 (p)			61 (p)	$11 + 61$
17 (p)		2 $(mod\ 5)$	55	
23 (p)		2 $(mod\ 7)$	49	
29 (p)			43 (p)	$29 + 43$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		37 (p)	

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	65	
13 (p)			59 (p)	$13 + 59$
19 (p)			53 (p)	$19 + 53$
25	0 $(mod\ 5)$		47 (p)	
31 (p)			41 (p)	$31 + 41$

- $n = 70$ $(DG : 3, 11, 17, 23, 29)$

  $n = 2.5.7$.
  $n/2 = 35$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	65	
11 (p)			59 (p)	$11 + 59$
17 (p)			53 (p)	$17 + 53$
23 (p)			47 (p)	$23 + 47$
29 (p)			41 (p)	$29 + 41$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$ et 0 $(mod\ 7)$	35	

- $n = 68$ $(DG : 7, 31)$

  $n = 2^2.17$.
  $n/2 = 34$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		61 (p)	
13 (p)		3 $(mod\ 5)$	55	
19 (p)		5 $(mod\ 7)$	49	
25	0 $(mod\ 5)$		43 (p)	
31 (p)			37 (p)	$31 + 37$

- $n = 66$ $(DG : 5, 7, 13, 19, 23, 29)$

  $n = 2.3.11$.
  $n/2 = 33$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		61 (p)	
11 (p)		1 $(mod\ 5)$	55	
17 (p)		3 $(mod\ 7)$	49	
23 (p)			43 (p)	$23 + 43$
29 (p)			37 (p)	$29 + 37$

7 (p)	0 $(mod\ 7)$		59 (p)	
13 (p)			53 (p)	$13 + 53$
19 (p)			47 (p)	$19 + 47$
25	0 $(mod\ 5)$		41 (p)	
31 (p)		1 $(mod\ 5)$ et 3 $(mod\ 7)$	35	

- $n = 64$ $(DG : 3, 5, 11, 17, 23)$

  $n = 2^6$.
  $n/2 = 32$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		59 (p)	
11 (p)			53 (p)	$11 + 53$
17 (p)			47 (p)	$17 + 47$
23 (p)			41 (p)	$23 + 41$
29 (p)		4 $(mod\ 5)$ *et* 1 $(mod\ 7)$	35	

- $n = 62$ $(DG : 3, 19, 31)$

  $n = 2.31$.
  $n/2 = 31$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	55	
13 (p)		6 $(mod\ 7)$	49	
19 (p)			43 (p)	$19 + 43$
25	0 $(mod\ 5)$		37 (p)	
31 (p)			31 (p)	$31 + 31$

- $n = 60$ $(DG : 7, 13, 17, 19, 23, 29)$

  $n = 2^2.3.5$.
  $n/2 = 30$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	55	
11 (p)		4 $(mod\ 7)$	49	
17 (p)			43 (p)	$17 + 43$
23 (p)			37 (p)	$23 + 37$
29 (p)			31 (p)	$29 + 31$

7 (p)	0 $(mod\ 7)$		53 (p)	
13 (p)			47 (p)	$13 + 47$
19 (p)			41 (p)	$19 + 41$
25	0 $(mod\ 5)$	4 $(mod\ 7)$ et 0 $(mod\ 5)$	35	

- $n = 58$ $(DG : 5, 11, 17, 29)$

  $n = 2.29$.
  $n/2 = 29$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		53 (p)	
11 (p)			47 (p)	$11 + 47$
17 (p)			41 (p)	$17 + 41$
23 (p)		3 $(mod\ 5)$ *et* 2 $(mod\ 7)$	35	
29 (p)			29 (p)	$29 + 29$

- $n = 56$ $(DG : 3, 13, 19)$

  $n = 2^3.7$.
  $n/2 = 28$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	49	
13 (p)			43 (p)	$13 + 43$
19 (p)			37 (p)	$19 + 37$
25	0 $(mod\ 5)$		31	

- $n = 54$ $(DG : 7, 11, 13, 17, 23)$

  $n = 2.3^3$.
  $n/2 = 27$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	49	
11 (p)			43 (p)	$11 + 43$
17 (p)			37 (p)	$17 + 37$
23 (p)			31 (p)	$23 + 31$

7 (p)	0 $(mod\ 7)$		47 (p)	
13 (p)			41 (p)	$13 + 41$
19 (p)		4 $(mod\ 5)$ et 5 $(mod\ 7)$	35	
25	0 $(mod\ 5)$		29	

- $n = 52$ $(DG : 5, 11, 23)$

  $n = 2^2.13$.
  $n/2 = 26$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		47 (p)	
11 (p)			41 (p)	$11 + 41$
17 (p)		2 $(mod\ 5)$ *et* 3 $(mod\ 7)$	35	
23 (p)			29 (p)	$23 + 29$

- $n = 50$ $(DG : 3, 7, 13, 19)$

  $n = 2.5^2$.
  $n/2 = 25$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		43 (p)	
13 (p)			37 (p)	$13 + 37$
19 (p)			31 (p)	$19 + 31$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	25	

- $n = 48$ $(DG : 5, 7, 11, 17, 19)$

  $n = 2^4.3$.
  $n/2 = 24$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		43 (p)	
11 (p)			37 (p)	$11 + 37$
17 (p)			31 (p)	$17 + 31$
23 (p)		3 $(mod\ 5)$	25	

7 (p)			41 (p)	$7 + 41$
13 (p)		3 $(mod\ 5)$	35	
19 (p)			29 (p)	$19 + 29$

- $n = 46$ $(DG : 3, 5, 17, 23)$

  $n = 2.23$.
  $n/2 = 23$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		41 (p)	
11 (p)		1 $(mod\ 5)$	35	
17 (p)			29 (p)	$17 + 29$
23 (p)			23 (p)	$23 + 23$

- $n = 44$ $(DG : 3, 7, 13)$

  $n = 2^2.11$.
  $n/2 = 22$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 4\ (mod\ 5)$.

7 (p)			37 (p)	
13 (p)			31 (p)	$13 + 31$
19 (p)		$4\ (mod\ 5)$	25	

- $n = 42$ $(DG : 5, 11, 13, 19)$

  $n = 2.3.7$.
  $n/2 = 21$.
  $5 < \sqrt{n} < 5$. Le module à considérer est 5.
  $n \equiv 2\ (mod\ 5)$.

5 (p)	$0\ (mod\ 5)$		37 (p)	
11 (p)			31 (p)	$11 + 31$
17 (p)		$2\ (mod\ 5)$	25	

7 (p)		$2\ (mod\ 5)$	35	
13 (p)			29 (p)	$13 + 29$
19 (p)			23 (p)	$19 + 23$

- $n = 40$ $(DG : 3, 11, 17)$

  $n = 2^3.5$.
  $n/2 = 20$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	$0\ (mod\ 5)$	$0\ (mod\ 5)$	35	
11 (p)			29 (p)	$11 + 29$
17 (p)			23 (p)	$17 + 23$

- $n = 38$ $(DG : 7, 19)$

  $n = 2.19$.
  $n/2 = 19$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

7 (p)			31 (p)	
13 (p)		$3\ (mod\ 5)$	25	
19			19 (p)	$19 + 19$

- $n = 36$ $(DG : 5, 7, 13, 17)$

  $n = 2^2.3^2$.
  $n/2 = 18$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	$0\ (mod\ 5)$		31 (p)	
11 (p)		$1\ (mod\ 5)$	25	
17 (p)			19 (p)	$17 + 19$

7 (p)			29 (p)	$7 + 29$
13 (p)			23 (p)	$13 + 23$

- $n = 34$ $(DG : 3, 5, 11, 17)$

  $n = 2.17$.
  $n/2 = 17$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 4\ (mod\ 5)$.

5 (p)	$0\ (mod\ 5)$		29 (p)	
11 (p)			23 (p)	$11 + 23$
17 (p)			17 (p)	$17 + 17$

- $n = 32$ $(DG : 3, 13)$

  $n = 2^5$.
  $n/2 = 16$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 2\ (mod\ 5)$.

7 (p)		2 $(mod\ 5)$	25	
13			19 (p)	$13 + 19$

- $n = 30$ $(DG : 7, 11, 13)$

  $n = 2.3.5$.
  $n/2 = 15$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	25	
11 (p)			19 (p)	$11 + 19$
7 (p)			23 (p)	$7 + 23$
13 (p)			17 (p)	$13 + 17$

- $n = 28$ $(DG : 5, 11)$

  $n = 2^2.7$.
  $n/2 = 14$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		23	
11 (p)			17 (p)	$11 + 17$

- $n = 26$ $(DG : 3, 7, 13)$

  $n = 2.13$.
  $n/2 = 13$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

7 (p)			19 (p)	
13			13 (p)	$13 + 13$

- $n = 144$ $(DG : 5, 7, 13, 17, 31, 37, 41, 43, 47, 61, 71)$

  $n = 2^4.3^2$.
  $n/2 = 72$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		139 (p)	
11 (p)	0 $(mod\ 11)$	4 $(mod\ 7)$	133	
17 (p)			127 (p)	$17 + 127$
23 (p)		1 $(mod\ 11)$	121	
29 (p)		4 $(mod\ 5)$	115	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		109 (p)	
41 (p)			103 (p)	$41 + 103$
47 (p)			97 (p)	$47 + 97$
53 (p)		4 $(mod\ 7)$	91	
59 (p)		4 $(mod\ 5)$	85	
65	0 $(mod\ 5)$		79 (p)	
71 (p)			73 (p)	$71 + 73$
7 (p)	0 $(mod\ 7)$		137 (p)	
13 (p)			131 (p)	$13 + 131$
19 (p)		4 $(mod\ 5)$	125	
25	0 $(mod\ 5)$	4 $(mod\ 7)$	119	
31 (p)			113 (p)	$31 + 113$
37 (p)			107 (p)	$37 + 107$
43 (p)			101 (p)	$43 + 101$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	95	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		89 (p)	
61 (p)			83 (p)	$61 + 83$
67 (p)		4 $(mod\ 7)$ et 1 $(mod\ 11)$	77	

- $n = 138$ $(DG : 7, 11, 29, 31, 37, 41, 59, 67)$

  $n = 2.3.23$.
  $n/2 = 69$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 6\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	133	
11 (p)	0 $(mod\ 11)$		127 (p)	
17 (p)		6 $(mod\ 11)$	121	
23 (p)		3 $(mod\ 5)$	115	
29 (p)			109 (p)	$29 + 109$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		103 (p)	
41 (p)			97 (p)	$41 + 97$
47 (p)		5 $(mod\ 7)$	91	
53 (p)		3 $(mod\ 5)$	85	
59			79 (p)	$59 + 79$
65	0 $(mod\ 5)$		73 (p)	
7 (p)	0 $(mod\ 7)$		131 (p)	
13 (p)		3 $(mod\ 5)$	125	
19 (p)		5 $(mod\ 7)$	119	
25	0 $(mod\ 5)$		113 (p)	
31 (p)			107 (p)	$31 + 107$
37 (p)			101 (p)	$37 + 101$
43 (p)		3 $(mod\ 5)$	95	
49	0 $(mod\ 7)$		89 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		83 (p)	
61 (p)		5 $(mod\ 7)$ et 6 $(mod\ 11)$	77	
67			71 (p)	$67 + 71$

- $n = 132$ $(DG : 5, 19, 23, 29, 31, 43, 53, 59, 61)$

  $n = 2^2.3.11.$
  $n/2 = 66.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7), n \equiv 0\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$		127 (p)	
11 (p)	0 $(mod\ 11)$	0 $(mod\ 11)$	121	
17 (p)		2 $(mod\ 5)$	115	
23 (p)			109 (p)	$23 + 109$
29 (p)			103 (p)	$29 + 103$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		97 (p)	
41 (p)		6 $(mod\ 7)$	91	
47 (p)		2 $(mod\ 5)$	85	
53 (p)			79 (p)	$53 + 79$
59 (p)			73 (p)	$59 + 73$
65	0 $(mod\ 5)$		67 (p)	

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	125	
13 (p)		6 $(mod\ 7)$	119	
19 (p)			113 (p)	$19 + 113$
25	0 $(mod\ 5)$		107 (p)	
31 (p)			101 (p)	$31 + 101$
37 (p)		2 $(mod\ 5)$	95	
43 (p)			89 (p)	$43 + 89$
49	0 $(mod\ 7)$		83 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	6 $(mod\ 7)$ et 0 $(mod\ 11)$	77	
61 (p)			71 (p)	$61 + 71$

- $n = 126$ $(DG : 13, 17, 19, 23, 29, 37, 43, 47, 53, 59)$

  $n = 2.3^2.7.$
  $n/2 = 63.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 5\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$	5 $(mod\ 11)$	121	
11 (p)	0 $(mod\ 11)$	1 $(mod\ 5)$	115	
17 (p)			109 (p)	$17 + 109$
23 (p)			103 (p)	$23 + 103$
29 (p)			97 (p)	$29 + 97$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	91	
41 (p)		1 $(mod\ 5)$	85	
47 (p)			79 (p)	$47 + 79$
53 (p)			73 (p)	$53 + 73$
59 (p)			67 (p)	$59 + 67$

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	119	
13 (p)			113 (p)	$13 + 113$
19 (p)			107 (p)	$19 + 107$
25	0 $(mod\ 5)$		101 (p)	
31 (p)		1 $(mod\ 5)$	95	
37 (p)			89 (p)	$37 + 89$
43 (p)			83 (p)	$43 + 83$
49	0 $(mod\ 7)$	0 $(mod\ 7)$ et 5 $(mod\ 11)$	77	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		71 (p)	
61 (p)		1 $(mod\ 5)$	65	

- $n = 120$ $(DG : 7, 11, 13, 17, 19, 23, 31, 37, 41, 47, 53, 59)$

  $n = 2^3.3.5.$
  $n/2 = 60.$
  $7 < \sqrt{n} < 11.$ Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	115	
11 (p)			109 (p)	$11 + 109$
17 (p)			103 (p)	$17 + 103$
23 (p)			97 (p)	$23 + 97$
29 (p)		1 $(mod\ 7)$	91	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	85	
41 (p)			79 (p)	$41 + 79$
47 (p)			73 (p)	$47 + 73$
53 (p)			67 (p)	$53 + 67$
59 (p)			61 (p)	$59 + 61$

7 (p)	0 $(mod\ 7)$		113 (p)	
13 (p)			107 (p)	$13 + 107$
19 (p)			101 (p)	$19 + 101$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	95	
31 (p)			89 (p)	$31 + 89$
37 (p)			83 (p)	$37 + 83$
43 (p)		1 $(mod\ 7)$	77 (p)	
49	0 $(mod\ 7)$		71 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	65	

- $n = 114$ $(DG : 5, 7, 11, 13, 17, 31, 41, 43, 47, 53)$

  $n = 2.3.19$.
  $n/2 = 57$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		109 (p)	
11 (p)			103 (p)	$11 + 103$
17 (p)			97 (p)	$17 + 97$
23 (p)		2 $(mod\ 7)$	91	
29 (p)		4 $(mod\ 5)$	85	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		79 (p)	
41 (p)			73 (p)	$41 + 73$
47 (p)			67 (p)	$47 + 67$
53 (p)			61 (p)	$53 + 61$

7 (p)	0 $(mod\ 7)$		107 (p)	
13 (p)			101 (p)	$13 + 101$
19 (p)		4 $(mod\ 5)$	95	
25	0 $(mod\ 5)$		89 (p)	
31 (p)			83 (p)	$31 + 83$
37 (p)		2 $(mod\ 7)$	77	
43 (p)			71 (p)	$43 + 71$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	65	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		59 (p)	

- $n = 108$ $(DG : 5, 7, 11, 19, 29, 37, 41, 47)$

  $n = 2^2.3^3$.
  $n/2 = 54$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		103 (p)	
11 (p)			97 (p)	$11 + 97$
17 (p)		3 $(mod\ 7)$	91	
23 (p)		3 $(mod\ 5)$	85	
29 (p)			79 (p)	$29 + 79$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		73 (p)	
41 (p)			67 (p)	$41 + 67$
47 (p)			61 (p)	$47 + 61$
53 (p)		3 $(mod\ 5)$	55	

7 (p)	0 $(mod\ 7)$		101 (p)	
13 (p)		3 $(mod\ 5)$	95	
19 (p)			89 (p)	$19 + 89$
25	0 $(mod\ 5)$		83 (p)	
31 (p)		3 $(mod\ 7)$	77	
37 (p)			71 (p)	$37 + 71$
43 (p)		3 $(mod\ 5)$	65	
49	0 $(mod\ 7)$		59 (p)	

- $n = 102$ $(DG : 5, 13, 19, 23, 29, 31, 41, 43)$

  $n = 2.3.17$.
  $n/2 = 51$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		97 (p)	
11 (p)		4 $(mod\ 7)$	91	
17 (p)		2 $(mod\ 5)$	85	
23 (p)			79 (p)	$23 + 79$
29 (p)			73 (p)	$29 + 73$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		67 (p)	
41 (p)			61 (p)	$41 + 61$
47 (p)		2 $(mod\ 5)$	55	

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	95	
13 (p)			89 (p)	$13 + 89$
19 (p)			83 (p)	$19 + 83$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	77	
31 (p)			71 (p)	$31 + 71$
37 (p)		2 $(mod\ 5)$	65	
43 (p)			59 (p)	$43 + 59$
49	0 $(mod\ 7)$		53 (p)	

- $n = 96$ $(DG : 7, 13, 17, 23, 29, 37, 43)$

  $n = 2^5.3$.
  $n/2 = 48$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	91	
11 (p)		1 $(mod\ 5)$	85	
17 (p)			79 (p)	$17 + 79$
23 (p)			73 (p)	$23 + 73$
29 (p)			67 (p)	$29 + 67$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		61 (p)	
41 (p)		1 $(mod\ 5)$	55	
47 (p)		5 $(mod\ 7)$	49	
7 (p)	0 $(mod\ 7)$		89 (p)	
13 (p)			83 (p)	$13 + 83$
19 (p)		5 $(mod\ 7)$	77	
25	0 $(mod\ 5)$		71 (p)	
31 (p)		1 $(mod\ 5)$	65	
37 (p)			59 (p)	$37 + 59$
43 (p)			53 (p)	$43 + 53$

- $n = 90$ $(DG : 7, 11, 17, 19, 23, 29, 31, 37, 43)$

  $n = 2.3^2.5$.
  $n/2 = 45$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	85	
11 (p)			79 (p)	$11 + 79$
17 (p)			73 (p)	$17 + 73$
23 (p)			67 (p)	$23 + 67$
29 (p)			61 (p)	$29 + 61$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	55	
41 (p)		6 $(mod\ 7)$	49	
7 (p)	0 $(mod\ 7)$		83 (p)	
13 (p)		6 $(mod\ 7)$	77	
19 (p)			71 (p)	$19 + 71$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	65	
31 (p)			59 (p)	$31 + 59$
37 (p)			53 (p)	$37 + 53$
43 (p)			47 (p)	$43 + 47$

- $n = 84$ $(DG : 5, 11, 13, 17, 23, 31, 37, 41)$

  $n = 2^2.3.7$.
  $n/2 = 42$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		79 (p)	
11 (p)			73 (p)	$11 + 73$
17 (p)			67 (p)	$17 + 67$
23 (p)			61 (p)	$23 + 61$
29 (p)		4 $(mod\ 5)$	55	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	49	
41 (p)			43 (p)	$41 + 43$
7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	77	
13 (p)			71 (p)	$13 + 71$
19 (p)		4 $(mod\ 5)$	65	
25	0 $(mod\ 5)$		59 (p)	
31 (p)			53 (p)	$31 + 53$
37 (p)			47 (p)	$37 + 47$

- $n = 78$ $(DG : 5, 7, 11, 17, 19, 31, 37)$

  $n = 2.3.13$.
  $n/2 = 39$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		73 (p)	
11 (p)			67 (p)	$11 + 67$
17 (p)			61 (p)	$17 + 61$
23 (p)		3 $(mod\ 5)$	55	
29 (p)		1 $(mod\ 7)$	49	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		43 (p)	
7 (p)	0 $(mod\ 7)$		71 (p)	
13 (p)		3 $(mod\ 5)$	65	
19 (p)			59 (p)	$19 + 59$
25	0 $(mod\ 5)$		53 (p)	
31 (p)			47 (p)	$31 + 47$
37 (p)			41 (p)	$37 + 41$

- $n = 72$ $(DG : 5, 11, 13, 19, 29, 31)$

  $n = 2^3.3^2$.
  $n/2 = 36$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		67 (p)	
11 (p)			61 (p)	$11 + 61$
17 (p)		2 $(mod\ 5)$	55	
23 (p)		2 $(mod\ 7)$	49	
29 (p)			43 (p)	$29 + 43$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		37 (p)	
7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	65	
13 (p)			59 (p)	$13 + 59$
19 (p)			53 (p)	$19 + 53$
25	0 $(mod\ 5)$		47 (p)	
31 (p)			41 (p)	$31 + 41$

- $n = 66$ $(DG : 5, 7, 13, 19, 23, 29)$

  $n = 2.3.11$.
  $n/2 = 33$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		61 (p)	
11 (p)		1 $(mod\ 5)$	55	
17 (p)		3 $(mod\ 7)$	49	
23 (p)			43 (p)	$23 + 43$
29 (p)			37 (p)	$29 + 37$
7 (p)	0 $(mod\ 7)$		59 (p)	
13 (p)			53 (p)	$13 + 53$
19 (p)			47 (p)	$19 + 47$
25	0 $(mod\ 5)$		41 (p)	
31 (p)		1 $(mod\ 5)$ et 3 $(mod\ 7)$	35	

- $n = 60$ $(DG : 7, 13, 17, 19, 23, 29)$

  $n = 2^2.3.5$.
  $n/2 = 30$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	55	
11 (p)		4 $(mod\ 7)$	49	
17 (p)			43 (p)	$17 + 43$
23 (p)			37 (p)	$23 + 37$
29 (p)			31 (p)	$29 + 31$
7 (p)	0 $(mod\ 7)$		53 (p)	
13 (p)			47 (p)	$13 + 47$
19 (p)			41 (p)	$19 + 41$
25	0 $(mod\ 5)$	4 $(mod\ 7)$ et 0 $(mod\ 5)$	35	

- $n = 54$ $(DG : 7, 11, 13, 17, 23)$

  $n = 2.3^3$.
  $n/2 = 27$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	49	
11 (p)			43 (p)	$11 + 43$
17 (p)			37 (p)	$17 + 37$
23 (p)			31 (p)	$23 + 31$
7 (p)	0 $(mod\ 7)$		47 (p)	
13 (p)			41 (p)	$13 + 41$
19 (p)		4 $(mod\ 5)$ et 5 $(mod\ 7)$	35	
25	0 $(mod\ 5)$		29	

- $n = 48$ $(DG : 5, 7, 11, 17, 19)$

  $n = 2^4.3$.
  $n/2 = 24$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		43 (p)	
11 (p)			37 (p)	$11 + 37$
17 (p)			31 (p)	$17 + 31$
23 (p)		3 $(mod\ 5)$	25	
7 (p)			41 (p)	$7 + 41$
13 (p)		3 $(mod\ 5)$	35	
19 (p)			29 (p)	$19 + 29$

- $n = 42$ $(DG : 5, 11, 13, 19)$

  $n = 2.3.7$.
  $n/2 = 21$.
  $5 < \sqrt{n} < 5$. Le module à considérer est 5.
  $n \equiv 2\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		37 (p)	
11 (p)			31 (p)	$11 + 31$
17 (p)		2 $(mod\ 5)$	25	
7 (p)		2 $(mod\ 5)$	35	
13 (p)			29 (p)	$13 + 29$
19 (p)			23 (p)	$19 + 23$

- $n = 36$ $(DG : 5, 7, 13, 17)$

  $n = 2^2.3^2$.
  $n/2 = 18$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		31 (p)	
11 (p)		1 $(mod\ 5)$	25	
17 (p)			19 (p)	$17 + 19$
7 (p)			29 (p)	$7 + 29$
13 (p)			23 (p)	$13 + 23$

- $n = 30$ $(DG : 7, 11, 13)$

  $n = 2.3.5$.
  $n/2 = 15$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	25	
11 (p)			19 (p)	$11 + 19$
7 (p)			23 (p)	$7 + 23$
13 (p)			17 (p)	$13 + 17$

- $n = 140$ $(DG : 3, 13, 31, 37, 43, 61, 67)$

  $n = 2^2.5.7.$
  $n/2 = 70.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 8\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	133	
13 (p)			127 (p)	$13 + 127$
19 (p)		8 $(mod\ 11)$	121	
25	0 $(mod\ 5)$	0 $(mod\ 5)$	115	
31 (p)			109 (p)	$31 + 109$
37 (p)			103 (p)	$37 + 103$
43 (p)			97 (p)	$43 + 97$
49	0 $(mod\ 7)$	0 $(mod\ 7)$	91	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	85	
61 (p)			79 (p)	$61 + 79$
67 (p)			73 (p)	$67 + 73$

- $n = 134$ $(DG : 3, 7, 31, 37, 61, 67)$

  $n = 2.67.$
  $n/2 = 67.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7), n \equiv 2\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$		127 (p)	
13 (p)		2 $(mod\ 11)$	121	
19 (p)		4 $(mod\ 5)$	115	
25	0 $(mod\ 5)$		109 (p)	
31 (p)			103 (p)	$31 + 103$
37 (p)			97 (p)	$37 + 97$
43 (p)		1 $(mod\ 7)$	91	
49	0 $(mod\ 7)$	4 $(mod\ 5)$	85	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		79 (p)	
61 (p)			73 (p)	$61 + 73$
67 (p)			67 (p)	$67 + 67$

- $n = 128$ $(DG : 19, 31, 61)$

  $n = 2^7.$
  $n/2 = 64.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 7\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$	7 $(mod\ 11)$	121	
13 (p)		3 $(mod\ 5)$	115	
19 (p)			109 (p)	$19 + 109$
25	0 $(mod\ 5)$		103 (p)	
31 (p)			97 (p)	$31 + 97$
37 (p)		2 $(mod\ 7)$	93	
43 (p)		3 $(mod\ 5)$	87	
49	0 $(mod\ 7)$		81	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		75	
61			69 (p)	$61 + 69$

- $n = 122$ $(DG : 13, 19, 43, 61)$

  $n = 2.61.$
  $n/2 = 61.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 1\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	115	
13 (p)			109 (p)	$13 + 109$
19 (p)			103 (p)	$19 + 103$
25	0 $(mod\ 5)$		97 (p)	
31 (p)		3 $(mod\ 7)$	91	
37 (p)		2 $(mod\ 5)$	85	
43 (p)			79 (p)	$43 + 79$
49	0 $(mod\ 7)$		73 (p)	
55	0 $(mod\ 5)$		67 (p)	
61 (p)			61 (p)	$61 + 61$

- $n = 116$ $(DG : 3, 7, 13, 19, 37, 43)$

  $n = 2^2.29$.
  $n/2 = 58$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		109 (p)	
13 (p)			103 (p)	$13 + 103$
19 (p)			97 (p)	$19 + 97$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	91	
31 (p)		1 $(mod\ 5)$	85	
37 (p)			79 (p)	$37 + 79$
43 (p)			73 (p)	$43 + 73$
49	0 $(mod\ 7)$		67	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		61 (p)	

- $n = 110$ $(DG : 3, 7, 13, 31, 37, 43)$

  $n = 2.5.11$.
  $n/2 = 55$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		103 (p)	
13 (p)			97 (p)	$13 + 97$
19 (p)		5 $(mod\ 7)$	91	
25	0 $(mod\ 5)$	0 $(mod\ 5)$	85	
31 (p)			79 (p)	$31 + 79$
37 (p)			73 (p)	$37 + 73$
43 (p)			67 (p)	$43 + 67$
49	0 $(mod\ 7)$		61 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	55	

- $n = 104$ $(DG : 3, 7, 31, 37, 43)$

  $n = 2^3.13$.
  $n/2 = 52$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		97 (p)	
13 (p)		6 $(mod\ 7)$	91	
19 (p)		4 $(mod\ 5)$	85	
25	0 $(mod\ 5)$		79 (p)	
31 (p)			73 (p)	$31 + 73$
37 (p)			67 (p)	$37 + 67$
43 (p)			61 (p)	$43 + 61$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	55	

- $n = 98$ $(DG : 19, 31, 37)$

  $n = 2.7^2$.
  $n/2 = 49$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	91	
13 (p)		3 $(mod\ 5)$	85	
19 (p)			79 (p)	$19 + 79$
25	0 $(mod\ 5)$		73	
31 (p)			67 (p)	$31 + 67$
37 (p)			61 (p)	$37 + 61$
43 (p)		3 $(mod\ 5)$	55	
49	0 $(mod\ 7)$	0 $(mod\ 7)$	49	

- $n = 92$ $(DG : 3, 13, 19, 31)$

  $n = 2^2.23$.
  $n/2 = 46$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	87	
13 (p)			81 (p)	$13 + 81$
19 (p)			75 (p)	$19 + 75$
25	0 $(mod\ 5)$		69	
31 (p)			63 (p)	$31 + 63$
37 (p)		2 $(mod\ 5)$	57 (p)	
43 (p)		1 $(mod\ 7)$	51	

- $n = 86$ $(DG : 3, 7, 13, 19, 43)$

  $n = 2.43$.
  $n/2 = 43$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		79 (p)	
13 (p)			73 (p)	$13 + 73$
19 (p)			67 (p)	$19 + 67$
25	0 $(mod\ 5)$		61 (p)	
31 (p)		1 $(mod\ 5)$	55	
37 (p)		2 $(mod\ 7)$	49	
43 (p)			43 (p)	$43 + 43$

- $n = 80$ $(DG : 7, 13, 19, 37)$

  $n = 2^4.5$.
  $n/2 = 40$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		73 (p)	
13 (p)			67 (p)	$13 + 67$
19 (p)			61 (p)	$19 + 61$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	55	
31 (p)		3 $(mod\ 7)$	49	
37 (p)			43 (p)	$37 + 43$

- $n = 74$ $(DG : 3, 7, 13, 31, 37)$

  $n = 2.37$.
  $n/2 = 37$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		67 (p)	
13 (p)			61 (p)	$13 + 61$
19 (p)		4 $(mod\ 5)$	55	
25	0 $(mod\ 5)$	4 $(mod\ 7)$	49	
31 (p)			43 (p)	$31 + 43$
37 (p)			37 (p)	$37 + 37$

- $n = 68$ $(DG : 7, 31)$

  $n = 2^2.17$.
  $n/2 = 34$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		61 (p)	
13 (p)		3 $(mod\ 5)$	55	
19 (p)		5 $(mod\ 7)$	49	
25	0 $(mod\ 5)$		43 (p)	
31 (p)			37 (p)	$31 + 37$

- $n = 62$ $(DG : 3, 19, 31)$

  $n = 2.31$.
  $n/2 = 31$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	55	
13 (p)		6 $(mod\ 7)$	49	
19 (p)			43 (p)	$19 + 43$
25	0 $(mod\ 5)$		37 (p)	
31 (p)			31 (p)	$31 + 31$

- $n = 56$ $(DG : 3, 13, 19)$

  $n = 2^3.7$.
  $n/2 = 28$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	49	
13 (p)			43 (p)	$13 + 43$
19 (p)			37 (p)	$19 + 37$
25	0 $(mod\ 5)$		31	

- $n = 50$ $(DG : 3, 7, 13, 19)$

  $n = 2.5^2$.
  $n/2 = 25$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		43 (p)	
13 (p)			37 (p)	$13 + 37$
19 (p)			31 (p)	$19 + 31$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	25	

- $n = 44$ $(DG : 3, 7, 13)$

  $n = 2^2.11$.
  $n/2 = 22$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 4\ (mod\ 5)$.

7 (p)			37 (p)	
13 (p)			31 (p)	$13 + 31$
19 (p)		4 $(mod\ 5)$	25	

- $n = 38$ $(DG : 7, 19)$

  $n = 2.19$.
  $n/2 = 19$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

7 (p)			31 (p)	
13 (p)		3 $(mod\ 5)$	25	
19			19 (p)	$19 + 19$

- $n = 32$ $(DG : 3, 13)$

  $n = 2^5$.
  $n/2 = 16$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 2\ (mod\ 5)$.

7 (p)		2 $(mod\ 5)$	25	
13			19 (p)	$13 + 19$

- $n = 26$ $(DG : 3, 7, 13)$

  $n = 2.13$.
  $n/2 = 13$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

7 (p)			19 (p)	
13			13 (p)	$13 + 13$

- $n = 142$ $(DG : 3, 5, 11, 29, 41, 53, 59, 71)$

  $n = 2.71$.
  $n/2 = 71$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 10\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		137 (p)	
11 (p)	0 $(mod\ 11)$		131 (p)	
17 (p)		2 $(mod\ 5)$	125	
23 (p)		2 $(mod\ 7)$	119	
29 (p)			113 (p)	$29 + 113$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		107 (p)	
41 (p)			101 (p)	$41 + 101$
47 (p)		2 $(mod\ 5)$	95	
53 (p)			89 (p)	$53 + 89$
59 (p)			83 (p)	$59 + 83$
65	0 $(mod\ 5)$	2 $(mod\ 7)$ *et* 10 $(mod\ 11)$	77	
71 (p)			71 (p)	$71 + 71$

- $n = 136$ $(DG : 5, 23, 29, 47, 53)$

  $n = 2^3.17$.
  $n/2 = 68$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 4\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		131 (p)	
11 (p)	0 $(mod\ 11)$	1 $(mod\ 5)$	125	
17 (p)		3 $(mod\ 7)$	119	
23 (p)			113 (p)	$23 + 113$
29 (p)			107 (p)	$29 + 107$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		101 (p)	
41 (p)		1 $(mod\ 5)$	95	
47 (p)			89 (p)	$47 + 89$
53 (p)			83 (p)	$53 + 83$
59 (p)		3 $(mod\ 7)$ *et* 4 $(mod\ 11)$	77	
65	0 $(mod\ 5)$		71 (p)	

- $n = 130$ $(DG : 3, 17, 23, 29, 41, 47, 59)$

  $n = 2.5.13$.
  $n/2 = 65$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 9\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	125	
11 (p)	0 $(mod\ 11)$	4 $(mod\ 7)$	119	
17 (p)			113 (p)	$17 + 113$
23 (p)			107 (p)	$23 + 107$
29 (p)			101 (p)	$29 + 101$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	95	
41 (p)			89 (p)	$41 + 89$
47 (p)			83 (p)	$47 + 83$
53 (p)		4 $(mod\ 7)$ *et* 9 $(mod\ 11)$	77	
59 (p)			71 (p)	$59 + 71$
65	0 $(mod\ 5)$	0 $(mod\ 5)$	65	

- $n = 124$ $(DG : 11, 17, 23, 41, 53)$

  $n = 2^2.31$.
  $n/2 = 62$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 3\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	119	
11 (p)	0 $(mod\ 11)$		113 (p)	
17 (p)			107 (p)	$17 + 107$
23 (p)			101 (p)	$23 + 101$
29 (p)		4 $(mod\ 5)$	95	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		89 (p)	
41 (p)			83 (p)	$41 + 83$
47 (p)		5 $(mod\ 7)$ *et* 3 $(mod\ 11)$	77	
53 (p)			71 (p)	$53 + 71$
59 (p)		4 $(mod\ 5)$	65	

- $n = 118$ $(DG : 5, 11, 17, 29, 47, 59)$

  $n = 2.59$.
  $n/2 = 59$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		113 (p)	
11 (p)			107 (p)	$11 + 107$
17 (p)			101 (p)	$17 + 101$
23 (p)		3 $(mod\ 5)$	95	
29 (p)			89 (p)	$29 + 89$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		83 (p)	
41 (p)		6 $(mod\ 7)$	77	
47 (p)			71 (p)	$47 + 71$
53 (p)		3 $(mod\ 5)$	65	
59 (p)			59 (p)	$59 + 59$

- $n = 112$ $(DG : 3, 5, 11, 23, 29, 41, 53)$

  $n = 2^4.7$.
  $n/2 = 56$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		107 (p)	
11 (p)			101 (p)	$11 + 101$
17 (p)		2 $(mod\ 5)$	95	
23 (p)			89 (p)	$23 + 89$
29 (p)			83 (p)	$29 + 83$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	77	
41 (p)			71 (p)	$41 + 71$
47 (p)		2 $(mod\ 5)$	65	
53 (p)			59 (p)	$53 + 59$

- $n = 106$ $(DG : 3, 5, 17, 23, 47, 53)$

  $n = 2.53$.
  $n/2 = 53$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		101 (p)	
11 (p)		1 $(mod\ 5)$	95	
17 (p)			89 (p)	$17 + 89$
23 (p)			83 (p)	$23 + 83$
29 (p)		1 $(mod\ 7)$	77	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		71 (p)	
41 (p)		1 $(mod\ 5)$	65	
47 (p)			59 (p)	$47 + 59$
53 (p)			53 (p)	$53 + 53$

- $n = 100$ $(DG : 3, 11, 17, 29, 41, 47)$

  $n = 2^2.5^2$.
  $n/2 = 50$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	95	
11 (p)			89 (p)	$11 + 89$
17 (p)			83 (p)	$17 + 83$
23 (p)		2 $(mod\ 7)$	77	
29 (p)			71 (p)	$29 + 71$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	65	
41 (p)			59 (p)	$41 + 59$
47 (p)			53 (p)	$47 + 53$

- $n = 94$ $(DG : 5, 11, 23, 41, 47)$

  $n = 2.47$.
  $n/2 = 47$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		89 (p)	
11 (p)			83 (p)	$11 + 83$
17 (p)		3 $(mod\ 7)$	77	
23 (p)			71 (p)	$23 + 71$
29 (p)		4 $(mod\ 5)$	65	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		59 (p)	
41 (p)			53 (p)	$41 + 53$
47 (p)			47 (p)	$47 + 47$

- $n = 88$ $(DG : 5, 17, 29, 41)$

  $n = 2^3.11$.
  $n/2 = 44$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		83 (p)	
11 (p)		4 $(mod\ 7)$	77	
17 (p)			71 (p)	$17 + 71$
23 (p)		3 $(mod\ 5)$	65	
29 (p)			59 (p)	$29 + 59$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		53 (p)	
41 (p)			47 (p)	$41 + 47$

- $n = 82$ $(DG : 3, 11, 23, 29, 41)$

  $n = 2.41$.
  $n/2 = 41$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	77	
11 (p)			71 (p)	$11 + 71$
17 (p)		2 $(mod\ 5)$	65	
23 (p)			59 (p)	$23 + 59$
29 (p)			53 (p)	$29 + 53$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		47 (p)	
41 (p)			41 (p)	$41 + 41$

- $n = 76$ $(DG : 3, 5, 17, 23, 29)$

  $n = 2^2.19$.
  $n/2 = 38$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		71 (p)	
11 (p)		1 $(mod\ 5)$	65	
17 (p)			59 (p)	$17 + 59$
23 (p)			53 (p)	$23 + 53$
29 (p)			47 (p)	$29 + 47$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		41 (p)	

- $n = 70$ $(DG : 3, 11, 17, 23, 29)$

  $n = 2.5.7$.
  $n/2 = 35$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	65	
11 (p)			59 (p)	$11 + 59$
17 (p)			53 (p)	$17 + 53$
23 (p)			47 (p)	$23 + 47$
29 (p)			41 (p)	$29 + 41$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$ et 0 $(mod\ 7)$	35	

- $n = 64$ $(DG : 3, 5, 11, 17, 23)$

  $n = 2^6$.
  $n/2 = 32$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		59 (p)	
11 (p)			53 (p)	$11 + 53$
17 (p)			47 (p)	$17 + 47$
23 (p)			41 (p)	$23 + 41$
29 (p)		4 $(mod\ 5)$ *et* 1 $(mod\ 7)$	35	

- $n = 58$ $(DG : 5, 11, 17, 29)$

  $n = 2.29$.
  $n/2 = 29$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		53 (p)	
11 (p)			47 (p)	$11 + 47$
17 (p)			41 (p)	$17 + 41$
23 (p)		3 $(mod\ 5)$ *et* 2 $(mod\ 7)$	35	
29 (p)			29 (p)	$29 + 29$

- $n = 52$ $(DG : 5, 11, 23)$

  $n = 2^2.13$.
  $n/2 = 26$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		47 (p)	
11 (p)			41 (p)	$11 + 41$
17 (p)		2 $(mod\ 5)$ *et* 3 $(mod\ 7)$	35	
23 (p)			29 (p)	$23 + 29$

- $n = 46$ $(DG : 3, 5, 17, 23)$

  $n = 2.23$.
  $n/2 = 23$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		41 (p)	
11 (p)		1 $(mod\ 5)$	35	
17 (p)			29 (p)	$17 + 29$
23 (p)			23 (p)	$23 + 23$

- $n = 40$ $(DG : 3, 11, 17)$

  $n = 2^3.5$.
  $n/2 = 20$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	35	
11 (p)			29 (p)	$11 + 29$
17 (p)			23 (p)	$17 + 23$

- $n = 34$ $(DG : 3, 5, 11, 17)$

  $n = 2.17$.
  $n/2 = 17$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 4\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		29 (p)	
11 (p)			23 (p)	$11 + 23$
17 (p)			17 (p)	$17 + 17$

- $n = 28$ $(DG : 5, 11)$

  $n = 2^2.7$.
  $n/2 = 14$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		23	
11 (p)			17 (p)	$11 + 17$

Application double du crible d'Eratosthène pour trouver les décomposants de Goldbach d'un nombre pair

Denise Vella-Chemla

Décembre 2012

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair x plus grand que 2 est la somme de deux nombres premiers. Ces nombres premiers p et q sont appelés décomposants de Goldbach de x.

Un décomposant de Goldbach d'un nombre pair x ne peut être congru à x selon aucun module premier m inférieur ou égal à $\sqrt{x}$, cette condition garantissant que son complémentaire q à x est premier également (et ce quel que soit r $(mod\ m)$ le reste de x).

2 Exemple du nombre pair 500 : détail de la double application du crible d'Eratosthène

Ci-après, pour le nombre pair 500, nous montrons comment procéde la double utilisation du crible d'Eratosthène :

1) la première application du crible consiste à éliminer les nombres congrus à 0 modulo un nombre premier inférieur ou égal à $\sqrt{x}$;

2) la deuxième application du crible consiste à éliminer les nombres congrus à x modulo un nombre premier inférieur ou égal à $\sqrt{x}$.

500 étant congru à 2 modulo 3, les seuls nombres à considérer sont ceux appartenant à la progression arithmétique $6k+1$, de 7 à 247. Tous les nombres appartenant à la progression arithmétique $6k-1$ sont congrus à 500 $(mod\ 6)$ et sont donc composés.

Nous notons dans la deuxième colonne les congruences éliminées lors de la première passe du crible (congruences à 0 modulo un nombre premier inférieur ou égal à $\sqrt{500} = 22, ...$). Les modules devant être considérés sont 5, 7, 11, 13, 17, 19.

Nous notons dans la troisième colonne les congruences éliminées lors de la deuxième passe du crible (congruences partagées avec x).
500 est congru à 0 $(mod\ 5)$, 3 $(mod\ 7)$, 5 $(mod\ 11)$, 6 $(mod\ 13)$, 7 $(mod\ 17)$ *et* 6 $(mod\ 19)$.
Les couleurs permettent de bien visualiser les périodicités.

7	$0\ (mod\ 7)$	$7\ (mod\ 17)$
13	$0\ (mod\ 13)$	
19	$0\ (mod\ 19)$	$6\ (mod\ 13)$
25	$0\ (mod\ 5)$	$0\ (mod\ 5)\ et\ 6\ (mod\ 19)$
31		$3\ (mod\ 7)$
37		
43		
49	$0\ (mod\ 7)$	$5\ (mod\ 11)$
55	$0\ (mod\ 5\ et\ 11)$	$0\ (mod\ 5)$
61		
67		
73		$3\ (mod\ 7)$
79		
85	$0\ (mod\ 5\ et\ 17)$	$0\ (mod\ 5)$
91	$0\ (mod\ 7\ et\ 13)$	
97		$6\ (mod\ 13)$
103		
109		$7\ (mod\ 17)$
115	$0\ (mod\ 5)$	$0\ (mod\ 5)\ et\ 3\ (mod\ 7)\ et\ 5\ (mod\ 11)$
121	$0\ (mod\ 11)$	
127		
133	$0\ (mod\ 7\ et\ 19)$	
139		$6\ (mod\ 19)$
145	$0\ (mod\ 5)$	$0\ (mod\ 5)$
151		
157		$3\ (mod\ 7)$
163		
169	$0\ (mod\ 13)$	
175	$0\ (mod\ 5\ et\ 7)$	$0\ (mod\ 5)\ et\ 6\ (mod\ 13)$
181		$5\ (mod\ 11)$
187	$0\ (mod\ 11\ et\ 17)$	
193		
199		$3\ (mod\ 7)$
205	$0\ (mod\ 5)$	$0\ (mod\ 5)$
211		$7\ (mod\ 17)$
217	$0\ (mod\ 7)$	
223		
229		
235	$0\ (mod\ 5)$	$0\ (mod\ 5)$
241		$3\ (mod\ 7)$
247	$0\ (mod\ 13\ et\ 19)$	$5\ (mod\ 11)$

Présentons une idée qui devrait être intéressante : on peut considérer que l'élimination des nombres dans la troisième colonne consiste à appliquer le crible d'Eratosthène sur un autre intervalle de la droite des entiers, obtenu par une translation adéquate depuis le nombre origine 0. Remplaçons chaque congruence à un nombre non nul (telle que $x \equiv r\ (mod\ m), r \neq 0$) par la congruence correspondante $x + \delta \equiv 0\ (mod\ m)$ avec δ convenablement choisi.

Pour l'exemple du nombre pair 500, le système de congruences qui permet de trouver l'intervalle translaté est :

$$\begin{cases} x \equiv 1\ (mod\ 6) \\ x \equiv 0\ (mod\ 17) \\ x + 12 \equiv 0\ (mod\ 13) \\ x + 18 \equiv 0\ (mod\ 19) \\ x + 24 \equiv 0\ (mod\ 7) \\ x + 42 \equiv 0\ (mod\ 11) \end{cases}$$

Ce système de congruences est équivalent à : $\begin{cases} x \equiv 1\ (mod\ 6) \\ x \equiv 4\ (mod\ 7) \\ x \equiv 2\ (mod\ 11) \\ x \equiv 1\ (mod\ 13) \\ x \equiv 0\ (mod\ 17) \\ x \equiv 1\ (mod\ 19) \end{cases}$ dont la plus petite solution est 646153.

Il y a une bijection entre les nombres x de l'intervalle $[7, 247]$ initial et les nombres $y = x + 646146$ de l'intervalle $[646153, 646393]$ telle que $x \equiv r\ (mod\ m), r \neq 0 \iff y \equiv 0\ (mod\ m)$.

7	$7\ (mod\ 17)$	646153	$0\ (mod\ 17)$
13		646159	
19	$6\ (mod\ 13)$	646165	$0\ (mod\ 13)$
25	$6\ (mod\ 19)$	646171	$0\ (mod\ 19)$
31	$3\ (mod\ 7)$	646177	$0\ (mod\ 7)$
37		646183	
43		646189	
49	$5\ (mod\ 11)$	646195	$0\ (mod\ 11)$
55		646201	
61		646207	
67		646213	
73	$3\ (mod\ 7)$	646219	$0\ (mod\ 7)$
79		646225	
85		646231	
91		646237	
97	$6\ (mod\ 13)$	646243	$0\ (mod\ 13)$
103		646249	
109	$7\ (mod\ 17)$	646255	$0\ (mod\ 17)$
115	$3\ (mod\ 7)$ *et* $0\ (mod\ 11)$	646261	$0\ (mod\ 7)$ *et* $0\ (mod\ 11)$
121		646267	
127		646273	
133		646279	
139	$6\ (mod\ 19)$	646285	$0\ (mod\ 19)$
145		646291	
151		646297	
157	$3\ (mod\ 7)$	646303	$0\ (mod\ 7)$
163		646309	
169		646315	
175	$6\ (mod\ 13)$	646321	$0\ (mod\ 13)$
181	$5\ (mod\ 11)$	646327	$0\ (mod\ 11)$
187		646333	
193		646339	
199	$3\ (mod\ 7)$	646345	$0\ (mod\ 7)$
205		646351	
211	$7\ (mod\ 17)$	646357	$0\ (mod\ 17)$
217		646363	
223		646369	
229		646375	
235		646381	
241	$3\ (mod\ 7)$	646387	$0\ (mod\ 7)$
247	$5\ (mod\ 11)$	646393	$0\ (mod\ 11)$

La réponse à notre question familière "Pourquoi les congruences à x ne *remplissent-elles pas tous les trous* correspondant aux nombres premiers de l'intervalle initial ?" est que l'on ne peut obtenir une bijection entre des congruences à $r\ (mod\ m), r \neq 0$ et des congruences à $0\ (mod\ m)$ en restant sur un même intervalle, le seul moyen d'obtenir une telle bijection est de changer d'intervalle, comme présenté dans la table page 3. C'est pour cette raison qu'il y a au moins un nombre premier qui, vérifiant toutes les incongruences à x nécessaires, a son complémentaire à x qui est premier également et ce nombre premier est un décomposant de Goldbach de x.

Minorer le nombre de décomposants de Goldbach

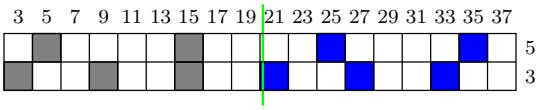
Denise Vella-Chemla

1/4/13

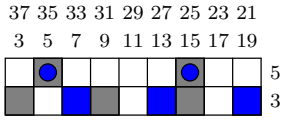
La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.

Les décomposants de Goldbach d'un nombre pair peuvent être caractérisés ainsi : un entier $m \in]\sqrt{n}, n/2]$ qui n'est divisible par aucun des nombres premiers $p < \sqrt{n}$ et dont le complémentaire à n qui est $n - m$ n'est pas non-plus divisible par p est un décomposant de Goldbach de n.

Découvrons graphiquement les décompositions de Goldbach du nombre pair 40 de sommants supérieurs à $\sqrt{40} = 6, ...$ On note en gris la divisibilité des nombres compris entre 3 et $n/2$ par les nombres premiers inférieurs à $\sqrt{n}$ et en bleu la divisibilité des nombres compris entre $n/2$ et n par ces mêmes nombres premiers.



En référence à l'arithmétique des tissus de Lucas, procédons à ce que l'on peut appeler un "pliage du tissu" autour de $n/2$ (le long de la ligne verte).



On obtient la grille ci-dessus, dont la longueur est réduite de moitié, et dans laquelle, trivialement, les décompositions de Goldbach de 40, dont les sommants sont supérieurs à $\sqrt{40}$, correspondent aux colonnes dans lesquelles aucune case n'est colorée.

On comprend aisément que parmi les nombres premiers de l'intervalle $]\sqrt{n}, n/2]$, seuls seront conservés ceux qui ne sont pas congrus à n selon un module premier inférieur à $\sqrt{n}$.

On peut donc minorer le nombre de décomposants de Goldbach de n en éliminant de l'ensemble des nombres premiers de l'intervalle $]\sqrt{n}, n/2]$ les nombres appartenant à une seule classe de congruence (la classe de congruence de n) selon tout module premier p inférieur à $\sqrt{n}$*.

Il semble ainsi naturel de minorer $dg(n)$, le nombre de décomposants de Goldbach de n ainsi :

$$dg(n) \quad \geqslant (\pi(n/2) - \pi(\sqrt{n})) \prod_{p \leqslant \sqrt{n}} \frac{p-1}{p}$$

Le nombre de nombres premiers compris entre $\sqrt{n}$ et $n/2$ croît de 1 à chaque pair double d'un nombre premier, mais décroît de 1 à chaque pair de la forme $p^2 + 1$ avec p premier. On peut utiliser pour minorer ce nombre la minoration fournie par Tchebychev.

*Dans la mesure où il faudrait éliminer les nombres premiers de la classe de congruence de n seulement selon les modules premiers ne divisant pas n, on doit, en éliminant une classe de congruence de manière systématique, indépendamment du fait que le module considéré soit ou ne soit pas un diviseur de n, minorer le nombre de décomposants de Goldbach.

Rosser et Schoenfeld (1962) fournissent la minoration suivante (pour $x \geqslant 285$):

$$\prod_{p \leqslant x} \left(1 - \frac{1}{p}\right) > \frac{e^{-\gamma}}{log\ x} \left(1 - \frac{1}{2(log\ x)^2}\right)$$

On pourrait donc penser que (pour $x \geqslant 285$) :

$$dg(n) \quad \geqslant \left(\frac{n\ log\ 2}{2(log\ n + log\ 0.5)} - \frac{2\ \sqrt{n}\ log\ 2}{log\ n}\right) \frac{e^{-\gamma}}{log\ x} \left(1 - \frac{1}{2(log\ x)^2}\right)$$

Mais un professeur nous explique que les termes d'erreur devenant trop importants par rapport aux termes principaux, une telle approche de la conjecture de Goldbach est inenvisageable.

Théorie des groupes et Conjecture de Goldbach

Denise Vella-Chemla

26 janvier 2013

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair n plus grand que 2 est la somme de deux nombres premiers. Dans la suite, on n'étudie pas les nombres pairs vérifiant trivialement la conjecture de Goldbach, de la forme $2p$ avec p premier.

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 $n/2$. On prend pour convention de noter les classes d'équivalence par leur plus petit représentant positif.

Notons $G_n = (\mathbb{Z}/n\mathbb{Z})^*/\{1,-1\}$, le quotient de $(\mathbb{Z}/n\mathbb{Z})^*$ par le sous groupe $\{1,-1\}$.

2 Exemples

Les données qui suivent ont été trouvées en utilisant le logiciel de programmation basé sur la théorie des groupes GAP.

2.1 $n = 88 = 2^3.11$

Intéressons-nous à G_{88}. Les éléments de G_{88} au nombre de 20 ($= \varphi(88)/2$), sont les nombres premiers à 88 : $1, 3, 5, 7, 9, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 35, 37, 39, 41, 43$ et inférieurs à $44 = 88/2$. Les tailles des classes des éléments de G_{88} sont bien systématiquement des diviseurs de $10 = 11 - 1$.

$G_{88} = C10 \times C2$.

Ecrivons les puissances des éléments de G_{88} (sauf 1) qui séparent le groupe en sous-groupes :

3 : $(1, 3, 9, 27, 7, 21, 25, 13, 39, 29)$ $(5, 15, 43, 41, 35, 17, 37, 23, 19, 31)$,

5 : $(1, 5, 25, 37, 9, 43, 39, 19, 7, 35)$ $(3, 15, 13, 23, 27, 41, 29, 31, 21, 17)$,

7 : $(1, 7, 39, 9, 25)$ $(3, 21, 29, 27, 13)$ $(5, 35, 19, 43, 37)$ $(15, 17, 31, 41, 23)$,

9 : $(1, 9, 7, 25, 39)$ $(3, 27, 21, 13, 29)$ $(5, 43, 35, 37, 19)$ $(15, 41, 17, 23, 31)$,

13 : $(1, 13, 7, 3, 39, 21, 9, 29, 25, 27)$ $(5, 23, 35, 15, 19, 17, 43, 31, 37, 41)$,

15 : $(1, 15, 39, 31, 25, 23, 7, 17, 9, 41)$ $(3, 43, 29, 5, 13, 19, 21, 37, 27, 35)$,

17 : $(1, 17, 25, 15, 9, 23, 39, 41, 7, 31)$ $(3, 37, 13, 43, 27, 19, 29, 35, 21, 5)$,

19 : $(1,19,9,5,7,43,25,35,39,37)$ $(3,31,27,15,21,41,13,17,29,23)$,

21 : $(1,21)$ $(3,25)$ $(5,17)$ $(7,29)$ $(9,13)$ $(15,37)$ $(19,41)$ $(23,43)$ $(27,39)$ $(31,35)$,

23 : $(1,23)$ $(3,19)$ $(5,27)$ $(7,15)$ $(9,31)$ $(13,35)$ $(17,39)$ $(21,43)$ $(25,41)$ $(29,37)$,

25 : $(1,25,9,39,7)$ $(3,13,27,29,21)$ $(5,37,43,19,35)$ $(15,23,41,31,17)$,

27 : $(1,27,25,29,9,21,39,3,7,13)$ $(5,41,37,31,43,17,19,15,35,23)$,

29 : $(1,29,39,13,25,21,7,27,9,3)$ $(5,31,19,23,37,17,35,41,43,15)$,

31 : $(1,31,7,41,39,23,9,15,25,17)$ $(3,5,21,35,29,19,27,43,13,37)$,

35 : $(1,35,7,19,39,43,9,37,25,5)$ $(3,17,21,31,29,41,27,23,13,15)$,

37 : $(1,37,39,35,25,43,7,5,9,19)$ $(3,23,29,17,13,41,21,15,27,31)$,

39 : $(1,39,25,7,9)$ $(3,29,13,21,27)$ $(5,19,37,35,43)$ $(15,31,23,17,41)$,

41 : $(1,41,9,17,7,23,25,31,39,15)$ $(3,35,27,37,21,19,13,5,29,43)$,

43 : $(1,43)$ $(3,41)$ $(5,39)$ $(7,37)$ $(9,35)$ $(13,31)$ $(15,29)$ $(17,27)$ $(19,25)$ $(21,23)$

On est tenté de regrouper certains éléments sous-prétexte que leurs puissances appartiennent à des ensembles égaux (si ce n'est que leurs éléments sont trouvés dans des ordres différents.

On regroupe les éléments 2 par 2, selon que leur produit est congru à ± 1 ($mod\ n$).
Ainsi, il semble naturel de regrouper 3 et 29.
On regroupe également 13 et 27, ou bien 15 et 41, ou encore 17 et 31, ainsi que 5 et 35, ou enfin 19 et 37.
Dans chacun de ces ensembles, on trouve un décomposant de Goldbach de 88.
En effet, $5, 17, 29$ et 41 sont des décomposants de Goldbach de 88.

2.2 Etude d'autres cas pour lesquels G_n n'est pas un groupe cyclique

- $n = 24 = 2^3.3$
  Groupe : C2×C2
  $G_{24} = \{1,5,7,11\}$.

  5 : (1,5) (7,11)
  7 : (1,7) (5,11)
  11 : (1,11) (5,7)

  Décomposants de Goldbach de 24 : 5, 7, 11.

- $n = 40 = 2^3.5$
  Groupe : C4×C2
  $G_{40} = \{1,3,7,9,11,13,17,19\}$.

  3 : (1,3,9,13) (7,17,19,11)
  7 : (1,7,9,17) (3,19,13,11)
  9 : (1,9) (3,13) (7,17) (11,19)
  11 : (1,11) (3,7) (9,19) (17,13)
  13 : (1,13,9,3) (7,11,17,19)
  17 : (1,17,9,7) (3,11,13,19)
  19 : (1,19) (3,17) (7,13) (9,11)

Décomposants de Goldbach de 40 : 3, 11, 17.

On regroupe 3 et 13 d'une part, 7 et 17 d'autre part.
Chaque regroupement contient un décomposant de Goldbach de 40.

- $n = 48 = 2^4.3$
Groupe : C4×C2
$G_{48} = \{1, 5, 7, 11, 13, 17, 19, 23\}$.

5 : (1,5,23,19) (7,13,17,11)
7 : (1,7) (5,13) (11,19) (17,23)
11 : (1,11,23,13) (5,7,19,17)
13 : (1,13,23,11) (5,17,19,7)
17 : (1,17) (5,11) (7,23) (13,19)
19 : (1,19,23,5) (7,11,17,13)
23 : (1,23) (5,19) (7,17) (11,13)

Décomposants de Goldbach de 48 : 5, 7, 11, 17, 19.

On regroupe 5 et 19 d'une part, 11 et 13 d'autre part.
Chaque regroupement contient un décomposant de Goldbach de 48.

- $n = 56 = 2^3.7$
Groupe : C6×C2
$G_{56} = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$.

3 : (1,3,9,27,25,19) (5,15,11,23,13,17)
5 : (1,5,25,13,9,11) (3,15,19,17,27,23)
9 : (1,9,25) (3,27,19) (5,11,13) (15,23,17)
11 : (1,11,9,13,25,5) (3,23,27,17,19,15)
13 : (1,13) (3,17) (5,9) (11,25) (15,27) (19,23)
15 : (1,15) (3,11) (5,19) (9,23) (13,27) (17,25)
17 : (1,17,9,15,25,23) (3,5,27,11,19,13)
19 : (1,19,25,27,9,3) (5,17,13,23,11,15)
23 : (1,23,25,15,9,17) (3,13,19,11,27,5)
25 : (1,25,9) (3,19,27) (5,13,11) (15,17,23)
27 : (1,27) (3,25) (5,23) (9,19) (11,17) (13,15)

Décomposants de Goldbach de 56 : 3, 13, 19.

On regroupe 3 et 19 d'une part, 5 et 11 d'autre part et enfin 17 et 23.
Deux regroupements des trois ci-dessous contiennent un décomposant de Goldbach de 56.

- $n = 60 = 2^2.3.5$
Groupe : C4×C2
$G_{60} = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

7 : (1,7,11,17) (13,29,23,19)
11 : (1,11) (7,17) (13,23) (19,29)
13 : (1,13,11,23) (7,29,17,19)
17 : (1,17,11,7) (13,19,23,29)
19 : (1,19) (7,13) (11,29) (17,23)
23 : (1,23,11,13) (7,19,17,29)
29 : (1,29) (7,23) (11,19) (13,17)

Décomposants de Goldbach de 60 : 7, 13, 17, 19, 23, 29.

On regroupe 7 et 17 d'une part, 13 et 23 d'autre part.
Les regroupements contiennent chacun un décomposant de Goldbach de 60 (et même deux).

- $n = 72 = 2^3.3^2$
  Groupe : C6×C2
  $G_{72} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.

  5 : (1,5,25,19,23,29) (7,35,31,11,17,13)
  7 : (1,7,23,17,25,31) (5,35,29,13,19,11)
  11 : (1,11,23,35,25,13) (5,17,29,31,19,7)
  13 : (1,13,25,35,23,11) (5,7,19,31,29,17)
  17 : (1,17) (5,13) (7,25) (11,29) (19,35) (23,31)
  19 : (1,19) (5,23) (7,11) (13,31) (17,35) (25,29)
  23 : (1,23,25) (5,29,19) (7,17,31) (11,35,13)
  25 : (1,25,23) (5,19,29) (7,31,17) (11,13,35)
  29 : (1,29,23,19,25,5) (7,13,17,11,31,35)
  31 : (1,31,25,17,23,7) (5,11,19,13,29,35)
  35 : (1,35) (5,31) (7,29) (11,25) (13,23) (17,19)

  Décomposants de Goldbach de 72 : 5, 11, 13, 19, 29, 31

  On regroupe 5 et 29 d'une part, 7 et 31 d'autre part et enfin 11 et 13.
  Les regroupements contiennent chacun un décomposant de Goldbach de 72 (et même parfois deux).

- $n = 80 = 2^4.5$
  Groupe : C4xC4
  $G_{80} = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$.

  3 : (1,3,9,27) (7,21,17,29) (11,33,19,23) (13,39,37,31)
  7 : (1,7,31,23) (3,21,13,11) (9,17,39,33) (19,27,29,37)
  9 : (1,9) (3,27) (7,17) (11,19) (13,37) (21,29) (23,33) (31,39)
  11 : (1,11,39,29) (3,33,37,7) (9,19,31,21) (13,17,27,23)
  13 : (1,13,9,37) (3,39,27,31) (7,11,17,19) (21,33,29,23)
  17 : (1,17,31,33) (3,29,13,19) (7,39,23,9) (11,27,21,37)
  19 : (1,19,39,21) (3,23,37,17) (7,27,33,13) (9,11,31,29)
  21 : (1,21,39,19) (3,17,37,23) (7,13,33,27) (9,29,31,11)
  23 : (1,23,31,7) (3,11,13,21) (9,33,39,17) (19,37,29,27)
  27 : (1,27,9,3) (7,29,17,21) (11,23,19,33) (13,31,37,39)
  29 : (1,29,39,11) (3,7,37,33) (9,21,31,19) (13,23,27,17)
  31 : (1,31) (3,13) (7,23) (9,39) (11,21) (17,33) (19,29) (27,37)
  33 : (1,33,31,17) (3,19,13,29) (7,9,23,39) (11,37,21,27)
  37 :(1,37,9,13) (3,31,27,39) (7,19,17,11) (21,23,29,33)
  39 : (1,39) (3,37) (7,33) (9,31) (11,29) (13,27) (17,23) (19,21)

  Décomposants de Goldbach de 80 : 7, 13, 19, 37.

  On regroupe 3 et 27 d'une part, 7 et 23 d'autre part, également 11 et 29 ou bien 13 et 37 ou encore 17 et 33, et enfin 19 et 21.
  Trois regroupements contiennent un décomposant de Goldbach de 80 (et un regroupement en contient deux).

- $n = 84 = 2^2.3.7$
  Groupe : C6xC2
  $G_{84} = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.\}$

  5 : (1,5,25,41,37,17)(11,29,23,31,13,19)
  11 : (1,11,37,13,25,23) (5,29,17,19,41,31)
  13 : (1,13) (5,19) (11,25) (17,31) (23,37) (29,41)
  17 : (1,17,37,41,25,5) (11,19,13,31,23,29)
  19 : (1,19,25,29,37,31) (5,11,41,23,17,13)
  23 : (1,23,25,13,37,11) (5,31,41,19,17,29)
  25 : (1,25,37) (5,41,17) (11,23,13) (19,29,31)
  29 : (1,29) (5,23) (11,17) (13,41) (19,37) (25,31)

31 : (1,31,37,29,25,19) (5,13,17,23,41,11)
37 : (1,37,25) (5,17,41) (11,13,23) (19,31,29)
41 : (1,41) (5,37) (11,31) (13,29) (17,25) (19,23)

Décomposants de Goldbach de 84 : 5, 11, 13, 17, 23, 31, 37, 41.

On regroupe 5 et 17 d'une part, 11 et 23 d'autre part, également 19 et 31 et enfin 25 et 37.
Tous les regroupements contiennent un décomposant de Goldbach de 84 (et parfois même deux).

- $n = 96 = 2^5.3$
  Groupe : C8xC2
  $G_{96} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47\}$.

  5 : (1,5,25,29,47,43,23,19) (7,35,17,11,41,13,31,37)
  7 : (1,7,47,41) (5,35,43,13) (11,19,37,29) (17,23,31,25)
  11 : (1,11,25,13,47,37,23,35) (5,41,29,31,43,7,19,17)
  13 : (1,13,23,11,47,35,25,37) (5,31,19,41,43,17,29,7)
  17 : (1,17) (5,11) (7,23) (13,29) (19,35) (25,41) (31,47) (37,43)
  19 : (1,19,23,43,47,29,25,5) (7,37,31,13,41,11,17,35)
  23 : (1,23,47,25) (5,19,43,29) (7,31,41,17) (11,35,37,13)
  25 : (1,25,47,23) (5,29,43,19) (7,17,41,31) (11,13,37,35)
  29 : (1,29,23,5,47,19,25,43) (7,11,31,35,41,37,17,13)
  31 : (1,31) (5,37) (7,25) (11,43) (13,19) (17,47) (23,41) (29,35)
  35 : (1,35,23,37,47,13,25,11) (5,17,19,7,43,31,29,41)
  37 : (1,37,25,35,47,11,23,13) (5,7,29,17,43,41,19,31)
  41 : (1,41,47,7) (5,13,43,35) (11,29,37,19) (17,25,31,23)
  43 : (1,43,25,19,47,5,23,29) (7,13,17,37,41,35,31,11)
  47 : (1,47) (5,43) (7,41) (11,37) (13,35) (17,31) (19,29) (23,25)

  Décomposants de Goldbach de 96 : 7, 13, 17, 23, 29, 37, 43.

  On regroupe 5 et 19, 7 et 41, 11 et 35, 13 et 37, 19 et 29, 23 et 25 et enfin 29 et 43.
  Tous les regroupements contiennent un décomposant de Goldbach de 96.

Il semblerait que pour les nombres pairs n tels que G_n n'est pas cyclique, G_n est souvent égal à $C_{\varphi(n)/4} \times C2$ sauf dans le cas où $\varphi(n)/2$ est un carré (par exemple lorsque $n = 80$) auquel cas $G_n = C_{\sqrt{\varphi(n)/2}} \times C_{\sqrt{\varphi(n)/2}}$.

Il semblerait que les décomposants de Goldbach de n soient à rechercher dans les sous-groupes de G_n d'ordres les plus grands possibles (de taille $\varphi(n)/4$ dans tous les cas étudiés sauf pour $n = 80$ où l'ordre des sous-groupes des décomposants de Goldbach est égal à $\varphi(n)/8$).

3 Cas pour lesquels G_n est un groupe cyclique

Lorsque G_n est un groupe cyclique, il semblerait qu'on trouve systématiquement un générateur de ce groupe qui est un décomposant de Goldbach de n.

Ces cas sont nombreux : ils concernent tous les pairs doubles d'impairs (nombres pairs n de la forme $4k + 2$), tous les doubles de doubles de nombres premiers (nombres pairs n de la forme $4p$ avec p premier impair) ainsi que tous les nombres pairs qui sont des puissances de 2.

- $n = 8 = 2^3$
  Groupe : C2
  $G_8 = \{1, 3\}$
  Générateur du groupe : 3.
  Décomposant de Goldbach de 8 : 3.

- $n = 12 = 2^2.3$
  Groupe : C2
  $G_{12} = \{1, 5\}$
  Générateur du groupe : 5.
  Décomposant de Goldbach de 12 : 5.

- $n = 16 = 2^4$
  Groupe : C4
  $G_{16} = \{1, 3, 5, 7\}$
  Générateurs du groupe : 3, 5.
  Décomposants de Goldbach de 16 : 3, 5.

- $n = 18 = 2.3^2$
  Groupe : C3
  $G_{18} = \{1, 5, 7\}$
  Générateurs du groupe : 5, 7.
  Décomposants de Goldbach de 18 : 5, 7.

- $n = 20 = 2^2.5$
  Groupe : C4
  $G_{20} = \{1, 3, 7, 9\}$
  Générateurs du groupe : 3, 7.
  Décomposants de Goldbach de 20 : 3, 7.

- $n = 28 = 2^2.7$
  Groupe : C6
  $G_{28} = \{1, 3, 5, 9, 11, 13\}$
  Générateurs du groupe : 5, 11.
  Décomposants de Goldbach de 28 : 5, 11.

- $n = 30 = 2.3.5$
  Groupe : C4
  $G_{30} = \{1, 7, 11, 13\}$
  Générateurs du groupe : 7, 13.
  Décomposants de Goldbach de 30 : 7, 11, 13.

- $n = 32 = 2^5$
  Groupe : C8*
  $G_{32} = \{1, 3, 5, 7, 9, 11, 13, 15\}$
  Générateurs du groupe : 3, 5, 11, 13.
  Décomposants de Goldbach de 32 : 3, 13.

- $n = 36 = 2^2.3^2$
  Groupe : C6
  $G_{36} = \{1, 5, 7, 11, 13, 17\}$
  Générateurs du groupe : 5, 7.
  Décomposants de Goldbach de 36 : 5, 7, 13, 17.

- $n = 42 = 2.3.7$
  Groupe : C6
  $G_{42} = \{1, 5, 11, 13, 17, 19\}$
  Générateurs du groupe : 11, 19.
  Décomposants de Goldbach de 42 : 5, 11, 13, 19.

- $n = 44 = 2^2.11$
  Groupe : C10
  $G_{44} = \{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$
  Générateurs du groupe : 3, 13, 15, 17.
  Décomposants de Goldbach de 44 : 3, 7, 13.

*Complémentaire : C4×C2

- $n = 50 = 2.5^2$
  Groupe : C10
  $G_{50} = \{1, 3, 7, 9, 11, 13, 17, 19, 21, 23\}$
  Générateurs du groupe : 3, 13, 17, 23.
  Décomposants de Goldbach de 50 : 3, 7, 13, 19.

- $n = 52 = 2^2.13$
  Groupe : C12
  $G_{52} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$
  Générateurs du groupe : 7, 11, 15, 19.
  Décomposants de Goldbach de 52 : 5, 11, 23.

- $n = 54 = 2.3^3$
  Groupe : C9[†]
  $G_{54} = \{1, 5, 7, 11, 13, 17, 19, 23, 25\}$
  Générateurs du groupe : 5, 7, 11, 13, 23, 25.
  Décomposants de Goldbach de 54 : 7, 11, 13, 17, 23.

- $n = 64 = 2^6$
  Groupe : C16
  $G_{64} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31\}$
  Générateurs du groupe : 3, 5, 11, 13, 19, 21, 27, 29.
  Décomposants de Goldbach de 64 : 3, 5, 11, 17, 23.

- $n = 66 = 2.3.11$
  Groupe : C10
  $G_{66} = \{1, 5, 7, 13, 17, 19, 23, 25, 29, 31\}$
  Générateurs du groupe : 5, 7, 13, 19.
  Décomposants de Goldbach de 66 : 5, 7, 13, 19, 23, 29.

- $n = 68 = 2^2.17$
  Groupe : C16
  $G_{68} = \{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 33\}$
  Générateurs du groupe : 3, 5, 7, 11, 23, 27, 29, 31.
  Décomposants de Goldbach de 68 : 7, 31.

- $n = 70 = 2.5.7$
  Groupe : C12
  $e_{70} = \{1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33\}$
  Générateurs du groupe : 3, 17, 23, 33.
  Décomposants de Goldbach de 68 : 3, 11, 17, 23, 29.

- $n = 76 = 2^2.19$
  Groupe : C18
  $G_{76} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 21, 23, 25, 27, 29, 31, 33, 35, 37\}$
  Générateurs du groupe : 13, 23, 25, 29, 33, 35.
  Décomposants de Goldbach de 68 : 3, 5, 17, 23, 29.

- $n = 78 = 2.3.13$
  Groupe : C12
  $G_{78} = \{1, 5, 7, 11, 17, 19, 23, 25, 29, 31, 35, 37\}$
  Générateurs du groupe : 7, 11, 19, 37.
  Décomposants de Goldbach de 68 : 5, 7, 11, 17, 19, 31, 37.

- $n = 90 = 2.3^2.5$
  Groupe : C12
  $G_{90} = \{1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43\}$
  Générateurs du groupe : 7, 13, 23, 43.
  Décomposants de Goldbach de 68 : 7, 11, 17, 19, 23, 29, 31, 37, 43.

[†]Complémentaire : C9

- $n = 92 = 2^2.23$
  Groupe : C22
  $G_{92} = \{1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45\}$
  Générateurs du groupe : 3, 5, 17, 21, 27, 31, 33, 35, 37, 39.
  Décomposants de Goldbach de 68 : 3, 13, 19, 31.

- $n = 98 = 2.7^2$
  Groupe : C21
  $G_{98} = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27, 29, 31, 33, 37, 39, 41, 43, 45, 47\}$
  Générateurs du groupe : 3, 5, 9, 11, 17, 23, 25, 33, 37, 39, 45, 47.
  Décomposants de Goldbach de 68 : 19, 31, 37

Application double du crible d'Eratosthène pour trouver les décomposants de Goldbach d'un nombre pair

Denise Vella-Chemla

1/12/2012

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.

Rappelons ici qu'un décomposant de Goldbach d'un nombre pair donné x doit vérifier deux propriétés : la première est qu'il doit être premier, la seconde est qu'il ne doit être congru à x selon aucun nombre premier inférieur ou égal à $\sqrt{x}$, ce qui garantit que son complémentaire à x est premier également*.

2 Exemple du nombre pair 500 : détail de l'application double du crible d'Eratosthène

On détaille ici pour le nombre pair 500 ce qu'on appellera l'application double du crible d'Eratosthène :

1) la première application du crible consiste à éliminer les nombres congrus à 0 selon un module premier inférieur ou égal à $\sqrt{x}$ (de manière à éliminer les nombres composés et les petits premiers inférieurs ou égaux à $\sqrt{x}$) ;

2) la deuxième application du crible consiste à éliminer les nombres congrus à x selon un module premier inférieur ou égal à $\sqrt{x}$.

500 étant congru à 2 selon le module 3, les seuls nombres à considérer sont ceux appartenant à la progression arithmétique $500 - 1 - 6k$, de 7 à 247.

On note dans la deuxième colonne le passage de la première passe du crible (élimination des nombres congrus à 0 selon un module inférieur ou égal à $\sqrt{x} = 22, ...$). Les modules à considérer sont 5, 7, 11, 13, 17, 19.

On note dans la troisième colonne le passage de la seconde passe du crible en spécifiant la congruence partagée avec x.
500 est congru à 0 (mod 5), 3 (mod 7), 5 (mod 11), 6 (mod 13), 7 (mod 17) *et* 6 (mod 19).
Les couleurs permettent de bien visualiser les périodicités.

*Un nombre premier appartient à l'une des deux progressions arithmétiques $6k - 1$ ou $6k + 1$. A cause de la deuxième propriété des décomposants de Goldbach de x, les nombres pairs x divisibles par 3 (les $6k$) peuvent avoir des décomposants de Goldbach dans les deux progressions $x + 1 - 6k$ ou $x - 1 - 6k$. Les nombres congrus à 1 selon le module 3 (les $6k + 4$) n'ont des décomposants que dans la progression arithmétique $x + 1 - 6k$ tandis que ceux congrus à -1 selon le module 3 (les $6k + 2$) n'ont des décomposants que dans la progression arithmétique $x - 1 - 6k$.

7	$0\ (mod\ 7)$	$7\ (mod\ 17)$
13	$0\ (mod\ 13)$	
19	$0\ (mod\ 19)$	$6\ (mod\ 13)$
25	$0\ (mod\ 5)$	$0\ (mod\ 5)\ et\ 6\ (mod\ 19)$
31		$3\ (mod\ 7)$
37		
43		
49	$0\ (mod\ 7)$	$5\ (mod\ 11)$
55	$0\ (mod\ 5\ et\ 11)$	$0\ (mod\ 5)$
61		
67		
73		$3\ (mod\ 7)$
79		
85	$0\ (mod\ 5\ et\ 17)$	$0\ (mod\ 5)$
91	$0\ (mod\ 7\ et\ 13)$	
97		$6\ (mod\ 13)$
103		
109		$7\ (mod\ 17)$
115	$0\ (mod\ 5)$	$0\ (mod\ 5)\ et\ 3\ (mod\ 7)\ et\ 5\ (mod\ 11)$
121	$0\ (mod\ 11)$	
127		
133	$0\ (mod\ 7\ et\ 19)$	
139		$6\ (mod\ 19)$
145	$0\ (mod\ 5)$	$0\ (mod\ 5)$
151		
157		$3\ (mod\ 7)$
163		
169	$0\ (mod\ 13)$	
175	$0\ (mod\ 5\ et\ 7)$	$0\ (mod\ 5)\ et\ 6\ (mod\ 13)$
181		$5\ (mod\ 11)$
187	$0\ (mod\ 11\ et\ 17)$	
193		
199		$3\ (mod\ 7)$
205	$0\ (mod\ 5)$	$0\ (mod\ 5)$
211		$7\ (mod\ 17)$
217	$0\ (mod\ 7)$	
223		
229		
235	$0\ (mod\ 5)$	$0\ (mod\ 5)$
241		$3\ (mod\ 7)$
247	$0\ (mod\ 13\ et\ 19)$	$5\ (mod\ 11)$

Dit familièrement, "pourquoi les congruences à x ne *bouchent-elles pas tous les trous* correspondant aux nombres premiers de l'intervalle initial ?

Présentons une idée qui peut être intéressante : on peut considérer que l'élimination des nombres dans la troisième colonne consiste à appliquer le crible d'Eratosthène, moyennant une translation adéquate à partir du nombre origine 0. On remplace chaque congruence à un nombre non-nul (telle que $x \equiv r\ (mod\ m)$) par la congruence correspondante $x + \delta \equiv 0\ (mod\ m)$ avec δ bien choisi.
Pour l'exemple du nombre pair 500, le système de congruences permettant de trouver l'intervalle "translaté" est le suivant :

$$\begin{cases} x \equiv 1\ (mod\ 6) \\ x \equiv 0\ (mod\ 17) \\ x + 12 \equiv 0\ (mod\ 13) \\ x + 18 \equiv 0\ (mod\ 19) \\ x + 24 \equiv 0\ (mod\ 7) \\ x + 42 \equiv 0\ (mod\ 11) \end{cases}$$

Ce système est équivalent au système : $\begin{cases} x \equiv 1 \ (mod\ 6) \\ x \equiv 4 \ (mod\ 7) \\ x \equiv 2 \ (mod\ 11) \\ x \equiv 1 \ (mod\ 13) \\ x \equiv 0 \ (mod\ 17) \\ x \equiv 1 \ (mod\ 19) \end{cases}$ de plus petite solution le nombre 646153.

On voit ainsi apparaître une judicieuse bijection entre les nombres x de l'intervalle initial $[7, 247]$ et les nombres $y = x + 646146$ de l'intervalle $[646153, 646393]$ telle que $x \equiv r \ (mod\ m) \iff y \equiv 0 \ (mod\ m)$.

7	$7 \ (mod\ 17)$	646153	$0 \ (mod\ 17)$
13		646159	
19	$6 \ (mod\ 13)$	646165	$0 \ (mod\ 13)$
25	$6 \ (mod\ 19)$	646171	$0 \ (mod\ 19)$
31	$3 \ (mod\ 7)$	646177	$0 \ (mod\ 7)$
37		646183	
43		646189	
49	$5 \ (mod\ 11)$	646195	$0 \ (mod\ 11)$
55		646201	
61		646207	
67		646213	
73	$3 \ (mod\ 7)$	646219	$0 \ (mod\ 7)$
79		646225	
85		646231	
91		646237	
97	$6 \ (mod\ 13)$	646243	$0 \ (mod\ 13)$
103		646249	
109	$7 \ (mod\ 17)$	646255	$0 \ (mod\ 17)$
115	$3 \ (mod\ 7)$ *et* $0 \ (mod\ 11)$	646261	$0 \ (mod\ 7)$ *et* $0 \ (mod\ 11)$
121		646267	
127		646273	
133		646279	
139	$6 \ (mod\ 19)$	646285	$0 \ (mod\ 19)$
145		646291	
151		646297	
157	$3 \ (mod\ 7)$	646303	$0 \ (mod\ 7)$
163		646309	
169		646315	
175	$6 \ (mod\ 13)$	646321	$0 \ (mod\ 13)$
181	$5 \ (mod\ 11)$	646327	$0 \ (mod\ 11)$
187		646333	
193		646339	
199	$3 \ (mod\ 7)$	646345	$0 \ (mod\ 7)$
205		646351	
211	$7 \ (mod\ 17)$	646357	$0 \ (mod\ 17)$
217		646363	
223		646369	
229		646375	
235		646381	
241	$3 \ (mod\ 7)$	646387	$0 \ (mod\ 7)$
247	$5 \ (mod\ 11)$	646393	$0 \ (mod\ 11)$

On peut donc considérer qu'on élimine sensiblement la même quantité de nombres dans les deux passes du crible. Le détail de la quantité de nombres éliminée selon chaque module est fourni dans le tableau ci-après. Le lemme de Gauss de l'article 127 des Recherches arithmétiques nous indique cela si ce n'est que les nombres sont consécutifs au lieu d'appartenir à des progressions arithmétiques (on aurait pu de toute façon ici se ramener à des suites de nombres consécutifs, les progressions arithmétiques en $6k$ n'étant utiles que pour alléger la présentation de cet exemple).

module	5	7	11	13	17	19
quantité de nbs éliminés par la première passe	8	6	3	4	2	3
quantité de nbs éliminés par la deuxième passe	8	6	3	3	3	2

On élimine 19 nombres sur 41 dans la colonne de gauche et 22 nombres sur 41 dans celle de droite. Il faudrait être capable de dénombrer les chevauchements pour montrer que même dans le cas où il y aurait le moins de chevauchements possibles, il resterait des nombres décomposants de Goldbach de x.

Considérons maintenant les nombres premiers de l'intervalle "translaté". A chacun d'eux correspond par bijection un nombre de l'intervalle initial $[7, 247]$. Chacun de ces nombres, s'il est premier, constituera un décomposant de Goldbach de x.
A 646159, premier, correspond 13, qui ne nous intéresse pas car inférieur à $\sqrt{500} = 22, ...$
A 646183, premier, correspond le nombre premier 37, décomposant de Goldbach de 500.
A 646189, premier, correspond le nombre premier 43, décomposant de Goldbach de 500.
A 646237, premier, correspond 91 qui n'est pas premier.
A 646267, premier, correspond 121 qui n'est pas premier.
A 646273, premier, correspond le nombre premier 127, décomposant de Goldbach de 500.
A 646309, premier, correspond le nombre premier 163, décomposant de Goldbach de 500.
A 646339, premier, correspond le nombre premier 193, décomposant de Goldbach de 500.

Les autres décomposants de Goldbach trouvés pour 500 ne sont pas en bijection avec des nombres premiers de l'intervalle translaté ; peut-être pourrions-nous nous passer d'eux pour aboutir à une démonstration...

Il est important de noter que le théorème des restes chinois nous assure de l'existence d'une infinité d"'intervalles translatés", qui peuvent être associés à l'intervalle initial.

Par exemple, pour le nombre pair 200, le même traitement fournit comme premier intervalle translaté l'intervalle $[2807, 2907]$ qui par bijection ne fournira que des nombres pairs de l'intervalle initial, qui ne peuvent donc trivialement pas être des décomposants de Goldbach de x. L'intervalle translaté suivant $[5813, 5913]$ (obtenu par addition de $3 \times 7 \times 11 \times 13$ nous fournira une certaine quantité de nombres premiers que l'on pourra "ramener" par translation dans l'intervalle initial à la recherche de nombres premiers plus petits susceptibles d'être des décomposants de Goldbach de x.
A 5813, premier, correspond le nombre premier 7, décomposant de Goldbach de 200.
A 5821, premier, correspond le nombre premier 15, qui n'est pas premier.
A 5827, premier, correspond le nombre premier 21, qui n'est pas premier.
A 5839, premier, correspond le nombre premier 33, qui n'est pas premier.
A 5843, premier, correspond le nombre premier 37, décomposant de Goldbach de 200.
A 5849, premier, correspond le nombre premier 43, décomposant de Goldbach de 200.
A 5851, premier, correspond le nombre premier 45, qui n'est pas premier.
A 5857, premier, correspond le nombre premier 51, qui n'est pas premier.
A 5861, premier, correspond le nombre premier 55, qui n'est pas premier.
A 5867, premier, correspond le nombre premier 61, décomposant de Goldbach de 200.
A 5869, premier, correspond le nombre premier 63, qui n'est pas premier.
A 5879, premier, correspond le nombre premier 73, décomposant de Goldbach de 200.
A 5881, premier, correspond le nombre premier 75, qui n'est pas premier.
A 5897, premier, correspond le nombre premier 91, qui n'est pas premier.
A 5903, premier, correspond le nombre premier 97, décomposant de Goldbach de 200.

Pour le nombre pair 100, le premier intervalle translaté possible, correspondant au système de congruences $\{x \equiv 2 \ (mod\ 3), x \equiv \ 1 \ (mod\ 7)\}$ commence au nombre 8 mais ne nous permet par translation vers l'intervalle initial de n'atteindre que des nombres pairs. On utilise donc le deuxième intervalle translaté fourni par le théorème des restes chinois, qui débute à 29, et qui nous permet par translation de 26 en arrière de trouver les décomposants de Goldbach de 100 que sont 11, 17, 41 *et* 47, qui sont à distance 26

des nombres premiers de cet intervalle $[29, 79]$ que sont $37,\ 43,\ 67$ *et* 73.

Il est étrange de lier ainsi les décomposants de Goldbach d'un nombre aux nombres premiers qui se trouvent appartenir à un intervalle de nombres plus grands que lui sur la droite numérique.

Il faudrait généraliser cette approche et s'assurer que cette nouvelle manière de concevoir la conjecture de Goldbach peut amener à une démonstration.

La réponse à notre question familière "pourquoi les congruences à x ne *bouchent-elles pas tous les trous* correspondant aux nombres premiers de l'intervalle initial ?" est qu'on ne peut obtenir une bijection entre des congruences à r $(mod\ m)$ et des congruences à 0 $(mod\ m)$ en restant sur le même intervalle, le seul moyen d'obtenir une telle bijection est de changer d'intervalle, comme présenté dans le tableau 3. C'est pour cette raison qu'il y a au moins un nombre premier qui, vérifiant toutes les incongruences à x nécessaires, a son complémentaire à x qui est premier également et le nombre premier en question fournit ainsi une décomposition de Goldbach de x.

C'est extra !

Denise Vella-Chemla

28/11/2012

1 Rappels

On se rappelle que dans la démonstration de l'infinité des nombres premiers d'Euclide, le nombre utilisé pour aboutir à une contradiction est égal au produit de tous les nombres premiers (dont on fait l'hypothèse de départ qu'ils sont en nombre fini) augmenté de 1. Ce nombre a comme propriété d'être congru à 1 selon chaque nombre premier du produit considéré comme module.

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.

Rappelons ici qu'un décomposant de Goldbach d'un nombre pair donné x doit vérifier deux propriétés : la première est qu'il doit être premier, la seconde est qu'il ne doit être congru à x selon aucun nombre premier inférieur ou égal à $\sqrt{x}$, ce qui garantit que son complémentaire à x est premier également.

Rappelons enfin que le nombre obtenu en ôtant un multiple de 6 à un nombre a les mêmes restes que (est congru à) ce nombre selon les modules 2 et 3. De même, le nombre obtenu en ôtant un multiple de 30 à un nombre a les mêmes restes que (est congru à) ce nombre selon les modules 2, 3 et 5.

Dernier élément utile : un nombre entier n'est jamais congru à son prédécesseur ou son successeur (au sens de Peano) selon aucun module.

2 Voir les décomposants de Goldbach de x comme appartenant à des progressions arithmétiques depuis le nombre $x+1$ ou depuis le nombre $x-1$

On considère les nombres pairs de 8 à 100 (ainsi que 200 et 500). Pour chacun d'eux, on fournit ses décomposants de Goldbach (les nombres premiers p tels que $x = p + q$ avec q premier également). A côté de chacun de ces décomposants, on note l'opération arithmétique qui permet de l'obtenir, depuis $x+1$ ou $x-1$ et en soustrayant un multiple de 6 (de façon à conserver les restes modulo 2 et 3)*. On notera en rouge les nombres appartenant à une progression arithmétique décroissante de début $x+1$ et en bleu ceux de la progression arithmétique de début $x-1$†.

Si l'on voulait aboutir à une preuve de la conjecture de Goldbach, il faudrait être capable de démontrer que ces multiples nombres, appartenant tous à un même intervalle (l'intervalle $[3, x/2]$) ainsi qu'à l'une de ces deux seules progressions arithmétiques, ne peuvent être congrus entre eux modulo les modules plus grands que 2 et 3, et que l'un d'eux étant ainsi incongru à x selon tout module fournit une décomposition de Goldbach de x.

*Les nombres marqués d'une astérisque sont des doubles de nombres premiers et vérifient donc trivialement la conjecture de Goldbach.

†Pour mémoire, on note d'une étoile en fin de ligne les décomposants de Goldbach de x qui sont des "petits premiers", i.e. des nombres premiers inférieurs à $\sqrt{x}$.

x	$=$	$p+q$	$p=$	$x \pm 1 - 6k$	
8	$=$	$3+5$	$3=$	$8+1-6$	
$10*$	$=$	$3+7$	$3=$	$10-1-6$	$*$
	$=$	$5+5$	$5=$	$10+1-6$	
12	$=$	$5+7$	$5=$	$12-1-6$	
$14*$	$=$	$3+11$	$3=$	$14+1-12$	$*$
	$=$	$7+7$	$7=$	$14-1-6$	
16	$=$	$3+13$	$3=$	$16-1-12$	$*$
	$=$	$5+11$	$5=$	$16+1-12$	
18	$=$	$5+13$	$5=$	$18-1-12$	
	$=$	$7+11$	$7=$	$18+1-12$	
20	$=$	$3+17$	$3=$	$20+1-18$	$*$
	$=$	$7+13$	$7=$	$20-1-12$	
$22*$	$=$	$3+19$	$3=$	$22-1-18$	$*$
	$=$	$5+17$	$5=$	$22+1-18$	
	$=$	$11+11$	$11=$	$22+1-12$	
24	$=$	$5+19$	$5=$	$24-1-18$	
	$=$	$7+17$	$7=$	$24+1-18$	
	$=$	$11+13$	$11=$	$24-1-12$	
$26*$	$=$	$3+23$	$3=$	$26+1-24$	$*$
	$=$	$7+19$	$7=$	$26-1-18$	
	$=$	$13+13$	$13=$	$26-1-12$	
28	$=$	$5+23$	$5=$	$28+1-24$	$*$
	$=$	$11+17$	$11=$	$28+1-18$	
30	$=$	$7+23$	$7=$	$30+1-24$	
	$=$	$11+19$	$11=$	$30-1-18$	
	$=$	$13+17$	$13=$	$30+1-18$	
32	$=$	$3+29$	$3=$	$32-1-18$	$*$
	$=$	$13+19$	$13=$	$32-1-18$	
$34*$	$=$	$3+31$	$3=$	$34-1-30$	$*$
	$=$	$5+29$	$5=$	$34+1-30$	$*$
	$=$	$11+23$	$11=$	$34+1-24$	
	$=$	$17+17$	$17=$	$34+1-18$	
36	$=$	$5+31$	$5=$	$36-1-30$	$*$
	$=$	$7+29$	$7=$	$36+1-30$	
	$=$	$13+23$	$13=$	$36+1-24$	
	$=$	$17+19$	$17=$	$36-1-18$	
$38*$	$=$	$7+31$	$7=$	$38-1-30$	
	$=$	$19+19$	$19=$	$38-1-18$	
40	$=$	$3+37$	$3=$	$40-1-36$	$*$
	$=$	$11+29$	$11=$	$40+1-30$	
	$=$	$17+23$	$17=$	$40+1-24$	
42	$=$	$5+37$	$5=$	$42-1-36$	$*$
	$=$	$11+31$	$11=$	$42-1-30$	
	$=$	$13+29$	$13=$	$42+1-30$	
	$=$	$19+23$	$19=$	$42+1-24$	
44	$=$	$3+41$	$3=$	$44+1-42$	$*$
	$=$	$7+37$	$7=$	$44-1-36$	
	$=$	$13+31$	$13=$	$44-1-30$	
$46*$	$=$	$3+43$	$3=$	$46-1-42$	$*$
	$=$	$5+41$	$5=$	$46+1-42$	$*$
	$=$	$17+29$	$17=$	$46+1-30$	
	$=$	$23+23$	$23=$	$46+1-24$	
48	$=$	$5+43$	$5=$	$48-1-42$	$*$
	$=$	$7+41$	$7=$	$48+1-42$	
	$=$	$11+37$	$11=$	$48-1-36$	
	$=$	$17+31$	$17=$	$48-1-30$	
	$=$	$19+29$	$19=$	$48+1-30$	

50	=	$3+47$	$3=$	$50+1-48$	$*$
	=	$7+43$	$7=$	$50-1-42$	$*$
	=	$13+37$	$13=$	$50-1-36$	
	=	$19+31$	$19=$	$50-1-30$	
52	=	$5+47$	$5=$	$52+1-48$	$*$
	=	$11+41$	$11=$	$52+1-42$	
	=	$23+29$	$23=$	$52+1-30$	
54	=	$7+47$	$7=$	$54+1-48$	$*$
	=	$11+43$	$11=$	$54-1-42$	
	=	$13+41$	$13=$	$54+1-42$	
	=	$17+37$	$17=$	$54-1-36$	
	=	$23+31$	$23=$	$54-1-30$	
56	=	$3+53$	$3=$	$56+1-54$	$*$
	=	$13+43$	$13=$	$56-1-42$	
	=	$19+37$	$19=$	$56-1-36$	
$58*$	=	$5+53$	$5=$	$58+1-54$	$*$
	=	$11+47$	$11=$	$58+1-48$	
	=	$17+41$	$17=$	$58+1-42$	
	=	$29+29$	$29=$	$58+1-30$	
60	=	$7+53$	$7=$	$60+1-54$	$*$
	=	$13+47$	$13=$	$60+1-48$	
	=	$17+43$	$17=$	$60-1-42$	
	=	$19+41$	$19=$	$60+1-42$	
	=	$23+37$	$23=$	$60-1-36$	
	=	$29+31$	$29=$	$60-1-30$	
$62*$	=	$3+59$	$3=$	$62+1-60$	$*$
	=	$19+43$	$19=$	$62-1-42$	
	=	$31+31$	$31=$	$62-1-30$	
64	=	$3+61$	$3=$	$64-1-60$	$*$
	=	$5+59$	$5=$	$64+1-60$	$*$
	=	$11+53$	$11=$	$64+1-54$	
	=	$17+47$	$17=$	$64+1-48$	
	=	$23+41$	$23=$	$64+1-42$	
66	=	$5+61$	$5=$	$66-1-60$	$*$
	=	$7+59$	$7=$	$66+1-60$	$*$
	=	$13+53$	$13=$	$66+1-54$	
	=	$19+47$	$19=$	$66+1-48$	
	=	$23+43$	$23=$	$66-1-42$	
	=	$29+37$	$29=$	$66-1-36$	
68	=	$7+61$	$7=$	$68-1-60$	$*$
	=	$31+37$	$31=$	$68-1-36$	
70	=	$3+67$	$3=$	$70-1-66$	$*$
	=	$11+59$	$11=$	$70+1-60$	
	=	$17+53$	$17=$	$70+1-54$	
	=	$23+47$	$23=$	$70+1-48$	
	=	$29+41$	$29=$	$70+1-42$	
72	=	$5+67$	$5=$	$72-1-66$	$*$
	=	$11+61$	$11=$	$72-1-60$	
	=	$13+59$	$13=$	$72+1-60$	
	=	$19+53$	$19=$	$72+1-54$	
	=	$29+43$	$29=$	$72-1-42$	
	=	$31+41$	$31=$	$72+1-42$	
$74*$	=	$3+71$	$3=$	$74+1-72$	$*$
	=	$7+67$	$7=$	$74-1-66$	$*$
	=	$13+61$	$13=$	$74-1-60$	
	=	$31+43$	$31=$	$74-1-42$	
	=	$37+37$	$37=$	$74-1-36$	

76	=	$3+73$	$3=$	$76-1-72$	$*$
	=	$5+71$	$5=$	$76+1-72$	$*$
	=	$17+59$	$17=$	$76+1-60$	
	=	$23+53$	$23=$	$76+1-54$	
	=	$29+47$	$29=$	$76+1-48$	
78	=	$5+73$	$5=$	$78-1-72$	$*$
	=	$7+71$	$7=$	$78+1-72$	$*$
	=	$11+67$	$11=$	$78-1-66$	
	=	$17+61$	$17=$	$78-1-60$	
	=	$19+59$	$19=$	$78+1-60$	
	=	$31+47$	$31=$	$78+1-48$	
	=	$37+41$	$37=$	$78+1-42$	
80	=	$7+73$	$7=$	$80-1-72$	$*$
	=	$13+67$	$13=$	$80-1-66$	
	=	$19+61$	$19=$	$80-1-60$	
	=	$37+43$	$37=$	$80-1-42$	
$82*$	=	$3+79$	$3=$	$82-1-78$	$*$
	=	$11+71$	$11=$	$82+1-72$	
	=	$23+59$	$23=$	$82+1-60$	
	=	$29+53$	$29=$	$82+1-54$	
	=	$41+41$	$41=$	$82+1-42$	
84	=	$5+79$	$5=$	$84-1-78$	$*$
	=	$11+73$	$11=$	$84-1-72$	
	=	$13+71$	$13=$	$84+1-72$	
	=	$17+67$	$17=$	$84-1-66$	
	=	$23+61$	$23=$	$84-1-60$	
	=	$31+53$	$31=$	$84+1-54$	
	=	$37+47$	$37=$	$84+1-48$	
	=	$41+43$	$41=$	$84-1-42$	
$86*$	=	$3+83$	$3=$	$86+1-84$	$*$
	=	$7+79$	$7=$	$86-1-78$	$*$
	=	$13+73$	$13=$	$86-1-72$	
	=	$19+67$	$19=$	$86-1-66$	
	=	$43+43$	$43=$	$86-1-42$	
88	=	$5+83$	$5=$	$88+1-84$	$*$
	=	$17+71$	$17=$	$88+1-72$	
	=	$29+59$	$29=$	$88+1-60$	
	=	$41+47$	$41=$	$88+1-48$	
90	=	$7+83$	$7=$	$90+1-84$	$*$
	=	$11+79$	$11=$	$90-1-78$	
	=	$17+73$	$17=$	$90-1-72$	
	=	$19+71$	$19=$	$90+1-72$	
	=	$23+67$	$23=$	$90-1-66$	
	=	$29+61$	$29=$	$90-1-60$	
	=	$31+59$	$31=$	$90+1-60$	
	=	$37+53$	$37=$	$90+1-54$	
	=	$43+47$	$43=$	$90+1-48$	
92	=	$3+89$	$3=$	$92+1-90$	$*$
	=	$13+79$	$13=$	$92-1-78$	
	=	$19+73$	$19=$	$92-1-72$	
	=	$31+61$	$31=$	$92-1-60$	
$94*$	=	$5+89$	$5=$	$94+1-90$	$*$
	=	$11+83$	$11=$	$94+1-84$	
	=	$23+71$	$23=$	$94+1-72$	
	=	$41+53$	$41=$	$94+1-54$	
	=	$47+47$	$47=$	$94+1-48$	

96	=	$7+89$	$7=$	$96+1-90$	$*$
	=	$13+83$	$13=$	$96+1-84$	
	=	$17+79$	$17=$	$96-1-78$	
	=	$23+73$	$23=$	$96-1-72$	
	=	$29+67$	$29=$	$96-1-66$	
	=	$37+59$	$37=$	$96+1-60$	
	=	$43+53$	$43=$	$96+1-54$	
98	=	$19+79$	$19=$	$98-1-78$	
	=	$31+67$	$31=$	$98-1-66$	
	=	$37+61$	$37=$	$98-1-60$	
100	=	$3+97$	$3=$	$100-1-96$	$*$
	=	$11+89$	$11=$	$100+1-90$	
	=	$17+83$	$17=$	$100+1-84$	
	=	$29+71$	$29=$	$100+1-72$	
	=	$41+59$	$41=$	$100+1-60$	
	=	$47+53$	$47=$	$100+1-54$	
200	=	$3+197$	$3=$	$200+1-198$	$*$
	=	$7+193$	$7=$	$200-1-192$	$*$
	=	$19+181$	$19=$	$200-1-180$	
	=	$37+163$	$37=$	$200-1-162$	
	=	$43+157$	$43=$	$200-1-156$	
	=	$61+139$	$61=$	$200-1-138$	
	=	$73+127$	$73=$	$200-1-126$	
	=	$97+103$	$97=$	$200-1-102$	
500	=	$13+487$	$13=$	$500-1-486$	$*$
	=	$37+463$	$37=$	$500-1-462$	
	=	$43+457$	$43=$	$500-1-456$	
	=	$61+439$	$61=$	$500-1-438$	
	=	$67+433$	$67=$	$500-1-432$	
	=	$79+421$	$79=$	$500-1-420$	
	=	$103+397$	$103=$	$500-1-396$	
	=	$127+373$	$127=$	$500-1-372$	
	=	$151+349$	$151=$	$500-1-348$	
	=	$163+337$	$163=$	$500-1-336$	
	=	$193+307$	$193=$	$500-1-306$	
	=	$223+277$	$223=$	$500-1-276$	
	=	$229+271$	$229=$	$500-1-270$	

Comme attendu, on voit que les nombres pairs divisibles par 3 (les $6k$) peuvent avoir des décomposants de Goldbach dans les deux progressions issues de $x+1$ ou $x-1$. Les nombres congrus à 1 selon le module 3 (les $6k+4$) n'ont des décomposants que dans la progression arithmétique d'origine $x+1$ tandis que ceux congrus à -1 selon le module 3 (les $6k+2$) n'ont des décomposants que dans la progression arithmétique d'origine $x-1$.

Ci-dessous, deux extraits de fichiers qui fournissent pour les 26 nombres pairs avant 10^7 et les 26 nombres pairs avant 10^8 leur nombre de décomposants de Goldbach, qui corroborent le fait que les $3x$ ont à peu près deux fois plus de décomposants de Goldbach que les $3x+1$ et $3x+2$ autour d'eux[‡].

[‡]Un grand merci à Daniel Diaz qui a écrit toute une série de logiciels dédiés à la conjecture de Goldbach.

x	$NbDG(x)$
9999950	38844
9999952	28964
9999954	60233
9999956	29255
9999958	29252
9999960	77889
9999962	34722
9999964	31851
9999966	61357
9999968	32128
9999970	38917
9999972	58510
9999974	29529
9999976	34915
9999978	63738
9999980	40437
9999982	29849
9999984	58268
9999986	30897
9999988	29153
9999990	116066
9999992	29047
9999994	29790
9999996	58553
9999998	28983
10000000	38807

x	$NbDG(x)$
99999950	315647
99999952	249991
99999954	436893
99999956	262390
99999958	220947
99999960	586429
99999962	218881
99999964	232440
99999966	489663
99999968	218402
99999970	349724
99999972	437909
99999974	224860
99999976	223368
99999978	477314
99999980	291440
99999982	218411
99999984	583321
99999986	226167
99999988	242838
99999990	585327
99999992	218826
99999994	218773
99999996	437175
99999998	274787
100000000	291400

Faisons apparaître dans le tableau ci-dessous les trois progressions arithmétiques de 6 en 6 à partir de 8, 10 ou 12 dont les nombres x partagent systématiquement un décomposant de Goldbach avec $x+6$. Les premières lignes du tableau concernent la première progression arithmétique contenant les nombres de la forme $8+6k$ (ou $6k+2$) et les décomposants partagés par un nombre et son successeur dans cette progression dans les lignes qui suivent. Les lignes 5 et suivantes concernent les nombres de la progression arithmétique $10+6k$ (ou $6k+4$) et les lignes 8 et suivantes concernent ceux de la progression $12+6k$ (ou $6k$).

8	14	20	26	32	38	44	50	56	62	68	74	80	86	92	98
3	3	3	3	3		3	3	3	3		3		3	3	
				7	7	7			31	31	31			19	19
											7	7	7		
10	16	22	28	34	40	46	52	58	64	70	76	82	88	94	100
3	3	3		3	3	3			3	3	3	3			3
		5	5	5		5	5	5	5			41	41	41	41
12	18	24	30	36	42	48	54	60	66	72	78	84	90	96	
5	5	5		5	5	5			5	5	5	5			
		7	7	7		7	7	7	7			17	17	17	

La conjecture : "x supérieur à 6 partage toujours un décomposant de Goldbach avec $x+6$" (i.e. $x = p+q, x+6 = p+q'$ *avec* p, q *et* q' *premiers*) a été vérifiée par ordinateur jusqu'à 16.10^8. Elle s'explique par le fait que l'un des nombres premiers décomposants de Goldbach de x étant non congru à x selon tout module inférieur à $\sqrt{x}$, aura vraiment toutes les chances d'être également non congru à $x+6$ selon tout module inférieur à $\sqrt{x+6}$.

3 Exemple du nombre pair 500 : détail de l'application du double crible

On détaille ici pour le nombre pair 500 ce qu'on pourrait appeler l'application du double crible :
1) la première application du crible consiste à éliminer les nombres congrus à 0 selon un module premier inférieur ou égal à $\sqrt{x}$ (de manière à éliminer les nombres composés et les petits premiers inférieurs ou égaux à $\sqrt{x}$) ;
2) la deuxième application du crible consiste à éliminer les nombres congrus à x selon un module premier inférieur ou égal à $\sqrt{x}$.

500 étant congru à 2 selon le module 3, les seuls nombres à considérer sont ceux appartenant à la progression arithmétique d'origine $500-1$.

On note dans la deuxième colonne le passage de la première passe du crible (élimination des nombres congrus à 0 selon un module inférieur ou égal à $\sqrt{x} = 22, ...$). Les modules à considérer sont 5, 7, 11, 13, 17, 19.

On note dans la troisième colonne le passage de la seconde passe du crible en notant entre parenthèse la congruence partagée avec x.
500 est congru à 0 (*mod* 5), 3 (*mod* 7), 5 (*mod* 11), 6 (*mod* 13), 7 (*mod* 17) *et* 6 (*mod* 19).

Les couleurs permettent de bien visualiser les périodicités.

7	0 (*mod* 7)	7 (*mod* 17)
13	0 (*mod* 13)	
19	0 (*mod* 19)	6 (*mod* 13)
25	0 (*mod* 5)	6 (*mod* 19)
31		3 (*mod* 7)
37		
43		
49	0 (*mod* 7)	5 (*mod* 11)
55	0 (*mod* 5 *et* 11)	
61		
67		
73		3 (*mod* 7)
79		
85	0 (*mod* 5 *et* 17)	
91	0 (*mod* 7 *et* 13)	
97		6 (*mod* 13)
103		
109		7 (*mod* 17)
115	0 (*mod* 5)	3 (*mod* 7) *et* 5 (*mod* 11)
121	0 (*mod* 11)	
127		
133	0 (*mod* 7 *et* 19)	
139		6 (*mod* 19)
145	0 (*mod* 5)	
151		
157		3 (*mod* 7)
163		
169	0 (*mod* 13)	
175	0 (*mod* 5 *et* 7)	6 (*mod* 13)
181		5 (*mod* 11)
187	0 (*mod* 11 *et* 17)	
193		
199		3 (*mod* 7)
205	0 (*mod* 5)	
211		7 (*mod* 17)
217	0 (*mod* 7)	
223		
229		

Les décomposants de Goldbach des nombres pairs sont systématiquement indiqués entre parenthèses après le nombre pair considéré, précédés des lettres DG.

1 Nombres pairs de la forme $n = 6m$ de 144 à 30

L'application double du crible d'Eratosthène est présentée dans des tableaux dans lesquels les $\left\lfloor \frac{n}{12} \right\rfloor$ nombres des parties supérieures des tableaux appartiennent à la progression arithmétique $6k-1$ tandis que les $\left\lfloor \frac{n-6}{12} \right\rfloor$ nombres des parties inférieures appartiennent à la progression arithmétique $6k+1$.

Nous notons dans la seconde colonne le résultat de l'application de la première passe de l'algorithme (élimination des nombres congrus à 0 $(mod\ m_i)$, $m_i < \sqrt{n}$, pour trouver les nombres premiers p, $\sqrt{n} < p \leq n/2$.

Nous notons dans la troisième colonne le résultat de la seconde passe de l'algorithme en spécifiant la congruence à $n\ (mod\ m_i), m_i < \sqrt{n}$, pour trouver les nombres dont le complémentaire à n est premier.

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.

- $n = 144$ $\quad (DG : 5, 7, 13, 17, 31, 37, 41, 43, 47, 61, 71)$
  $n = 2^4.3^2$.
  $n/2 = 72$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		139 (p)	
11 (p)	0 $(mod\ 11)$	4 $(mod\ 7)$	133	
17 (p)			127 (p)	$17 + 127$
23 (p)		1 $(mod\ 11)$	121	
29 (p)		4 $(mod\ 5)$	115	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		109 (p)	
41 (p)			103 (p)	$41 + 103$
47 (p)			97 (p)	$47 + 97$
53 (p)		4 $(mod\ 7)$	91	
59 (p)		4 $(mod\ 5)$	85	
65	0 $(mod\ 5)$		79 (p)	
71 (p)			73 (p)	$71 + 73$
7 (p)	0 $(mod\ 7)$		137 (p)	
13 (p)			131 (p)	$13 + 131$
19 (p)		4 $(mod\ 5)$	125	
25	0 $(mod\ 5)$	4 $(mod\ 7)$	119	
31 (p)			113 (p)	$31 + 113$
37 (p)			107 (p)	$37 + 107$
43 (p)			101 (p)	$43 + 101$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	95	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		89 (p)	
61 (p)			83 (p)	$61 + 83$
67 (p)		4 $(mod\ 7)$ et 1 $(mod\ 11)$	77	

- $n = 138$ $\quad (DG : 7, 11, 29, 31, 37, 41, 59, 67)$

  $n = 2.3.23.$
  $n/2 = 69.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 6\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	133	
11 (p)	0 $(mod\ 11)$		127 (p)	
17 (p)		6 $(mod\ 11)$	121	
23 (p)		3 $(mod\ 5)$	115	
29 (p)			109 (p)	$29 + 109$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		103 (p)	
41 (p)			97 (p)	$41 + 97$
47 (p)		5 $(mod\ 7)$	91	
53 (p)		3 $(mod\ 5)$	85	
59			79 (p)	$59 + 79$
65	0 $(mod\ 5)$		73 (p)	
7 (p)	0 $(mod\ 7)$		131 (p)	
13 (p)		3 $(mod\ 5)$	125	
19 (p)		5 $(mod\ 7)$	119	
25	0 $(mod\ 5)$		113 (p)	
31 (p)			107 (p)	$31 + 107$
37 (p)			101 (p)	$37 + 101$
43 (p)		3 $(mod\ 5)$	95	
49	0 $(mod\ 7)$		89 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		83 (p)	
61 (p)		5 $(mod\ 7)$ et 6 $(mod\ 11)$	77	
67			71 (p)	$67 + 71$

- $n = 132$ $\quad (DG : 5, 19, 23, 29, 31, 43, 53, 59, 61)$

  $n = 2^2.3.11.$
  $n/2 = 66.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7), n \equiv 0\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$		127 (p)	
11 (p)	0 $(mod\ 11)$		121	
17 (p)		2 $(mod\ 5)$	115	
23 (p)			109 (p)	$23 + 109$
29 (p)			103 (p)	$29 + 103$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		97 (p)	
41 (p)		6 $(mod\ 7)$	91	
47 (p)		2 $(mod\ 5)$	85	
53 (p)			79 (p)	$53 + 79$
59 (p)			73 (p)	$59 + 73$
65	0 $(mod\ 5)$		67 (p)	
7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	125	
13 (p)		6 $(mod\ 7)$	119	
19 (p)			113 (p)	$19 + 113$
25	0 $(mod\ 5)$		107 (p)	
31 (p)			101 (p)	$31 + 101$
37 (p)		2 $(mod\ 5)$	95	
43 (p)			89 (p)	$43 + 89$
49	0 $(mod\ 7)$		83 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		77	
61 (p)			71 (p)	$61 + 71$

- $n = 126$ $(DG : 13, 17, 19, 23, 29, 37, 43, 47, 53, 59)$

  $n = 2.3^2.7$.
  $n/2 = 63$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 5\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 11)$	121	
11 (p)	0 $(mod\ 11)$	1 $(mod\ 5)$	115	
17 (p)			109 (p)	$17 + 109$
23 (p)			103 (p)	$23 + 103$
29 (p)			97 (p)	$29 + 97$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		91	
41 (p)		1 $(mod\ 5)$	85	
47 (p)			79 (p)	$47 + 79$
53 (p)			73 (p)	$53 + 73$
59 (p)			67 (p)	$59 + 67$
7 (p)	0 $(mod\ 7)$		119	
13 (p)			113 (p)	$13 + 113$
19 (p)			107 (p)	$19 + 107$
25	0 $(mod\ 5)$		101 (p)	
31 (p)		1 $(mod\ 5)$	95	
37 (p)			89 (p)	$37 + 89$
43 (p)			83 (p)	$43 + 83$
49	0 $(mod\ 7)$	5 $(mod\ 11)$	77	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		71 (p)	
61 (p)		1 $(mod\ 5)$	65	

- $n = 120$ $(DG : 7, 11, 13, 17, 19, 23, 31, 37, 41, 47, 53, 59)$

  $n = 2^3.3.5$.
  $n/2 = 60$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		115	
11 (p)			109 (p)	$11 + 109$
17 (p)			103 (p)	$17 + 103$
23 (p)			97 (p)	$23 + 97$
29 (p)		1 $(mod\ 7)$	91	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		85	
41 (p)			79 (p)	$41 + 79$
47 (p)			73 (p)	$47 + 73$
53 (p)			67 (p)	$53 + 67$
59 (p)			61 (p)	$59 + 61$
7 (p)	0 $(mod\ 7)$		103 (p)	
13 (p)			97 (p)	$13 + 97$
19 (p)			91 (p)	$19 + 91$
25	0 $(mod\ 5)$		85	
31 (p)			79 (p)	$31 + 79$
37 (p)			73 (p)	$37 + 73$
43 (p)		1 $(mod\ 7)$	67 (p)	
49	0 $(mod\ 7)$		61 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		55	

- $n = 114$ $\quad (DG : 5, 7, 11, 13, 17, 31, 41, 43, 47, 53)$

  $n = 2.3.19.$
  $n/2 = 57.$
  $7 < \sqrt{n} < 11.$ Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 2\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		109 (p)	
11 (p)			103 (p)	$11 + 103$
17 (p)			97 (p)	$17 + 97$
23 (p)		2 $(mod\ 7)$	91	
29 (p)		4 $(mod\ 5)$	85	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		79 (p)	
41 (p)			73 (p)	$41 + 73$
47 (p)			67 (p)	$47 + 67$
53 (p)			61 (p)	$53 + 61$
7 (p)	0 $(mod\ 7)$		107 (p)	
13 (p)			101 (p)	$13 + 101$
19 (p)		4 $(mod\ 5)$	95	
25	0 $(mod\ 5)$		89 (p)	
31 (p)			83 (p)	$31 + 83$
37 (p)		2 $(mod\ 7)$	77	
43 (p)			71 (p)	$43 + 71$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	65	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		59 (p)	

- $n = 108$ $\quad (DG : 5, 7, 11, 19, 29, 37, 41, 47)$

  $n = 2^2.3^3.$
  $n/2 = 54.$
  $7 < \sqrt{n} < 11.$ Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 3\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		103 (p)	
11 (p)			97 (p)	$11 + 97$
17 (p)		3 $(mod\ 7)$	91	
23 (p)		3 $(mod\ 5)$	85	
29 (p)			79 (p)	$29 + 79$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		73 (p)	
41 (p)			67 (p)	$41 + 67$
47 (p)			61 (p)	$47 + 61$
53 (p)		3 $(mod\ 5)$	55	
7 (p)	0 $(mod\ 7)$		101 (p)	
13 (p)		3 $(mod\ 5)$	95	
19 (p)			89 (p)	$19 + 89$
25	0 $(mod\ 5)$		83 (p)	
31 (p)		3 $(mod\ 7)$	77	
37 (p)			71 (p)	$37 + 71$
43 (p)		3 $(mod\ 5)$	65	
49	0 $(mod\ 7)$		59 (p)	

- $n = 102$ $\quad (DG : 5, 13, 19, 23, 29, 31, 41, 43)$

  $n = 2.3.17.$
  $n/2 = 51.$
  $7 < \sqrt{n} < 11.$ Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 4\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		97 (p)	
11 (p)		4 $(mod\ 7)$	91	
17 (p)		2 $(mod\ 5)$	85	
23 (p)			79 (p)	$23 + 79$
29 (p)			73 (p)	$29 + 73$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		67 (p)	
41 (p)			61 (p)	$41 + 61$
47 (p)		2 $(mod\ 5)$	55	
7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	95	
13 (p)			89 (p)	$13 + 89$
19 (p)			83 (p)	$19 + 83$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	77	
31 (p)			71 (p)	$31 + 71$
37 (p)		2 $(mod\ 5)$	65	
43 (p)			59 (p)	$43 + 59$
49	0 $(mod\ 7)$		53 (p)	

- $n = 96$ $\quad (DG : 7, 13, 17, 23, 29, 37, 43)$

  $n = 2^5.3.$
  $n/2 = 48.$
  $7 < \sqrt{n} < 11.$ Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 5\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	91	
11 (p)		1 $(mod\ 5)$	85	
17 (p)			79 (p)	$17 + 79$
23 (p)			73 (p)	$23 + 73$
29 (p)			67 (p)	$29 + 67$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		61 (p)	
41 (p)		1 $(mod\ 5)$	55	
47 (p)		5 $(mod\ 7)$	49	
7 (p)	0 $(mod\ 7)$		89 (p)	
13 (p)			83 (p)	$13 + 83$
19 (p)		5 $(mod\ 7)$	77	
25	0 $(mod\ 5)$		71 (p)	
31 (p)		1 $(mod\ 5)$	65	
37 (p)			59 (p)	$37 + 59$
43 (p)			53 (p)	$43 + 53$

- $n = 90$ $(DG : 7, 11, 17, 19, 23, 29, 31, 37, 43)$

  $n = 2.3^2.5$.
  $n/2 = 45$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		85	
11 (p)			79 (p)	$11 + 79$
17 (p)			73 (p)	$17 + 73$
23 (p)			67 (p)	$23 + 67$
29 (p)			61 (p)	$29 + 61$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		55	
41 (p)		6 $(mod\ 7)$	49	
7 (p)	0 $(mod\ 7)$		83 (p)	
13 (p)		6 $(mod\ 7)$	77	
19 (p)			71 (p)	$19 + 71$
25	0 $(mod\ 5)$		65	
31 (p)			59 (p)	$31 + 59$
37 (p)			53 (p)	$37 + 53$
43 (p)			47 (p)	$43 + 47$

- $n = 84$ $(DG : 5, 11, 13, 17, 23, 31, 37, 41)$

  $n = 2^2.3.7$.
  $n/2 = 42$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		79 (p)	
11 (p)			73 (p)	$11 + 73$
17 (p)			67 (p)	$17 + 67$
23 (p)			61 (p)	$23 + 61$
29 (p)		4 $(mod\ 5)$	55	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		49	
41 (p)			43 (p)	$41 + 43$
7 (p)	0 $(mod\ 7)$		77	
13 (p)			71 (p)	$13 + 71$
19 (p)		4 $(mod\ 5)$	65	
25	0 $(mod\ 5)$		59 (p)	
31 (p)			53 (p)	$31 + 53$
37 (p)			47 (p)	$37 + 47$

- $n = 78$ $(DG : 5, 7, 11, 17, 19, 31, 37)$

  $n = 2.3.13$.
  $n/2 = 39$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		73 (p)	
11 (p)			67 (p)	$11 + 67$
17 (p)			61 (p)	$17 + 61$
23 (p)		3 $(mod\ 5)$	55	
29 (p)		1 $(mod\ 7)$	49	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		43 (p)	
7 (p)	0 $(mod\ 7)$		71 (p)	
13 (p)		3 $(mod\ 5)$	65	
19 (p)			59 (p)	$19 + 59$
25	0 $(mod\ 5)$		53 (p)	
31 (p)			47 (p)	$31 + 47$
37 (p)			41 (p)	$37 + 41$

- $n = 72$ $(DG : 5, 11, 13, 19, 29, 31)$

  $n = 2^3.3^2$.
  $n/2 = 36$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		67 (p)	
11 (p)			61 (p)	$11 + 61$
17 (p)		2 $(mod\ 5)$	55	
23 (p)		2 $(mod\ 7)$	49	
29 (p)			43 (p)	$29 + 43$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		37 (p)	
7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	65	
13 (p)			59 (p)	$13 + 59$
19 (p)			53 (p)	$19 + 53$
25	0 $(mod\ 5)$		47 (p)	
31 (p)			41 (p)	$31 + 41$

- $n = 66$ $(DG : 5, 7, 13, 19, 23, 29)$

  $n = 2.3.11$.
  $n/2 = 33$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		61 (p)	
11 (p)		1 $(mod\ 5)$	55	
17 (p)		3 $(mod\ 7)$	49	
23 (p)			43 (p)	$23 + 43$
29 (p)			37 (p)	$29 + 37$
7 (p)	0 $(mod\ 7)$		59 (p)	
13 (p)			53 (p)	$13 + 53$
19 (p)			47 (p)	$19 + 47$
25	0 $(mod\ 5)$		41 (p)	
31 (p)		1 $(mod\ 5)$ et 3 $(mod\ 7)$	35	

- $n = 60$ $(DG : 7, 13, 17, 19, 23, 29)$

  $n = 2^2.3.5$.
  $n/2 = 30$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		55	
11 (p)		4 $(mod\ 7)$	49	
17 (p)			43 (p)	$17 + 43$
23 (p)			37 (p)	$23 + 37$
29 (p)			31 (p)	$29 + 31$
7 (p)	0 $(mod\ 7)$		53 (p)	
13 (p)			47 (p)	$13 + 47$
19 (p)			41 (p)	$19 + 41$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	35	

- $n = 54$ $(DG : 7, 11, 13, 17, 23)$

  $n = 2.3^3$.
  $n/2 = 27$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	49	
11 (p)			43 (p)	$11 + 43$
17 (p)			37 (p)	$17 + 37$
23 (p)			31 (p)	$23 + 31$
7 (p)	0 $(mod\ 7)$		47 (p)	
13 (p)			41 (p)	$13 + 41$
19 (p)		4 $(mod\ 5)$ et 5 $(mod\ 7)$	35	
25	0 $(mod\ 5)$		29	

- $n = 48$ $(DG : 5, 7, 11, 17, 19)$

  $n = 2^4.3$.
  $n/2 = 24$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		43 (p)	
11 (p)			37 (p)	$11 + 37$
17 (p)			31 (p)	$17 + 31$
23 (p)		3 $(mod\ 5)$	25	
7 (p)			41 (p)	$7 + 41$
13 (p)		3 $(mod\ 5)$	35	
19 (p)			29 (p)	$19 + 29$

- $n = 42$ $(DG : 5, 11, 13, 19)$

  $n = 2.3.7$.
  $n/2 = 21$.
  $5 < \sqrt{n} < 5$. Le module à considérer est 5.
  $n \equiv 2\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		37 (p)	
11 (p)			31 (p)	$11 + 31$
17 (p)		2 $(mod\ 5)$	25	
7 (p)		2 $(mod\ 5)$	35	
13 (p)			29 (p)	$13 + 29$
19 (p)			23 (p)	$19 + 23$

- $n = 36$ $(DG : 5, 7, 13, 17)$

  $n = 2^2.3^2$.
  $n/2 = 18$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		31 (p)	
11 (p)		1 $(mod\ 5)$	25	
17 (p)			19 (p)	$17 + 19$
7 (p)			29 (p)	$7 + 29$
13 (p)			23 (p)	$13 + 23$

- $n = 30$ $(DG : 7, 11, 13)$

  $n = 2.3.5$.
  $n/2 = 15$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		25	
11 (p)			19 (p)	$11 + 19$
7 (p)			23 (p)	$7 + 23$
13 (p)			17 (p)	$13 + 17$

2 Nombres pairs de la forme $n = 6m + 4$ de 142 à 28

L'application double du crible d'Eratosthène est présentée dans des tableaux ne contenant que $\left\lfloor \frac{n+6}{12} \right\rfloor$ nombres de la progression arithmétique $6k - 1$.

- $n = 142$ $(DG : 3, 5, 11, 29, 41, 53, 59, 71)$

  $n = 2.71$.
  $n/2 = 71$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 10\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		137 (p)	
11 (p)	0 $(mod\ 11)$		131 (p)	
17 (p)		2 $(mod\ 5)$	125	
23 (p)		2 $(mod\ 7)$	119	
29 (p)			113 (p)	$29 + 113$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		107 (p)	
41 (p)			101 (p)	$41 + 101$
47 (p)		2 $(mod\ 5)$	95	
53 (p)			89 (p)	$53 + 89$
59 (p)			83 (p)	$59 + 83$
65	0 $(mod\ 5)$	2 $(mod\ 7)$ *et* 10 $(mod\ 11)$	77	
71 (p)			71 (p)	$71 + 71$

- $n = 136$ $(DG : 5, 23, 29, 47, 53)$

  $n = 2^3.17$.
  $n/2 = 68$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 4\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		131 (p)	
11 (p)	0 $(mod\ 11)$	1 $(mod\ 5)$	125	
17 (p)		3 $(mod\ 7)$	119	
23 (p)			113 (p)	$23 + 113$
29 (p)			107 (p)	$29 + 107$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		101 (p)	
41 (p)		1 $(mod\ 5)$	95	
47 (p)			89 (p)	$47 + 89$
53 (p)			83 (p)	$53 + 83$
59 (p)		3 $(mod\ 7)$ *et* 4 $(mod\ 11)$	77	
65	0 $(mod\ 5)$		71 (p)	

- $n = 130$ $(DG : 3, 17, 23, 29, 41, 47, 59)$

  $n = 2.5.13$.
  $n/2 = 65$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 9\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		125	
11 (p)	0 $(mod\ 11)$	4 $(mod\ 7)$	119	
17 (p)			113 (p)	$17 + 113$
23 (p)			107 (p)	$23 + 107$
29 (p)			101 (p)	$29 + 101$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		95	
41 (p)			89 (p)	$41 + 89$
47 (p)			83 (p)	$47 + 83$
53 (p)		4 $(mod\ 7)$ *et* 9 $(mod\ 11)$	77	
59 (p)			71 (p)	$59 + 71$
65	0 $(mod\ 5)$		65	

- $n = 124$ $(DG : 11, 17, 23, 41, 53)$

  $n = 2^2.31$.
  $n/2 = 62$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 3\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	119	
11 (p)	0 $(mod\ 11)$		113 (p)	
17 (p)			107 (p)	$17 + 107$
23 (p)			101 (p)	$23 + 101$
29 (p)		4 $(mod\ 5)$	95	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		89 (p)	
41 (p)			83 (p)	$41 + 83$
47 (p)		5 $(mod\ 7)$ *et* 3 $(mod\ 11)$	77	
53 (p)			71 (p)	$53 + 71$
59 (p)		4 $(mod\ 5)$	65	

- $n = 118$ $(DG : 5, 11, 17, 29, 47, 59)$

  $n = 2.59$.
  $n/2 = 59$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		113 (p)	
11 (p)			107 (p)	$11 + 107$
17 (p)			101 (p)	$17 + 101$
23 (p)		3 $(mod\ 5)$	95	
29 (p)			89 (p)	$29 + 89$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		83 (p)	
41 (p)		6 $(mod\ 7)$	77	
47 (p)			71 (p)	$47 + 71$
53 (p)		3 $(mod\ 5)$	65	
59 (p)			59 (p)	$59 + 59$

- $n = 112$ $(DG : 3, 5, 11, 23, 29, 41, 53)$

  $n = 2^4.7$.
  $n/2 = 56$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		107 (p)	
11 (p)			101 (p)	$11 + 101$
17 (p)		2 $(mod\ 5)$	95	
23 (p)			89 (p)	$23 + 89$
29 (p)			83 (p)	$29 + 83$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		77	
41 (p)			71 (p)	$41 + 71$
47 (p)		2 $(mod\ 5)$	65	
53 (p)			59 (p)	$53 + 59$

- $n = 106$ $(DG : 3, 5, 17, 23, 47, 53)$

  $n = 2.53$.
  $n/2 = 53$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		101 (p)	
11 (p)		1 $(mod\ 5)$	95	
17 (p)			89 (p)	$17 + 89$
23 (p)			83 (p)	$23 + 83$
29 (p)		1 $(mod\ 7)$	77	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		71 (p)	
41 (p)		1 $(mod\ 5)$	65	
47 (p)			59 (p)	$47 + 59$
53 (p)			53 (p)	$53 + 53$

- $n = 100$ $(DG : 3, 11, 17, 29, 41, 47)$

  $n = 2^2.5^2$.
  $n/2 = 50$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		95	
11 (p)			89 (p)	$11 + 89$
17 (p)			83 (p)	$17 + 83$
23 (p)		2 $(mod\ 7)$	77	
29 (p)			71 (p)	$29 + 71$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		65	
41 (p)			59 (p)	$41 + 59$
47 (p)			53 (p)	$47 + 53$

- $n = 94$ $(DG : 5, 11, 23, 41, 47)$

  $n = 2.47$.
  $n/2 = 47$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		89 (p)	
11 (p)			83 (p)	$11 + 83$
17 (p)		3 $(mod\ 7)$	77	
23 (p)			71 (p)	$23 + 71$
29 (p)		4 $(mod\ 5)$	65	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		59 (p)	
41 (p)			53 (p)	$41 + 53$
47 (p)			47 (p)	$47 + 47$

- $n = 88$ $(DG : 5, 17, 29, 41)$

  $n = 2^3.11$.
  $n/2 = 44$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		83 (p)	
11 (p)		4 $(mod\ 7)$	77	
17 (p)			71 (p)	$17 + 71$
23 (p)		3 $(mod\ 5)$	65	
29 (p)			59 (p)	$29 + 59$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		53 (p)	
41 (p)			47 (p)	$41 + 47$

- $n = 82$ $(DG : 3, 11, 23, 29, 41)$

  $n = 2.41$.
  $n/2 = 41$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	77	
11 (p)			71 (p)	$11 + 71$
17 (p)		2 $(mod\ 5)$	65	
23 (p)			59 (p)	$23 + 59$
29 (p)			53 (p)	$29 + 53$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		47 (p)	
41 (p)			41 (p)	$41 + 41$

- $n = 76$ $(DG : 3, 5, 17, 23, 29)$

  $n = 2^2.19$.
  $n/2 = 38$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		71 (p)	
11 (p)		1 $(mod\ 5)$	65	
17 (p)			59 (p)	$17 + 59$
23 (p)			53 (p)	$23 + 53$
29 (p)			47 (p)	$29 + 47$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		41 (p)	

- $n = 70$ $(DG : 3, 11, 17, 23, 29)$

  $n = 2.5.7$.
  $n/2 = 35$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		65	
11 (p)			59 (p)	$11 + 59$
17 (p)			53 (p)	$17 + 53$
23 (p)			47 (p)	$23 + 47$
29 (p)			41 (p)	$29 + 41$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		35	

- $n = 64$ $(DG : 3, 5, 11, 17, 23)$

  $n = 2^6$.
  $n/2 = 32$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		59 (p)	
11 (p)			53 (p)	$11 + 53$
17 (p)			47 (p)	$17 + 47$
23 (p)			41 (p)	$23 + 41$
29 (p)		4 $(mod\ 5)$ *et* 1 $(mod\ 7)$	35	

- $n = 58$ $(DG : 5, 11, 17, 29)$

  $n = 2.29$.
  $n/2 = 29$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		53 (p)	
11 (p)			47 (p)	$11 + 47$
17 (p)			41 (p)	$17 + 41$
23 (p)		3 $(mod\ 5)$ *et* 2 $(mod\ 7)$	35	
29 (p)			29 (p)	$29 + 29$

- $n = 52$ $(DG : 5, 11, 23)$

  $n = 2^2.13$.
  $n/2 = 26$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		47 (p)	
11 (p)			41 (p)	$11 + 41$
17 (p)		2 $(mod\ 5)$ *et* 3 $(mod\ 7)$	35	
23 (p)			29 (p)	$23 + 29$

- $n = 46$ $(DG : 3, 5, 17, 23)$

  $n = 2.23$.
  $n/2 = 23$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		41 (p)	
11 (p)		1 $(mod\ 5)$	35	
17 (p)			29 (p)	$17 + 29$
23 (p)			23 (p)	$23 + 23$

- $n = 40$ $(DG : 3, 11, 17)$

  $n = 2^3.5$.
  $n/2 = 20$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	35	
11 (p)		29 (p)	$11 + 29$
17 (p)		23 (p)	$17 + 23$

- $n = 34$ $(DG : 3, 5, 11, 17)$

  $n = 2.17$.
  $n/2 = 17$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 4\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	29 (p)	
11 (p)		23 (p)	$11 + 23$
17 (p)		17 (p)	$17 + 17$

- $n = 28$ $(DG : 5, 11)$

  $n = 2^2.7$.
  $n/2 = 14$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	23	
11 (p)		17 (p)	$11 + 17$

3 Nombres pairs de la forme $n = 6m + 2$ de 140 à 26

L'application double du crible d'Eratosthène est présentée dans des tableaux ne contenant que $\left\lfloor \frac{n}{12} \right\rfloor$ nombres de la progression arithmétique $6k + 1$.

- $n = 140$ $(DG : 3, 13, 31, 37, 43, 61, 67)$

  $n = 2^2.5.7$.
  $n/2 = 70$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 8\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$		133	
13 (p)			127 (p)	$13 + 127$
19 (p)		8 $(mod\ 11)$	121	
25	0 $(mod\ 5)$		115	
31 (p)			109 (p)	$31 + 109$
37 (p)			103 (p)	$37 + 103$
43 (p)			97 (p)	$43 + 97$
49	0 $(mod\ 7)$		91	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		85	
61 (p)			79 (p)	$61 + 79$
67 (p)			73 (p)	$67 + 73$

- $n = 134$ $(DG : 3, 7, 31, 37, 61, 67)$

  $n = 2.67$.
  $n/2 = 67$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7), n \equiv 2\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$		127 (p)	
13 (p)		2 $(mod\ 11)$	121	
19 (p)		4 $(mod\ 5)$	115	
25	0 $(mod\ 5)$		109 (p)	
31 (p)			103 (p)	$31 + 103$
37 (p)			97 (p)	$37 + 97$
43 (p)		1 $(mod\ 7)$	91	
49	0 $(mod\ 7)$	4 $(mod\ 5)$	85	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		79 (p)	
61 (p)			73 (p)	$61 + 73$
67 (p)			67 (p)	$67 + 67$

- $n = 128$ $(DG : 19, 31, 61)$

  $n = 2^7$.
  $n/2 = 64$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 7\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$	7 $(mod\ 11)$	121	
13 (p)		3 $(mod\ 5)$	115	
19 (p)			109 (p)	$19 + 109$
25	0 $(mod\ 5)$		103 (p)	
31 (p)			97 (p)	$31 + 97$
37 (p)		2 $(mod\ 7)$	93	
43 (p)		3 $(mod\ 5)$	87	
49	0 $(mod\ 7)$		81	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		75	
61			69 (p)	$61 + 69$

- $n = 122$ $(DG : 13, 19, 43, 61)$

  $n = 2.61$.
  $n/2 = 61$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	115	
13 (p)			109 (p)	$13 + 109$
19 (p)			103 (p)	$19 + 103$
25	0 $(mod\ 5)$		97 (p)	
31 (p)		3 $(mod\ 7)$	91	
37 (p)		2 $(mod\ 5)$	85	
43 (p)			79 (p)	$43 + 79$
49	0 $(mod\ 7)$		73 (p)	
55	0 $(mod\ 5)$		67 (p)	
61 (p)			61 (p)	$61 + 61$

- $n = 116$ $(DG : 3, 7, 13, 19, 37, 43)$

  $n = 2^2.29$.
  $n/2 = 58$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		109 (p)	
13 (p)			103 (p)	$13 + 103$
19 (p)			97 (p)	$19 + 97$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	91	
31 (p)		1 $(mod\ 5)$	85	
37 (p)			79 (p)	$37 + 79$
43 (p)			73 (p)	$43 + 73$
49	0 $(mod\ 7)$		67	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		61 (p)	

- $n = 110$ $(DG : 3, 7, 13, 31, 37, 43)$

  $n = 2.5.11$.
  $n/2 = 55$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		103 (p)	
13 (p)			97 (p)	$13 + 97$
19 (p)		5 $(mod\ 7)$	91	
25	0 $(mod\ 5)$		85	
31 (p)			79 (p)	$31 + 79$
37 (p)			73 (p)	$37 + 73$
43 (p)			67 (p)	$43 + 67$
49	0 $(mod\ 7)$		61 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		55	

- $n = 104$ $(DG : 3, 7, 31, 37, 43)$

  $n = 2^3.13$.
  $n/2 = 52$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		97 (p)	
13 (p)		6 $(mod\ 7)$	91	
19 (p)		4 $(mod\ 5)$	85	
25	0 $(mod\ 5)$		79 (p)	
31 (p)			73 (p)	$31 + 73$
37 (p)			67 (p)	$37 + 67$
43 (p)			61 (p)	$43 + 61$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	55	

- $n = 98$ $(DG : 19, 31, 37)$

  $n = 2.7^2$.
  $n/2 = 49$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		91	
13 (p)		3 $(mod\ 5)$	85	
19 (p)			79 (p)	$19 + 79$
25	0 $(mod\ 5)$		73	
31 (p)			67 (p)	$31 + 67$
37 (p)			61 (p)	$37 + 61$
43 (p)		3 $(mod\ 5)$	55	
49	0 $(mod\ 7)$		49	

- $n = 92$ $(DG : 3, 13, 19, 31)$

  $n = 2^2.23$.
  $n/2 = 46$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	87	
13 (p)			81 (p)	$13 + 81$
19 (p)			75 (p)	$19 + 75$
25	0 $(mod\ 5)$		69	
31 (p)			63 (p)	$31 + 63$
37 (p)		2 $(mod\ 5)$	57 (p)	
43 (p)		1 $(mod\ 7)$	51	

- $n = 86$ $(DG : 3, 7, 13, 19, 43)$

  $n = 2.43$.
  $n/2 = 43$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		79 (p)	
13 (p)			73 (p)	$13 + 73$
19 (p)			67 (p)	$19 + 67$
25	0 $(mod\ 5)$		61 (p)	
31 (p)		1 $(mod\ 5)$	55	
37 (p)		2 $(mod\ 7)$	49	
43 (p)			43 (p)	$43 + 43$

- $n = 80 \qquad (DG : 7, 13, 19, 37)$

  $n = 2^4.5$.
  $n/2 = 40$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		73 (p)	
13 (p)			67 (p)	$13 + 67$
19 (p)			61 (p)	$19 + 61$
25	0 $(mod\ 5)$		55	
31 (p)		3 $(mod\ 7)$	49	
37 (p)			43 (p)	$37 + 43$

- $n = 74 \qquad (DG : 3, 7, 13, 31, 37)$

  $n = 2.37$.
  $n/2 = 37$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		67 (p)	
13 (p)			61 (p)	$13 + 61$
19 (p)		4 $(mod\ 5)$	55	
25	0 $(mod\ 5)$	4 $(mod\ 7)$	49	
31 (p)			43 (p)	$31 + 43$
37 (p)			37 (p)	$37 + 37$

- $n = 68 \qquad (DG : 7, 31)$

  $n = 2^2.17$.
  $n/2 = 34$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		61 (p)	
13 (p)		3 $(mod\ 5)$	55	
19 (p)		5 $(mod\ 7)$	49	
25	0 $(mod\ 5)$		43 (p)	
31 (p)			37 (p)	$31 + 37$

- $n = 62 \qquad (DG : 3, 19, 31)$

  $n = 2.31$.
  $n/2 = 31$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	55	
13 (p)		6 $(mod\ 7)$	49	
19 (p)			43 (p)	$19 + 43$
25	0 $(mod\ 5)$		37 (p)	
31 (p)			31 (p)	$31 + 31$

- $n = 56$ $(DG : 3, 13, 19)$

  $n = 2^3.7$.
  $n/2 = 28$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		49	
13 (p)			43 (p)	$13 + 43$
19 (p)			37 (p)	$19 + 37$
25	0 $(mod\ 5)$		31	

- $n = 50$ $(DG : 3, 7, 13, 19)$

  $n = 2.5^2$.
  $n/2 = 25$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		43 (p)	
13 (p)			37 (p)	$13 + 37$
19 (p)			31 (p)	$19 + 31$
25	0 $(mod\ 5)$		25	

- $n = 44$ $(DG : 3, 7, 13)$

  $n = 2^2.11$.
  $n/2 = 22$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 4\ (mod\ 5)$.

7 (p)			37 (p)	
13 (p)			31 (p)	$13 + 31$
19 (p)		4 $(mod\ 5)$	25	

- $n = 38$ $(DG : 7, 19)$

  $n = 2.19$.
  $n/2 = 19$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

7 (p)			31 (p)	
13 (p)		3 $(mod\ 5)$	25	
19			19 (p)	$19 + 19$

- $n = 32$ $(DG : 3, 13)$

  $n = 2^5$.
  $n/2 = 16$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 2\ (mod\ 5)$.

7 (p)		2 $(mod\ 5)$	25	
13			19 (p)	$13 + 19$

- $n = 26$ $(DG : 3, 7, 13)$

  $n = 2.13$.
  $n/2 = 13$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

7 (p)			19 (p)	
13			13 (p)	$13 + 13$

Even numbers'Goldbach components are systematically indicated within parentheses after the even number considered, preceded by the letters GC.

1 Even numbers of the form $n = 6m$ from 144 to 30

The double sieve of Eratosthenes application is presented in a table in which $\left\lfloor \frac{n}{12} \right\rfloor$ numbers of the top part belong to the arithmetic progression $6k-1$ while $\left\lfloor \frac{n-6}{12} \right\rfloor$ numbers of the bottom part belong to the arithmetic progression $6k+1$.

We note in the second column the result of the first pass of the sieve (elimination of numbers that are congruent to 0 according to a modulus smaller than or equal to $\sqrt{n}$, to find prime numbers between $\sqrt{n}$ and $n/2$).

We note in the third column result of the second pass of the sieve by specifying the shared congruence with n (to find numbers whose complementary to n is prime).

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.

- $n = 144$ $\quad (GC : 5, 7, 13, 17, 31, 37, 41, 43, 47, 61, 71)$

  $n = 2^4.3^2$.
  $n/2 = 72$.
  $11 < \sqrt{n} < 13$. The moduli to be considered are $5,\ 7\ and\ 11$.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		139 (p)	
11 (p)	0 $(mod\ 11)$	4 $(mod\ 7)$	133	
17 (p)			127 (p)	$17 + 127$
23 (p)		1 $(mod\ 11)$	121	
29 (p)		4 $(mod\ 5)$	115	
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		109 (p)	
41 (p)			103 (p)	$41 + 103$
47 (p)			97 (p)	$47 + 97$
53 (p)		4 $(mod\ 7)$	91	
59 (p)		4 $(mod\ 5)$	85	
65	0 $(mod\ 5)$		79 (p)	
71 (p)			73 (p)	$71 + 73$

7 (p)	0 $(mod\ 7)$		137 (p)	
13 (p)			131 (p)	$13 + 131$
19 (p)		4 $(mod\ 5)$	125	
25	0 $(mod\ 5)$	4 $(mod\ 7)$	119	
31 (p)			113 (p)	$31 + 113$
37 (p)			107 (p)	$37 + 107$
43 (p)			101 (p)	$43 + 101$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	95	
55	0 $(mod\ 5)$ and 0 $(mod\ 11)$		89 (p)	
61 (p)			83 (p)	$61 + 83$
67 (p)		4 $(mod\ 7)$ and 1 $(mod\ 11)$	77	

- $n = 138$ $(GC : 7, 11, 29, 31, 37, 41, 59, 67)$

  $n = 2.3.23.$
  $n/2 = 69.$
  $11 < \sqrt{n} < 13.$ The moduli to be considered are $5,\ 7$ *and* $11.$
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 6\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	133	
11 (p)	0 $(mod\ 11)$		127 (p)	
17 (p)		6 $(mod\ 11)$	121	
23 (p)		3 $(mod\ 5)$	115	
29 (p)			109 (p)	$29 + 109$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		103 (p)	
41 (p)			97 (p)	$41 + 97$
47 (p)		5 $(mod\ 7)$	91	
53 (p)		3 $(mod\ 5)$	85	
59			79 (p)	$59 + 79$
65	0 $(mod\ 5)$		73 (p)	
7 (p)	0 $(mod\ 7)$		131 (p)	
13 (p)		3 $(mod\ 5)$	125	
19 (p)		5 $(mod\ 7)$	119	
25	0 $(mod\ 5)$		113 (p)	
31 (p)			107 (p)	$31 + 107$
37 (p)			101 (p)	$37 + 101$
43 (p)		3 $(mod\ 5)$	95	
49	0 $(mod\ 7)$		89 (p)	
55	0 $(mod\ 5)$ and 0 $(mod\ 11)$		83 (p)	
61 (p)		5 $(mod\ 7)$ and 6 $(mod\ 11)$	77	
67			71 (p)	$67 + 71$

- $n = 132$ $(GC : 5, 19, 23, 29, 31, 43, 53, 59, 61)$

  $n = 2^2.3.11.$
  $n/2 = 66.$
  $11 < \sqrt{n} < 13.$ The moduli to be considered are $5,\ 7$ *and* $11.$
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7), n \equiv 0\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$		127 (p)	
11 (p)	0 $(mod\ 11)$		121	
17 (p)		2 $(mod\ 5)$	115	
23 (p)			109 (p)	$23 + 109$
29 (p)			103 (p)	$29 + 103$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		97 (p)	
41 (p)		6 $(mod\ 7)$	91	
47 (p)		2 $(mod\ 5)$	85	
53 (p)			79 (p)	$53 + 79$
59 (p)			73 (p)	$59 + 73$
65	0 $(mod\ 5)$		67 (p)	
7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	125	
13 (p)		6 $(mod\ 7)$	119	
19 (p)			113 (p)	$19 + 113$
25	0 $(mod\ 5)$		107 (p)	
31 (p)			101 (p)	$31 + 101$
37 (p)		2 $(mod\ 5)$	95	
43 (p)			89 (p)	$43 + 89$
49	0 $(mod\ 7)$		83 (p)	
55	0 $(mod\ 5)$ and 0 $(mod\ 11)$		77	
61 (p)			71 (p)	$61 + 71$

- $n = 126$ $(DG : 13, 17, 19, 23, 29, 37, 43, 47, 53, 59)$

  $n = 2.3^2.7$.
  $n/2 = 63$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 and 11.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 5\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 11)$	121	
11 (p)	0 $(mod\ 11)$	1 $(mod\ 5)$	115	
17 (p)			109 (p)	$17 + 109$
23 (p)			103 (p)	$23 + 103$
29 (p)			97 (p)	$29 + 97$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		91	
41 (p)		1 $(mod\ 5)$	85	
47 (p)			79 (p)	$47 + 79$
53 (p)			73 (p)	$53 + 73$
59 (p)			67 (p)	$59 + 67$
7 (p)	0 $(mod\ 7)$		119	
13 (p)			113 (p)	$13 + 113$
19 (p)			107 (p)	$19 + 107$
25	0 $(mod\ 5)$		101 (p)	
31 (p)		1 $(mod\ 5)$	95	
37 (p)			89 (p)	$37 + 89$
43 (p)			83 (p)	$43 + 83$
49	0 $(mod\ 7)$	5 $(mod\ 11)$	77	
55	0 $(mod\ 5)$ and 0 $(mod\ 11)$		71 (p)	
61 (p)		1 $(mod\ 5)$	65	

- $n = 120$ $(GC : 7, 11, 13, 17, 19, 23, 31, 37, 41, 47, 53, 59)$

  $n = 2^3.3.5$.
  $n/2 = 60$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		115	
11 (p)			109 (p)	$11 + 109$
17 (p)			103 (p)	$17 + 103$
23 (p)			97 (p)	$23 + 97$
29 (p)		1 $(mod\ 7)$	91	
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		85	
41 (p)			79 (p)	$41 + 79$
47 (p)			73 (p)	$47 + 73$
53 (p)			67 (p)	$53 + 67$
59 (p)			61 (p)	$59 + 61$
7 (p)	0 $(mod\ 7)$		103 (p)	
13 (p)			97 (p)	$13 + 97$
19 (p)			91 (p)	$19 + 91$
25	0 $(mod\ 5)$		85	
31 (p)			79 (p)	$31 + 79$
37 (p)			73 (p)	$37 + 73$
43 (p)		1 $(mod\ 7)$	67 (p)	
49	0 $(mod\ 7)$		61 (p)	
55	0 $(mod\ 5)$ and 0 $(mod\ 11)$		55	

- $n = 114$ $(GC : 5, 7, 11, 13, 17, 31, 41, 43, 47, 53)$

  $n = 2.3.19.$
  $n/2 = 57.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 4\ (mod\ 5), n \equiv 2\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		109 (p)	
11 (p)			103 (p)	$11 + 103$
17 (p)			97 (p)	$17 + 97$
23 (p)		2 $(mod\ 7)$	91	
29 (p)		4 $(mod\ 5)$	85	
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		79 (p)	
41 (p)			73 (p)	$41 + 73$
47 (p)			67 (p)	$47 + 67$
53 (p)			61 (p)	$53 + 61$
7 (p)	0 $(mod\ 7)$		107 (p)	
13 (p)			101 (p)	$13 + 101$
19 (p)		4 $(mod\ 5)$	95	
25	0 $(mod\ 5)$		89 (p)	
31 (p)			83 (p)	$31 + 83$
37 (p)		2 $(mod\ 7)$	77	
43 (p)			71 (p)	$43 + 71$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	65	
55	0 $(mod\ 5)$ and 0 $(mod\ 11)$		59 (p)	

- $n = 108$ $(GC : 5, 7, 11, 19, 29, 37, 41, 47)$

  $n = 2^2.3^3.$
  $n/2 = 54.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 3\ (mod\ 5), n \equiv 3\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		103 (p)	
11 (p)			97 (p)	$11 + 97$
17 (p)		3 $(mod\ 7)$	91	
23 (p)		3 $(mod\ 5)$	85	
29 (p)			79 (p)	$29 + 79$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		73 (p)	
41 (p)			67 (p)	$41 + 67$
47 (p)			61 (p)	$47 + 61$
53 (p)		3 $(mod\ 5)$	55	
7 (p)	0 $(mod\ 7)$		101 (p)	
13 (p)		3 $(mod\ 5)$	95	
19 (p)			89 (p)	$19 + 89$
25	0 $(mod\ 5)$		83 (p)	
31 (p)		3 $(mod\ 7)$	77	
37 (p)			71 (p)	$37 + 71$
43 (p)		3 $(mod\ 5)$	65	
49	0 $(mod\ 7)$		59 (p)	

- $n = 102$ $(GC : 5, 13, 19, 23, 29, 31, 41, 43)$

  $n = 2.3.17.$
  $n/2 = 51.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 2\ (mod\ 5), n \equiv 4\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		97 (p)	
11 (p)		4 $(mod\ 7)$	91	
17 (p)		2 $(mod\ 5)$	85	
23 (p)			79 (p)	$23 + 79$
29 (p)			73 (p)	$29 + 73$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		67 (p)	
41 (p)			61 (p)	$41 + 61$
47 (p)		2 $(mod\ 5)$	55	
7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	95	
13 (p)			89 (p)	$13 + 89$
19 (p)			83 (p)	$19 + 83$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	77	
31 (p)			71 (p)	$31 + 71$
37 (p)		2 $(mod\ 5)$	65	
43 (p)			59 (p)	$43 + 59$
49	0 $(mod\ 7)$		53 (p)	

- $n = 96$ $(GC : 7, 13, 17, 23, 29, 37, 43)$

  $n = 2^5.3.$
  $n/2 = 48.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 1\ (mod\ 5), n \equiv 5\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	91	
11 (p)		1 $(mod\ 5)$	85	
17 (p)			79 (p)	$17 + 79$
23 (p)			73 (p)	$23 + 73$
29 (p)			67 (p)	$29 + 67$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		61 (p)	
41 (p)		1 $(mod\ 5)$	55	
47 (p)		5 $(mod\ 7)$	49	
7 (p)	0 $(mod\ 7)$		89 (p)	
13 (p)			83 (p)	$13 + 83$
19 (p)		5 $(mod\ 7)$	77	
25	0 $(mod\ 5)$		71 (p)	
31 (p)		1 $(mod\ 5)$	65	
37 (p)			59 (p)	$37 + 59$
43 (p)			53 (p)	$43 + 53$

- $n = 90$ $(GC : 7, 11, 17, 19, 23, 29, 31, 37, 43)$

  $n = 2.3^2.5.$
  $n/2 = 45.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 0\ (mod\ 5), n \equiv 6\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		85	
11 (p)			79 (p)	$11 + 79$
17 (p)			73 (p)	$17 + 73$
23 (p)			67 (p)	$23 + 67$
29 (p)			61 (p)	$29 + 61$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		55	
41 (p)		6 $(mod\ 7)$	49	
7 (p)	0 $(mod\ 7)$		83 (p)	
13 (p)		6 $(mod\ 7)$	77	
19 (p)			71 (p)	$19 + 71$
25	0 $(mod\ 5)$		65	
31 (p)			59 (p)	$31 + 59$
37 (p)			53 (p)	$37 + 53$
43 (p)			47 (p)	$43 + 47$

- $n = 84$ $(GC : 5, 11, 13, 17, 23, 31, 37, 41)$

  $n = 2^2.3.7.$
  $n/2 = 42.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 4\ (mod\ 5), n \equiv 0\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		79 (p)	
11 (p)			73 (p)	$11 + 73$
17 (p)			67 (p)	$17 + 67$
23 (p)			61 (p)	$23 + 61$
29 (p)		4 $(mod\ 5)$	55	
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		49	
41 (p)			43 (p)	$41 + 43$
7 (p)	0 $(mod\ 7)$		77	
13 (p)			71 (p)	$13 + 71$
19 (p)		4 $(mod\ 5)$	65	
25	0 $(mod\ 5)$		59 (p)	
31 (p)			53 (p)	$31 + 53$
37 (p)			47 (p)	$37 + 47$

- $n = 78$ $(GC : 5, 7, 11, 17, 19, 31, 37)$

  $n = 2.3.13$.
  $n/2 = 39$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 3\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		73 (p)	
11 (p)			67 (p)	$11 + 67$
17 (p)			61 (p)	$17 + 61$
23 (p)		3 $(mod\ 5)$	55	
29 (p)		1 $(mod\ 7)$	49	
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		43 (p)	
7 (p)	0 $(mod\ 7)$		71 (p)	
13 (p)		3 $(mod\ 5)$	65	
19 (p)			59 (p)	$19 + 59$
25	0 $(mod\ 5)$		53 (p)	
31 (p)			47 (p)	$31 + 47$
37 (p)			41 (p)	$37 + 41$

- $n = 72$ $(GC : 5, 11, 13, 19, 29, 31)$

  $n = 2^3.3^2$.
  $n/2 = 36$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		67 (p)	
11 (p)			61 (p)	$11 + 61$
17 (p)		2 $(mod\ 5)$	55	
23 (p)		2 $(mod\ 7)$	49	
29 (p)			43 (p)	$29 + 43$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		37 (p)	
7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	65	
13 (p)			59 (p)	$13 + 59$
19 (p)			53 (p)	$19 + 53$
25	0 $(mod\ 5)$		47 (p)	
31 (p)			41 (p)	$31 + 41$

- $n = 66$ $(GC : 5, 7, 13, 19, 23, 29)$

  $n = 2.3.11$.
  $n/2 = 33$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		61 (p)	
11 (p)		1 $(mod\ 5)$	55	
17 (p)		3 $(mod\ 7)$	49	
23 (p)			43 (p)	$23 + 43$
29 (p)			37 (p)	$29 + 37$
7 (p)	0 $(mod\ 7)$		59 (p)	
13 (p)			53 (p)	$13 + 53$
19 (p)			47 (p)	$19 + 47$
25	0 $(mod\ 5)$		41 (p)	
31 (p)		1 $(mod\ 5)$ and 3 $(mod\ 7)$	35	

- $n = 60$ $(GC : 7, 13, 17, 19, 23, 29)$

  $n = 2^2.3.5.$
  $n/2 = 30.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$		55	
11 (p)		4 $(mod\ 7)$	49	
17 (p)			43 (p)	$17 + 43$
23 (p)			37 (p)	$23 + 37$
29 (p)			31 (p)	$29 + 31$
7 (p)	0 $(mod\ 7)$		53 (p)	
13 (p)			47 (p)	$13 + 47$
19 (p)			41 (p)	$19 + 41$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	35	

- $n = 54$ $(DG : 7, 11, 13, 17, 23)$

  $n = 2.3^3.$
  $n/2 = 27.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 and 7.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7).$

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	49	
11 (p)			43 (p)	$11 + 43$
17 (p)			37 (p)	$17 + 37$
23 (p)			31 (p)	$23 + 31$
7 (p)	0 $(mod\ 7)$		47 (p)	
13 (p)			41 (p)	$13 + 41$
19 (p)		4 $(mod\ 5)$ and 5 $(mod\ 7)$	35	
25	0 $(mod\ 5)$		29	

- $n = 48$ $(GC : 5, 7, 11, 17, 19)$

  $n = 2^4.3.$
  $n/2 = 24.$
  $5 < \sqrt{n} < 7.$ The modulus to be considered is 5.
  $n \equiv 3\ (mod\ 5).$

5 (p)	0 $(mod\ 5)$		43 (p)	
11 (p)			37 (p)	$11 + 37$
17 (p)			31 (p)	$17 + 31$
23 (p)		3 $(mod\ 5)$	25	
7 (p)			41 (p)	$7 + 41$
13 (p)		3 $(mod\ 5)$	35	
19 (p)			29 (p)	$19 + 29$

- $n = 42$ $(GC : 5, 11, 13, 19)$

  $n = 2.3.7.$
  $n/2 = 21.$
  $5 < \sqrt{n} < 5.$ The modulus to be considered is 5.
  $n \equiv 2\ (mod\ 5).$

5 (p)	0 $(mod\ 5)$		37 (p)	
11 (p)			31 (p)	$11 + 31$
17 (p)		2 $(mod\ 5)$	25	
7 (p)		2 $(mod\ 5)$	35	
13 (p)			29 (p)	$13 + 29$
19 (p)			23 (p)	$19 + 23$

- $n = 36 \qquad (GC : 5, 7, 13, 17)$

  $n = 2^2.3^2$.
  $n/2 = 18$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		31 (p)	
11 (p)		1 $(mod\ 5)$	25	
17 (p)			19 (p)	$17 + 19$
7 (p)			29 (p)	$7 + 29$
13 (p)			23 (p)	$13 + 23$

- $n = 30 \qquad (GC : 7, 11, 13)$

  $n = 2.3.5$.
  $n/2 = 15$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		25	
11 (p)			19 (p)	$11 + 19$
7 (p)			23 (p)	$7 + 23$
13 (p)			17 (p)	$13 + 17$

2 Even numbers of the form $n = 6m + 4$ from 142 to 28

The double sieve of Eratosthenes application is presented in a table containing only $\left\lfloor \frac{n+6}{12} \right\rfloor$ numbers belonging to the arithmetic progression $6k - 1$.

- $n = 142 \qquad (GC : 3, 5, 11, 29, 41, 53, 59, 71)$

  $n = 2.71$.
  $n/2 = 71$.
  $11 < \sqrt{n} < 13$. The moduli to be considered are 5, 7 *and* 11.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 10\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		137 (p)	
11 (p)	0 $(mod\ 11)$		131 (p)	
17 (p)		2 $(mod\ 5)$	125	
23 (p)		2 $(mod\ 7)$	119	
29 (p)			113 (p)	$29 + 113$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		107 (p)	
41 (p)			101 (p)	$41 + 101$
47 (p)		2 $(mod\ 5)$	95	
53 (p)			89 (p)	$53 + 89$
59 (p)			83 (p)	$59 + 83$
65	0 $(mod\ 5)$	2 $(mod\ 7)$ *et* 10 $(mod\ 11)$	77	
71 (p)			71 (p)	$71 + 71$

- $n = 136$ $(GC : 5, 23, 29, 47, 53)$

  $n = 2^3.17$.
  $n/2 = 68$.
  $11 < \sqrt{n} < 13$. The moduli to be considered are 5, 7 *and* 11.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 4\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		131 (p)	
11 (p)	0 $(mod\ 11)$	1 $(mod\ 5)$	125	
17 (p)		3 $(mod\ 7)$	119	
23 (p)			113 (p)	$23 + 113$
29 (p)			107 (p)	$29 + 107$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		101 (p)	
41 (p)		1 $(mod\ 5)$	95	
47 (p)			89 (p)	$47 + 89$
53 (p)			83 (p)	$53 + 83$
59 (p)		3 $(mod\ 7)$ *et* 4 $(mod\ 11)$	77	
65	0 $(mod\ 5)$		71 (p)	

- $n = 130$ $(GC : 3, 17, 23, 29, 41, 47, 59)$

  $n = 2.5.13$.
  $n/2 = 65$.
  $11 < \sqrt{n} < 13$. The moduli to be considered are 5, 7 *and* 11.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 9\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		125	
11 (p)	0 $(mod\ 11)$	4 $(mod\ 7)$	119	
17 (p)			113 (p)	$17 + 113$
23 (p)			107 (p)	$23 + 107$
29 (p)			101 (p)	$29 + 101$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		95	
41 (p)			89 (p)	$41 + 89$
47 (p)			83 (p)	$47 + 83$
53 (p)		4 $(mod\ 7)$ *et* 9 $(mod\ 11)$	77	
59 (p)			71 (p)	$59 + 71$
65	0 $(mod\ 5)$		65	

- $n = 124$ $(GC : 11, 17, 23, 41, 53)$

  $n = 2^2.31$.
  $n/2 = 62$.
  $11 < \sqrt{n} < 13$. The moduli to be considered are 5, 7 *and* 11.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 3\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	119	
11 (p)	0 $(mod\ 11)$		113 (p)	
17 (p)			107 (p)	$17 + 107$
23 (p)			101 (p)	$23 + 101$
29 (p)		4 $(mod\ 5)$	95	
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		89 (p)	
41 (p)			83 (p)	$41 + 83$
47 (p)		5 $(mod\ 7)$ *et* 3 $(mod\ 11)$	77	
53 (p)			71 (p)	$53 + 71$
59 (p)		4 $(mod\ 5)$	65	

- $n = 118$ $(GC : 5, 11, 17, 29, 47, 59)$

  $n = 2.59$.
  $n/2 = 59$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 3\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		113 (p)	
11 (p)			107 (p)	$11 + 107$
17 (p)			101 (p)	$17 + 101$
23 (p)		3 $(mod\ 5)$	95	
29 (p)			89 (p)	$29 + 89$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		83 (p)	
41 (p)		6 $(mod\ 7)$	77	
47 (p)			71 (p)	$47 + 71$
53 (p)		3 $(mod\ 5)$	65	
59 (p)			59 (p)	$59 + 59$

- $n = 112$ $(DG : 3, 5, 11, 23, 29, 41, 53)$

  $n = 2^4.7$.
  $n/2 = 56$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 and 7.
  $n \equiv 2\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		107 (p)	
11 (p)			101 (p)	$11 + 101$
17 (p)		2 $(mod\ 5)$	95	
23 (p)			89 (p)	$23 + 89$
29 (p)			83 (p)	$29 + 83$
35	0 $(mod\ 5)$ and 0 $(mod\ 7)$		77	
41 (p)			71 (p)	$41 + 71$
47 (p)		2 $(mod\ 5)$	65	
53 (p)			59 (p)	$53 + 59$

- $n = 106$ $(GC : 3, 5, 17, 23, 47, 53)$

  $n = 2.53$.
  $n/2 = 53$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 1\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		101 (p)	
11 (p)		1 $(mod\ 5)$	95	
17 (p)			89 (p)	$17 + 89$
23 (p)			83 (p)	$23 + 83$
29 (p)		1 $(mod\ 7)$	77	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		71 (p)	
41 (p)		1 $(mod\ 5)$	65	
47 (p)			59 (p)	$47 + 59$
53 (p)			53 (p)	$53 + 53$

- $n = 100$ $(GC : 3, 11, 17, 29, 41, 47)$

  $n = 2^2.5^2$.
  $n/2 = 50$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 0\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		95	
11 (p)			89 (p)	$11 + 89$
17 (p)			83 (p)	$17 + 83$
23 (p)		2 $(mod\ 7)$	77	
29 (p)			71 (p)	$29 + 71$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		65	
41 (p)			59 (p)	$41 + 59$
47 (p)			53 (p)	$47 + 53$

- $n = 94$ $(GC : 5, 11, 23, 41, 47)$

  $n = 2.47$.
  $n/2 = 47$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 4\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		89 (p)	
11 (p)			83 (p)	$11 + 83$
17 (p)		3 $(mod\ 7)$	77	
23 (p)			71 (p)	$23 + 71$
29 (p)		4 $(mod\ 5)$	65	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		59 (p)	
41 (p)			53 (p)	$41 + 53$
47 (p)			47 (p)	$47 + 47$

- $n = 88$ $(DG : 5, 17, 29, 41)$

  $n = 2^3.11$.
  $n/2 = 44$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 and 7.
  $n \equiv 3\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		83 (p)	
11 (p)		4 $(mod\ 7)$	77	
17 (p)			71 (p)	$17 + 71$
23 (p)		3 $(mod\ 5)$	65	
29 (p)			59 (p)	$29 + 59$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		53 (p)	
41 (p)			47 (p)	$41 + 47$

- $n = 82$ $(GC : 3, 11, 23, 29, 41)$

  $n = 2.41$.
  $n/2 = 41$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 2\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	5 $(mod\ 7)$	77	
11 (p)			71 (p)	$11 + 71$
17 (p)		2 $(mod\ 5)$	65	
23 (p)			59 (p)	$23 + 59$
29 (p)			53 (p)	$29 + 53$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		47 (p)	
41 (p)			41 (p)	$41 + 41$

- $n = 76$ $(GC : 3, 5, 17, 23, 29)$

  $n = 2^2.19$.
  $n/2 = 38$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 1\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		71 (p)	
11 (p)		1 $(mod\ 5)$	65	
17 (p)			59 (p)	$17 + 59$
23 (p)			53 (p)	$23 + 53$
29 (p)			47 (p)	$29 + 47$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		41 (p)	

- $n = 70$ $(GC : 3, 11, 17, 23, 29)$

  $n = 2.5.7$.
  $n/2 = 35$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		65	
11 (p)			59 (p)	$11 + 59$
17 (p)			53 (p)	$17 + 53$
23 (p)			47 (p)	$23 + 47$
29 (p)			41 (p)	$29 + 41$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		35	

- $n = 64$ $(GC : 3, 5, 11, 17, 23)$

  $n = 2^6$.
  $n/2 = 32$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		59 (p)	
11 (p)			53 (p)	$11 + 53$
17 (p)			47 (p)	$17 + 47$
23 (p)			41 (p)	$23 + 41$
29 (p)		4 $(mod\ 5)$ *et* 1 $(mod\ 7)$	35	

- $n = 58$ $(GC : 5, 11, 17, 29)$

  $n = 2.29$.
  $n/2 = 29$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		53 (p)	
11 (p)			47 (p)	$11 + 47$
17 (p)			41 (p)	$17 + 41$
23 (p)		3 $(mod\ 5)$ *et* 2 $(mod\ 7)$	35	
29 (p)			29 (p)	$29 + 29$

- $n = 52$ $(GC : 5, 11, 23)$

  $n = 2^2.13$.
  $n/2 = 26$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		47 (p)	
11 (p)			41 (p)	$11 + 41$
17 (p)		2 $(mod\ 5)$ *et* 3 $(mod\ 7)$	35	
23 (p)			29 (p)	$23 + 29$

- $n = 46$ $(GC : 3, 5, 17, 23)$

  $n = 2.23$.
  $n/2 = 23$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		41 (p)	
11 (p)		1 $(mod\ 5)$	35	
17 (p)			29 (p)	$17 + 29$
23 (p)			23 (p)	$23 + 23$

- $n = 40$ $(GC : 3, 11, 17)$

  $n = 2^3.5$.
  $n/2 = 20$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	35	
11 (p)		29 (p)	$11 + 29$
17 (p)		23 (p)	$17 + 23$

- $n = 34$ $(GC : 3, 5, 11, 17)$

  $n = 2.17$.
  $n/2 = 17$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 4\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	29 (p)	
11 (p)		23 (p)	$11 + 23$
17 (p)		17 (p)	$17 + 17$

- $n = 28$ $(GC : 5, 11)$

  $n = 2^2.7$.
  $n/2 = 14$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	23	
11 (p)		17 (p)	$11 + 17$

3 Even numbers of the form $n = 6m + 2$ from 140 to 26

The double sieve of Eratosthenes application is presented in a table containing only $\left\lfloor \frac{n}{12} \right\rfloor$ numbers belonging to the arithmetic progression $6k + 1$.

- $n = 140$ $(GC : 3, 13, 31, 37, 43, 61, 67)$

  $n = 2^2.5.7.$
  $n/2 = 70.$
  $11 < \sqrt{n} < 13.$ The moduli to be considered are 5, 7 *and* 11.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 8\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$		133	
13 (p)			127 (p)	$13 + 127$
19 (p)		8 $(mod\ 11)$	121	
25	0 $(mod\ 5)$		115	
31 (p)			109 (p)	$31 + 109$
37 (p)			103 (p)	$37 + 103$
43 (p)			97 (p)	$43 + 97$
49	0 $(mod\ 7)$		91	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		85	
61 (p)			79 (p)	$61 + 79$
67 (p)			73 (p)	$67 + 73$

- $n = 134$ $(GC : 3, 7, 31, 37, 61, 67)$

  $n = 2.67.$
  $n/2 = 67.$
  $11 < \sqrt{n} < 13.$ The moduli to be considered are 5, 7 *and* 11.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7), n \equiv 2\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$		127 (p)	
13 (p)		2 $(mod\ 11)$	121	
19 (p)		4 $(mod\ 5)$	115	
25	0 $(mod\ 5)$		109 (p)	
31 (p)			103 (p)	$31 + 103$
37 (p)			97 (p)	$37 + 97$
43 (p)		1 $(mod\ 7)$	91	
49	0 $(mod\ 7)$	4 $(mod\ 5)$	85	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		79 (p)	
61 (p)			73 (p)	$61 + 73$
67 (p)			67 (p)	$67 + 67$

- $n = 128$ $(GC : 19, 31, 61)$

  $n = 2^7.$
  $n/2 = 64.$
  $11 < \sqrt{n} < 13.$ The moduli to be considered are 5, 7 *and* 11.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 7\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$	7 $(mod\ 11)$	121	
13 (p)		3 $(mod\ 5)$	115	
19 (p)			109 (p)	$19 + 109$
25	0 $(mod\ 5)$		103 (p)	
31 (p)			97 (p)	$31 + 97$
37 (p)		2 $(mod\ 7)$	93	
43 (p)		3 $(mod\ 5)$	87	
49	0 $(mod\ 7)$		81	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		75	
61			69 (p)	$61 + 69$

- $n = 122$ $(GC : 13, 19, 43, 61)$

  $n = 2.61$.
  $n/2 = 61$.
  $11 < \sqrt{n} < 13$. The moduli to be considered are 5, 7 *and* 11.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	115	
13 (p)			109 (p)	$13 + 109$
19 (p)			103 (p)	$19 + 103$
25	0 $(mod\ 5)$		97 (p)	
31 (p)		3 $(mod\ 7)$	91	
37 (p)		2 $(mod\ 5)$	85	
43 (p)			79 (p)	$43 + 79$
49	0 $(mod\ 7)$		73 (p)	
55	0 $(mod\ 5)$		67 (p)	
61 (p)			61 (p)	$61 + 61$

- $n = 116$ $(GC : 3, 7, 13, 19, 37, 43)$

  $n = 2^2.29$.
  $n/2 = 58$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 1\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		109 (p)	
13 (p)			103 (p)	$13 + 103$
19 (p)			97 (p)	$19 + 97$
25	0 $(mod\ 5)$	4 $(mod\ 7)$	91	
31 (p)		1 $(mod\ 5)$	85	
37 (p)			79 (p)	$37 + 79$
43 (p)			73 (p)	$43 + 73$
49	0 $(mod\ 7)$		67	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		61 (p)	

- $n = 110$ $(GC : 3, 7, 13, 31, 37, 43)$

  $n = 2.5.11$.
  $n/2 = 55$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 0\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		103 (p)	
13 (p)			97 (p)	$13 + 97$
19 (p)		5 $(mod\ 7)$	91	
25	0 $(mod\ 5)$		85	
31 (p)			79 (p)	$31 + 79$
37 (p)			73 (p)	$37 + 73$
43 (p)			67 (p)	$43 + 67$
49	0 $(mod\ 7)$		61 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		55	

- $n = 104$ $(GC : 3, 7, 31, 37, 43)$

  $n = 2^3.13$.
  $n/2 = 52$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 4\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		97 (p)	
13 (p)		6 $(mod\ 7)$	91	
19 (p)		4 $(mod\ 5)$	85	
25	0 $(mod\ 5)$		79 (p)	
31 (p)			73 (p)	$31 + 73$
37 (p)			67 (p)	$37 + 67$
43 (p)			61 (p)	$43 + 61$
49	0 $(mod\ 7)$	4 $(mod\ 5)$	55	

- $n = 98$ $(GC : 19, 31, 37)$

  $n = 2.7^2$.
  $n/2 = 49$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 3\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		91	
13 (p)		3 $(mod\ 5)$	85	
19 (p)			79 (p)	$19 + 79$
25	0 $(mod\ 5)$		73	
31 (p)			67 (p)	$31 + 67$
37 (p)			61 (p)	$37 + 61$
43 (p)		3 $(mod\ 5)$	55	
49	0 $(mod\ 7)$		49	

- $n = 92$ $(GC : 3, 13, 19, 31)$

  $n = 2^2.23$.
  $n/2 = 46$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 2\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	87	
13 (p)			81 (p)	$13 + 81$
19 (p)			75 (p)	$19 + 75$
25	0 $(mod\ 5)$		69	
31 (p)			63 (p)	$31 + 63$
37 (p)		2 $(mod\ 5)$	57 (p)	
43 (p)		1 $(mod\ 7)$	51	

- $n = 86$ $(GC : 3, 7, 13, 19, 43)$

  $n = 2.43$.
  $n/2 = 43$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 1\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		79 (p)	
13 (p)			73 (p)	$13 + 73$
19 (p)			67 (p)	$19 + 67$
25	0 $(mod\ 5)$		61 (p)	
31 (p)		1 $(mod\ 5)$	55	
37 (p)		2 $(mod\ 7)$	49	
43 (p)			43 (p)	$43 + 43$

- $n = 80 \qquad (GC : 7, 13, 19, 37)$

  $n = 2^4.5.$
  $n/2 = 40.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 0\ (mod\ 5), n \equiv 3\ (mod\ 7).$

7 (p)	0 $(mod\ 7)$		73 (p)	
13 (p)			67 (p)	$13 + 67$
19 (p)			61 (p)	$19 + 61$
25	0 $(mod\ 5)$		55	
31 (p)		3 $(mod\ 7)$	49	
37 (p)			43 (p)	$37 + 43$

- $n = 74 \qquad (GC : 3, 7, 13, 31, 37)$

  $n = 2.37.$
  $n/2 = 37.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7).$

7 (p)	0 $(mod\ 7)$		67 (p)	
13 (p)			61 (p)	$13 + 61$
19 (p)		4 $(mod\ 5)$	55	
25	0 $(mod\ 5)$	4 $(mod\ 7)$	49	
31 (p)			43 (p)	$31 + 43$
37 (p)			37 (p)	$37 + 37$

- $n = 68 \qquad (GC : 7, 31)$

  $n = 2^2.17.$
  $n/2 = 34.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7).$

7 (p)	0 $(mod\ 7)$		61 (p)	
13 (p)		3 $(mod\ 5)$	55	
19 (p)		5 $(mod\ 7)$	49	
25	0 $(mod\ 5)$		43 (p)	
31 (p)			37 (p)	$31 + 37$

- $n = 62 \qquad (GC : 3, 19, 31)$

  $n = 2.31.$
  $n/2 = 31.$
  $7 < \sqrt{n} < 11.$ The moduli to be considered are 5 *and* 7.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7).$

7 (p)	0 $(mod\ 7)$	2 $(mod\ 5)$	55	
13 (p)		6 $(mod\ 7)$	49	
19 (p)			43 (p)	$19 + 43$
25	0 $(mod\ 5)$		37 (p)	
31 (p)			31 (p)	$31 + 31$

- $n = 56$ $(GC : 3, 13, 19)$

  $n = 2^3.7$.
  $n/2 = 28$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		49	
13 (p)			43 (p)	$13 + 43$
19 (p)			37 (p)	$19 + 37$
25	0 $(mod\ 5)$		31	

- $n = 50$ $(GC : 3, 7, 13, 19)$

  $n = 2.5^2$.
  $n/2 = 25$.
  $7 < \sqrt{n} < 11$. The moduli to be considered are 5 *and* 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		43 (p)	
13 (p)			37 (p)	$13 + 37$
19 (p)			31 (p)	$19 + 31$
25	0 $(mod\ 5)$		25	

- $n = 44$ $(GC : 3, 7, 13)$

  $n = 2^2.11$.
  $n/2 = 22$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 4\ (mod\ 5)$.

7 (p)			37 (p)	
13 (p)			31 (p)	$13 + 31$
19 (p)		4 $(mod\ 5)$	25	

- $n = 38$ $(GC : 7, 19)$

  $n = 2.19$.
  $n/2 = 19$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 3\ (mod\ 5)$.

7 (p)			31 (p)	
13 (p)		3 $(mod\ 5)$	25	
19			19 (p)	$19 + 19$

- $n = 32$ $(GC : 3, 13)$

  $n = 2^5$.
  $n/2 = 16$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 2\ (mod\ 5)$.

7 (p)		2 $(mod\ 5)$	25	
13			19 (p)	$13 + 19$

- $n = 26$ $(GC : 3, 7, 13)$

  $n = 2.13$.
  $n/2 = 13$.
  $5 < \sqrt{n} < 7$. The modulus to be considered is 5.
  $n \equiv 1\ (mod\ 5)$.

7 (p)			19 (p)	
13			13 (p)	$13 + 13$

Théorie de Galois et Conjecture de Goldbach

Denise Vella-Chemla

4/2/2013

1 Rappels

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers. 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 $n/2$.

2 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n consiste à chercher un nombre premier p dont le complémentaire à n est premier.

Après lecture d'un extrait de Galois : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$"*, puis de l'extrait de Libri qui fournit sa méthode exhaustive pour trouver les solutions entières d'une équation polynomiale (cf Annexe), on réalise que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tout simplement racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation polynomiale suivante :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0.$$

Les coefficients s'obtiennent ainsi :

$$\begin{aligned}
&26 = 3 + 5 + 7 + 11.\\
&236 = 3.5 + 3.7 + 3.11 + 5.7 + 5.11 + 7.11.\\
&886 = 3.5.7 + 3.5.11 + 3.7.11 + 5.7.11.\\
&1155 = 3.5.7.11.
\end{aligned}$$

Plus généralement, pour exprimer que x, le nombre à chercher, est premier, on utilise une équation polynomiale de la forme :

$$\pm x^{\pi(n-2)-1} \pm \sigma_1.x^{\pi(n-2)-2} \pm \sigma_2.x^{\pi(n-2)-3} \pm \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

La plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1+(n-1)$ n'est jamais considérée comme une décomposition de Goldbach, le -1 servant à éliminer le nombre premier 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers considérés. Par exemple, $\sigma_1 = p_1+p_2+p_3+p_4... = 3+5+7+11...$, $\sigma_2 = p_1p_2+p_1p_3+...+p_2p_3+p_2p_4+...$ et le dernier sigma est le produit de tous les nombres premiers inférieurs à $n-2$.

Pour exprimer que $n-x$, le complémentaire du nombre premier cherché doit être l'un des nombres premiers 3, 5, 7 *ou* 11, on remplace x par $(n-x)$ dans l'équation polynomiale ci-dessus ; on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

Par élévation aux différentes puissances du monôme $n-x$, on obtient :

$$\begin{aligned}(n-x)^4 &= x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.\\ (n-x)^3 &= -x^3 + 3nx^2 - 3n^2x + n^3.\\ (n-x)^2 &= n^2 - 2nx + x^2.\end{aligned}$$

On reconnaît les coefficients du binôme C_i^j dans l'élévation de $n-x$ à la puissance i.

Les résultats de la théorie de Galois sur la résolubilité des équations polynomiales ne pourraient-ils pas être utilisés ici pour montrer que notre système de deux équations admet toujours une solution en x au moins ?

3 Pgcd des polynômes

Dans la mesure où l'on cherche une racine r qui vérifie et la première et la deuxième équation, le fait que les deux polynômes en question aient un pgcd différent de 1 assurerait l'existence d'une telle racine.

Avec l'outil libre Sage, on expérimente cette idée à la recherche des décomposants de Goldbach de 14.

$Sage : decomp14 = var('x')$
$Sage : eq1 = x^5 - 39 * x^4 + 574 * x^3 - 3954 * x^2 + 12673 * x - 15015$
$Sage : eq2 = -x^5 + 31 * x^4 - 350 * x^3 + 1730 * x^2 - 3489 * x + 2079$
$Sage : eq1.gcd(eq2)$

$Sage :\ x^3 - 21 * x^2 + 131 * x - 231$

$Sage : eq4 = x^3 - 21 * x^2 + 131 * x - 231 == 0$

$Sage : solve([eq4], x)$
$Sage :\ [x == 7, x == 11, x == 3]$

Intéressons-nous maintenant, comme le suggère Galois en proposant comme deuxième équation $x^{p-1} = 1$ dans la phrase *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à Fx = 0 et à* $x^{p-1} = 1$*"* au groupe des unités, qui ne contient d'ailleurs que des nombres impairs si n est pair.

4 Le groupe des unités

Rappelons que 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 $n/2$.

La structure du groupe des unités $(Z/nZ)^\times$ est bien connue. On la trouve notamment dans [3].

Notons $G_n = (\mathbb{Z}/n\mathbb{Z})^\times/\{1,-1\}$, le quotient de $(\mathbb{Z}/n\mathbb{Z})^\times$ par le sous-groupe $\{1,-1\}$.

La structure du groupe G_n dans lequel on se place pour trouver des décomposants de Goldbach de n se déduit aisément de la structure de $(\mathbb{Z}/n\mathbb{Z})^\times$, comme présenté dans le tableau ci-après. G_n est de structure cyclique C_k si $(\mathbb{Z}/n\mathbb{Z})^\times$ est de structure cyclique C_{2k} ou bien de structure $\prod C_i$ si $(\mathbb{Z}/n\mathbb{Z})^\times$ est de structure $C2.\prod C_i$.

n	$facto(n)$	$(\mathbb{Z}/n\mathbb{Z})^\times$	G_n	n	$facto(n)$	$(\mathbb{Z}/n\mathbb{Z})^\times$	G_n
8	2^3	Id	$C2$	60	$2^2.3.5$	$C4.C2.C2$	$C4.C2$
10	2.5	$C4$	$C2$	62	2.31	$C30$	$C15$
12	$2^2.3$	$C2.C4$	$C2$	64	2^6	$C16.C2$	$C16$
14	2.7	$C6$	$C3$	66	$2.3.11$	$C10.C2$	$C10$
16	2^4	$C4.C2$	$C4$	68	$2^2.17$	$C16.C2$	$C16$
18	2.3^2	$C6$	$C3$	70	$2.5.7$	$C12.C2$	$C12$
20	$2^2.5$	$C4.C2$	$C4$	72	$2^3.3^2$	$C6.C2.C2$	$C6.C2$
22	2.11	$C10$	$C5$	74	2.37	$C36$	$C18$
24	$2^3.3$	$C2.C2.C2$	$C2.C2$	76	$2^2.19$	$C18.C2$	$C18$
26	2.13	$C12$	$C6$	78	$2.3.13$	$C12.C2$	$C12$
28	$2^2.7$	$C6.C2$	$C6$	80	$2^4.5$	$C4.C4.C2$	$C4.C4$
30	$2.3.5$	$C4.C2$	$C4$	82	2.41	$C40$	$C20$
32	2^5	$C8.C2$	$C8$	84	$2^2.3.7$	$C6.C2.C2$	$C6.C2$
34	2.17	$C16$	$C8$	86	2.43	$C42$	$C21$
36	$2^2.3^2$	$C6.C2$	$C6$	88	$2^3.11$	$C10.C2.C2$	$C10.C2$
38	2.19	$C18$	$C9$	90	$2.3^2.5$	$C12.C2$	$C12$
40	$2^3.5$	$C4.C2.C2$	$C4.C2$	92	$2^2.23$	$C22.C2$	$C22$
42	$2.3.7$	$C6.C2$	$C6$	94	2.47	$C46$	$C23$
44	$2^2.11$	$C10.C2$	$C10$	96	$2^5.3$	$C8.C2.C2$	$C8.C2$
46	2.23	$C22$	$C11$	98	2.7^2	$C42$	$C21$
48	$2^4.3$	$C4.C2.C2$	$C4.C2$	100	$2^2.5^2$	$C20.C2$	$C20$
50	2.5^2	$C20$	$C10$				
52	$2^2.13$	$C12.C2$	$C12$				
54	2.3^3	$C18$	$C9$	242	2.11^2	$C55.C2$	$C55$
56	$2^3.7$	$C6.C2.C2$	$C6.C2$				
58	2.29	$C28$	$C14$				

Pour les nombres pairs de la forme $2p$, avec p premier impair, qui vérifient trivialement la conjecture puisqu'alors $2p = p + p$, G_n est le groupe cyclique $C_{\frac{p-1}{2}}$.

Pour les nombres pairs de la forme $4p$ ou $6p$ avec p premier impair, G_n est le groupe cyclique C_{p-1}.

Pour les nombres pairs de la forme 2^k, G_n est le groupe cyclique $C_{2^{k-2}}$.

Pour les nombres pairs de la forme $2p^2$, G_n est le groupe cyclique $C_{p(\frac{p-1}{2})}$.

Ne serait-il pas possible de déduire l'existence de décomposants de Goldbach pour les nombres pairs doubles de nombres composés de l'existence triviale de décomposants de Goldbach pour les nombres pairs doubles de nombres premiers sous prétexte qu'il existe un isomorphisme entre leurs groupes respectifs ?

Par exemple, on voit que 98 a pour groupe $G_{98} = C_{21}$ car $7(\frac{7-1}{2}) = 21$. Mais $86 = 2.43$ a également pour groupe $G_{86} = C_{21}$. L'existence d'une solution pour l'équation polynomiale associée à 86 cumulée à l'équation correspondant au groupe cyclique C_{21} qui est $x^{21} = 1$ comme expliqué par Galois n'entraîne-t-elle pas automatiquement l'existence d'une solution pour l'équation polynomiale associée à 98 ?

Bibliographie

[1], **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 42 8, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2], **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

[3], **Gilles Bailly-Maitre**, *Arithmétique et Cryptologie*, éditions Ellipses, 2012.

Equations polynomiales modulaires et Conjecture de Goldbach

Denise Vella-Chemla

5/2/2013

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.

1 Modéliser la recherche des décomposants de Goldbach par des équations algébriques

Chercher un décomposant de Goldbach p d'un nombre pair n consiste à chercher un nombre premier p dont le complémentaire à n est premier.

Après lecture d'un extrait de Galois : *"Ensuite, pour avoir les solutions entières, il suffira, ainsi que M. Libri paraît en avoir fait le premier la remarque, de chercher le plus grand facteur commun à $Fx = 0$ et à $x^{p-1} = 1$"*, puis de l'extrait de Libri qui fournit sa méthode exhaustive pour trouver les solutions entières d'une équation polynomiale, on réalise que les nombres premiers 3, 5, 7 *et* 11, par exemple, sont tout simplement racines de l'équation polynomiale

$$(x-3)(x-5)(x-7)(x-11) = 0.$$

En développant le produit, on obtient l'équation de degré 4 :

$$x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0. \quad (1)$$

Les coefficients s'obtiennent ainsi :

$26 = 3 + 5 + 7 + 11.$
$236 = 3.5 + 3.7 + 3.11 + 5.7 + 5.11 + 7.11.$
$886 = 3.5.7 + 3.5.11 + 3.7.11 + 5.7.11.$
$1155 = 3.5.7.11.$

Plus généralement, pour exprimer que x, un décomposant de Goldbach de n, est premier, on utilise une équation polynomiale de la forme :

$$x^{\pi(n-2)-1} - \sigma_1.x^{\pi(n-2)-2} + \sigma_2.x^{\pi(n-2)-3} - \sigma_3.x^{\pi(n-2)-1} \ldots = 0$$

En utilisant la notation $\pi(n)$ pour la fonction de décompte des nombres premiers inférieurs ou égaux à n, la plus grande puissance de x est $\pi(n-2)-1$ parce que la décomposition $1 + (n-1)$ n'est jamais considérée comme une décomposition de Goldbach et qu'on souhaite éliminer le nombre premier pair 2. Les nombres σ_i désignent respectivement les sommes de produits de i nombres premiers pris parmi tous les nombres premiers considérés. Par exemple, $\sigma_1 = p_1 + p_2 + p_3 + p_4... = 3 + 5 + 7 + 11...$, $\sigma_2 = p_1p_2 + p_1p_3 + ... + p_2p_3 + p_2p_4 + ...$ et le dernier sigma est le produit de tous les nombres premiers impairs inférieurs à $n-2$.

Pour trouver par exemple les décomposants de Goldbach des nombres pairs compris entre les nombres premiers 11 et 13, pour exprimer que $n - x$, le complémentaire du nombre premier cherché doit être l'un

des nombres premiers 3, 5, 7 ou 11, on remplace x par $(n-x)$ dans l'équation polynomiale (1) ci-dessus ; on obtient l'équation polynomiale suivante :

$$(n-x)^4 - 26(n-x)^3 + 236(n-x)^2 - 886(n-x) + 1155 = 0.$$

Par élévation aux différentes puissances du monôme $n-x$, on obtient :

$$(n-x)^4 = x^4 - 4nx^3 + 6n^2x^2 - 4n^3x + n^4.$$
$$(n-x)^3 = -x^3 + 3nx^2 - 3n^2x + n^3.$$
$$(n-x)^2 = n^2 - 2nx + x^2.$$

Remplaçons n par 12, on obtient le polynôme $x^4 - 22x^3 + 164x^2 - 458x + 315 = 0$, qui est bien le développement de $(x-1)(x-5)(x-7)(x-9)$ dont chaque racine est le complémentaire à 12 d'un nombre premier inférieur à 12.

En annexe 1 sont fournis les 2 polynômes dont les racines sont soit les nombres premiers inférieurs à n, soit leur complémentaire à n pour les nombres n compris entre 6 et 18 (ainsi que leur pgcd étudié dans la section suivante).

2 Pgcd des polynômes

Dans la mesure où l'on cherche une racine r qui vérifie et la première et la deuxième équation, le fait que les deux polynômes en question aient un pgcd différent de 1 assurerait l'existence d'une telle racine, et ainsi l'existence d'un décomposant de Goldbach pour n.

Avec l'outil libre Sage, on expérimente cette idée à la recherche des décomposants de Goldbach de 14.

$Sage : decomp14 = var('x')$
$Sage : eq1 = x^5 - 39 * x^4 + 574 * x^3 - 3954 * x^2 + 12673 * x - 15015$
$Sage : eq2 = -x^5 + 31 * x^4 - 350 * x^3 + 1730 * x^2 - 3489 * x + 2079$
$Sage : eq1.gcd(eq2)$

$Sage : x^3 - 21 * x^2 + 131 * x - 231$

$Sage : eq4 = x^3 - 21 * x^2 + 131 * x - 231 == 0$

$Sage : solve([eq4], x)$
$Sage : [x == 7, x == 11, x == 3]$

Comme attendu, les racines du polynôme pgcd sont bien les décomposants de Goldbach de 14.

3 Factorisation modulo p

Lors d'une conférence donnée dans le cadre du bicentenaire de la naissance de Galois, Alain Connes présente la théorie de Galois et fournit deux exemples de factorisation de polynômes modulo différents nombres premiers. Testons cette factorisation sur les polynômes pgcd trouvés dans la section précédente.

Pour $n = 8$, le pgcd des polynômes est $x^2 - 8x + 15$.
Dans $\mathbb{Z}/3\mathbb{Z}$, ce polynôme est égal à $x^2 + x$ qui est trivialement annulable donc 3 est décomposant de Goldbach de 8.
De même, dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme pgcd est égal à $x^2 + 2x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 8.

Pour $n = 10$, le pgcd des polynômes est $x^3 - 15x^2 + 71x - 105$.
Dans $\mathbb{Z}/3\mathbb{Z}$, ce polynôme est égal à $x^3 + 2x$ qui est trivialement annulable donc 3 est décomposant de Goldbach de 10.

De même, dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme pgcd est égal à $x^3 + x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 10 (décomposition de Goldbach dite triviale).

Pour $n = 12$, le pgcd des polynômes est $x^2 - 12x + 35$.
Dans $\mathbb{Z}/5\mathbb{Z}$, ce polynôme est égal à $x^2 + 3x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 12.

Pour $n = 14$, le pgcd des polynômes est $x^3 - 21x^2 + 131x - 231$.
Dans $\mathbb{Z}/3\mathbb{Z}$, ce polynôme est égal à $x^3 + 2x$ qui est trivialement annulable donc 3 est décomposant de Goldbach de 14.
Par contre, dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme pgcd est égal à $x^3 + 4x^2 + x + 4$ qui n'est pas annulable par un entier et donc 5 n'est pas décomposant de Goldbach de 8.

Pour $n = 16$, le pgcd des polynômes est $x^4 - 32x^3 + 350x^2 - 1504x + 2145$.
Dans $\mathbb{Z}/3\mathbb{Z}$, ce polynôme est égal à $x^4+x^3+2x^2+2x$ qui est trivialement annulable donc 3 est décomposant de Goldbach de 16.
De même, dans $\mathbb{Z}/5\mathbb{Z}$, le polynôme pgcd devient $x^4 + 3x^3 + x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 16.
Par contre, dans $\mathbb{Z}/7\mathbb{Z}$, le polynôme pgcd est égal à $x^4 + 3x^3 + x + 4$ qui n'est pas annulable par un entier donc 7 n'est pas décomposant de Goldbach de 16.

Pour $n = 18$, le pgcd des polynômes est $x^4 - 36x^3 + 466x^2 - 2556x + 5005$.
Dans $\mathbb{Z}/5\mathbb{Z}$, ce polynôme est égal à $x^4+4x^3+x^2+4x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 18.
De même, dans $\mathbb{Z}/7\mathbb{Z}$, le polynôme pgcd est égal à $x^4 + 6x^3 + 4x^2 + 6x$ qui est trivialement annulable donc 5 est décomposant de Goldbach de 8.

4 A quelle condition le pgcd factorisé dans un certain corps premier est-il trivialement annulable ?

On voit aisément que le polynôme pgcd sera trivialement annulable dans un corps premier $\mathbb{Z}/p\mathbb{Z}$ à chaque fois qu'on réussira à éliminer la constante, habituellement dénotée a_0 du polynôme de la forme $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$.

A quoi est égale la constante a_0 du polynôme pgcd ? Etudions quelques exemples :

- pour $n = 6$, la constante a_0 est égale à $\frac{3.5}{1.3} = 3$;
- pour $n = 8$, la constante a_0 est égale à $\frac{3.5.7}{1.3.5} = 15$;
- pour $n = 10$, la constante a_0 est égale à $\frac{3.5.7}{3.5.7} = 105$;
- pour $n = 12$, la constante a_0 est égale à $\frac{3.5.7.11}{1.5.7.9} = 35$;
- pour $n = 14$, la constante a_0 est égale à $\frac{3.5.7.11.13}{1.3.7.9.11} = 231$;
- pour $n = 16$, la constante a_0 est égale à $\frac{3.5.7.11.13}{3.5.9.11.13} = 2145$;
- pour $n = 18$, la constante a_0 est égale à $\frac{3.5.7.11.13.17}{1.5.7.11.13.15} = 5005$;

La constante a_0 est le produit des décomposants de Goldbach de n. Il faudrait être capable de prouver que cette constante n'est jamais égale à 1.

5 Résumé et obstacle

On prend l'équation polynômiale $Fx = 0$ avec Fx produit des $(x - p_i)$ avec p_i un nombre premier impair inférieur à n, le nombre pair dont on cherche des décompositions de Goldbach.

On utilise le générateur $x \mapsto n - x$ qui envoie trivialement les décomposants de Goldbach les uns sur les autres.

Le polynôme Fx s'annule pour les nombres premiers ainsi que pour leur complémentaire, obtenu par le générateur, lorsque ce complémentaire est premier. Il ne s'annule pas pour les valeurs des complémentaires lorsque ceux-ci sont des nombres composés. Il faudrait être capable de démontrer que le groupe de Galois associé au polynôme Fx rend ce polynôme obligatoirement réductible modulo l'un des p_i. Malheureusement, parmi les unités $\mathbb{Z}/n\mathbb{Z}$, les nombres premiers pris seuls ne forment pas un sous-groupe (est une unité tout nombre qui est premier à n, les nombres premiers ne divisant pas n sont des unités mais les nombres composés premiers à n sont des unités également).

Il faudrait être capable de trouver un autre polynôme, qui serait invariant par le générateur proposé et qui serait tel que, comme le dit Galois, $Fx = 0$ et $x^{\varphi(n)} = 1$ auraient un facteur commun qui soit de degré 1 ou plus.

Bibliographie

[1] **Evariste Galois**, *Sur la théorie des nombres*, Bulletin des Sciences mathématiques de M. Férussac, tome XIII, page 42 8, juin 1830. Note de J. Liouville : ce mémoire fait partie des recherches de M. Galois sur la théorie des permutations et des équations algébriques.

[2] **Guillaume Libri**, *Mémoire sur la théorie des nombres*, in *Mémoires de mathématiques*, extraits du *Journal de Mathématiques Pures et Appliquées*, publié par A.L. Crelle, Berlin, 1835, p.44.

[3] **Alain Connes**, *Conférence donnée à l'Académie des Sciences à l'occasion du bicentenaire de la naissance d'Evariste Galois*, vidéo visionnable à l'adresse $http://www.youtube.com/watch?v=rMb9UE5msH8$ et transparents téléchargeables à l'adresse $http://www.alainconnes.org/fr/downloads.php$ sous l'entrée Conférence Galois de la section Autres conférences.

Annexe : polynômes pour n compris entre 6 et 18 et leur pgcd

- $n = 6$

$$\begin{cases} x^2 - 8x + 15 = 0 \\ x^2 - 4x + 3 = 0 \end{cases} \longrightarrow \quad pgcd : x - 3$$

- $n = 8$

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 9x^2 - 23x + 15 = 0 \end{cases} \longrightarrow \quad pgcd = x^2 - 8x + 15 = 0$$

- $n = 10$

$$\begin{cases} x^3 - 15x^2 + 71x - 105 = 0 \\ -x^3 + 15x^2 - 71x + 105 = 0 \end{cases} \longrightarrow \quad pgcd = x^3 - 15x^2 + 71x - 105 = 0$$

- $n = 12$

$$\begin{cases} x^4 - 26x^3 + 236x^2 - 886x + 1155 = 0 \\ x^4 - 22x^3 + 164x^2 - 458x + 315 = 0 \end{cases} \longrightarrow \quad pgcd = x^2 - 12x + 35 = 0$$

- $n = 14$

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 31x^4 - 350x^3 + 1730x^2 - 3489x + 2079 = 0 \end{cases}$$
$$\longrightarrow \quad pgcd = x^3 - 21x^2 + 131x - 231 = 0$$

- $n = 16$

$$\begin{cases} x^5 - 39x^4 + 574x^3 - 3954x^2 + 12673x - 15015 = 0 \\ -x^5 + 41x^4 - 638x^3 + 4654x^2 + 15681x - 19305 = 0 \end{cases}$$
$$\longrightarrow \quad pgcd = x^4 - 32x^3 + 350x^2 - 1504x + 2145 = 0$$

- $n = 18$

$$\begin{cases} x^6 - 56x^5 + 1237x^4 - 13712x^3 + 79891x^2 - 230456x + 255255 = 0 \\ x^6 - 52x^5 + 1057x^4 - 10552x^3 + 52891x^2 - 118420x + 75075 = 0 \end{cases}$$
$$\longrightarrow \quad pgcd = x^4 - 36x^3 + 466x^2 - 2556x + 5005 = 0$$

```
gap> LoadPackage(« loops ») ;
true

n=12
gap> CanonicalCayleyTable([[1,5],[5,1]]);
[ [ 1, 2 ], [ 2, 1 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 2 with 2 generators>
gap> IsCyclic(last);
true

n=14
gap> CanonicalCayleyTable([[1,3,5],[3,5,1],[5,1,3]]);
[ [ 1, 2, 3 ], [ 2, 3, 1 ], [ 3, 1, 2 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 3 with 3 generators>
gap> IsCyclic(last);
true

n=16
gap> CanonicalCayleyTable([[1,3,5,7],[3,7,1,5],[5,1,7,3],[7,5,3,1]]);
[ [ 1, 2, 3, 4 ], [ 2, 4, 1, 3 ], [ 3, 1, 4, 2 ], [ 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 4 with 4 generators>
gap> IsCyclic(last);
true

n=18
gap> CanonicalCayleyTable([[1,5,7],[5,7,1],[7,1,5]]);[ [ 1, 2, 3 ], [ 2, 3, 1 ], [ 3, 1, 2 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 3 with 3 generators>
gap> IsCyclic(last);
true

n=20
gap> CanonicalCayleyTable([[1,3,7,9],[3,9,1,7],[7,1,9,3],[9,7,3,1]]);
[ [ 1, 2, 3, 4 ], [ 2, 4, 1, 3 ], [ 3, 1, 4, 2 ], [ 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 4 with 4 generators>
gap> IsCyclic(last);
true

n=22
gap> CanonicalCayleyTable([[1,3,5,7,9],[3,9,7,1,5],[5,7,3,9,1],[7,1,9,5,3],[9,5,1,3,7]]);
[ [ 1, 2, 3, 4, 5 ], [ 2, 5, 4, 1, 3 ], [ 3, 4, 2, 5, 1 ], [ 4, 1, 5, 3, 2 ],
  [ 5, 3, 1, 2, 4 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 5 with 5 generators>
gap> IsCyclic(last);
true
```

n=24
gap> CanonicalCayleyTable([[1,5,7,11],[5,1,11,7],[7,11,1,5],[11,7,5,1]]);[[1, 2, 3, 4], [2, 1, 4, 3],
[3, 4, 1, 2], [4, 3, 2, 1]]
gap> GroupByMultiplicationTable(ct);
<group of size 4 with 4 generators>
gap> IsCyclic(last);
false

n=26
gap> CanonicalCayleyTable([[1,3,5,7,9,11],[3,9,11,5,1,7],[5,11,1,9,7,3],[7,5,9,3,11,1],
[9,1,7,11,3,5],[11,7,3,1,5,9]]);
[[1, 2, 3, 4, 5, 6], [2, 5, 6, 3, 1, 4], [3, 6, 1, 5, 4, 2],
  [4, 3, 5, 2, 6, 1], [5, 1, 4, 6, 2, 3], [6, 4, 2, 1, 3, 5]]
gap> GroupByMultiplicationTable(ct);
<group of size 6 with 6 generators>
gap> IsCyclic(last);
true

n=28
gap> CanonicalCayleyTable([[1,3,5,9,11,13],[3,9,13,1,5,11],[5,13,3,11,1,9],[9,1,11,3,13,5],
[11,5,1,13,9,3],[13,11,9,5,3,1]]);
[[1, 2, 3, 4, 5, 6], [2, 4, 6, 1, 3, 5], [3, 6, 2, 5, 1, 4],
  [4, 1, 5, 2, 6, 3], [5, 3, 1, 6, 4, 2], [6, 5, 4, 3, 2, 1]]
gap> GroupByMultiplicationTable(ct);
<group of size 6 with 6 generators>
gap> IsCyclic(last);
true

n=30
gap> CanonicalCayleyTable([[1,7,11,13],[7,11,13,1],[11,13,1,7],[13,1,7,11]]);[[1, 2, 3, 4], [2, 3,
4, 1], [3, 4, 1, 2], [4, 1, 2, 3]]
gap> GroupByMultiplicationTable(ct);
<group of size 4 with 4 generators>
gap> IsCyclic(last);
true

n=32
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15],[3,9,15,11,5,1,7,13],[5,15,7,3,13,9,1,11],
[7,11,3,15,1,13,5,9],[9,5,13,1,15,3,11,7],[11,1,9,13,3,7,15,5],[13,7,1,5,11,15,9,3],
[15,13,11,9,7,5,3,1]]);
[[1, 2, 3, 4, 5, 6, 7, 8], [2, 5, 8, 6, 3, 1, 4, 7],
  [3, 8, 4, 2, 7, 5, 1, 6], [4, 6, 2, 8, 1, 7, 3, 5],
  [5, 3, 7, 1, 8, 2, 6, 4], [6, 1, 5, 7, 2, 4, 8, 3],
  [7, 4, 1, 3, 6, 8, 5, 2], [8, 7, 6, 5, 4, 3, 2, 1]]
gap> GroupByMultiplicationTable();
<group of size 8 with 8 generators>
gap> IsCyclic(last);
true

```
n=34
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11],[3,9,11,5,1,7],[5,11,1,9,7,3],[7,5,9,3,11,1],
[9,1,7,11,3,5],[11,7,3,1,5,9]]);
[ [ 1, 2, 3, 4, 5, 6 ], [ 2, 5, 6, 3, 1, 4 ], [ 3, 6, 1, 5, 4, 2 ],
  [ 4, 3, 5, 2, 6, 1 ], [ 5, 1, 4, 6, 2, 3 ], [ 6, 4, 2, 1, 3, 5 ] ]
gap> GroupByMultiplicationTable();
<group of size 6 with 6 generators>
gap> IsCyclic(last);
true

n=36
gap> ct:=CanonicalCayleyTable([[1,5,7,11,13,17],[5,11,1,17,7,13],[7,1,13,5,17,11],[11,17,5,13,1,7],
[13,7,17,1,11,5],[17,13,11,7,5,1]]);
[ [ 1, 2, 3, 4, 5, 6 ], [ 2, 4, 1, 6, 3, 5 ], [ 3, 1, 5, 2, 6, 4 ],
  [ 4, 6, 2, 5, 1, 3 ], [ 5, 3, 6, 1, 4, 2 ], [ 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable();
<group of size 6 with 6 generators>
gap> IsCyclic(last);
true

n=38
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17],[3,9,15,17,11,5,1,7,13],
[5,15,13,3,7,17,11,1,9],[7,17,3,11,13,1,15,9,5],[9,11,7,13,5,15,3,17,1],[11,5,17,1,15,7,9,13,3],
[13,1,11,15,3,9,17,5,7],[15,7,1,9,17,13,5,3,11],[17,13,9,5,1,3,7,11,15]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9 ], [ 2, 5, 8, 9, 6, 3, 1, 4, 7 ],
  [ 3, 8, 7, 2, 4, 9, 6, 1, 5 ], [ 4, 9, 2, 6, 7, 1, 8, 5, 3 ],
  [ 5, 6, 4, 7, 3, 8, 2, 9, 1 ], [ 6, 3, 9, 1, 8, 4, 5, 7, 2 ],
  [ 7, 1, 6, 8, 2, 5, 9, 3, 4 ], [ 8, 4, 1, 5, 9, 7, 3, 2, 6 ],
  [ 9, 7, 5, 3, 1, 2, 4, 6, 8 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 9 with 9 generators>
gap> IsCyclic(last);
true

n=40
gap> ct:=CanonicalCayleyTable([[1,3,7,9,11,13,17,19],[3,9,19,13,7,1,11,17],[7,19,9,17,3,11,1,13],
[9,13,17,1,19,3,7,11],[11,7,3,19,1,17,13,9],[13,1,11,3,17,9,19,7],[17,11,1,7,13,19,9,3],
[19,17,13,11,9,7,3,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8 ], [ 2, 4, 8, 6, 3, 1, 5, 7 ],
  [ 3, 8, 4, 7, 2, 5, 1, 6 ], [ 4, 6, 7, 1, 8, 2, 3, 5 ],
  [ 5, 3, 2, 8, 1, 7, 6, 4 ], [ 6, 1, 5, 2, 7, 4, 8, 3 ],
  [ 7, 5, 1, 3, 6, 8, 4, 2 ], [ 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 8 with 8 generators>
gap> IsCyclic(last);
false

n=42
gap> ct:=CanonicalCayleyTable([[1,5,11,13,17,19],[5,17,13,19,1,11],[11,13,5,17,19,1],
[13,19,17,1,11,5],[17,1,19,11,5,13],[19,11,1,5,13,17]]);
[ [ 1, 2, 3, 4, 5, 6 ], [ 2, 5, 4, 6, 1, 3 ], [ 3, 4, 2, 5, 6, 1 ],
  [ 4, 6, 5, 1, 3, 2 ], [ 5, 1, 6, 3, 2, 4 ], [ 6, 3, 1, 2, 4, 5 ] ]
```

```
gap> GroupByMultiplicationTable(ct);
<group of size 6 with 6 generators>
gap> IsCyclic(last);
true


n=44
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,13,15,17,19,21],[3,9,15,21,17,5,1,7,13,19],
[5,15,19,9,1,21,13,3,7,17],[7,21,9,5,19,3,17,13,1,15],[9,17,1,19,7,15,3,21,5,13],
[13,5,21,3,15,7,19,1,17,9],[15,1,13,17,3,19,5,9,21,7],[17,7,3,13,21,1,9,19,15,5],
[19,13,7,1,5,17,21,15,9,3],[21,19,17,15,13,9,7,5,3,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 ], [ 2, 5, 7, 10, 8, 3, 1, 4, 6, 9 ],
  [ 3, 7, 9, 5, 1, 10, 6, 2, 4, 8 ], [ 4, 10, 5, 3, 9, 2, 8, 6, 1, 7 ],
  [ 5, 8, 1, 9, 4, 7, 2, 10, 3, 6 ], [ 6, 3, 10, 2, 7, 4, 9, 1, 8, 5 ],
  [ 7, 1, 6, 8, 2, 9, 3, 5, 10, 4 ], [ 8, 4, 2, 6, 10, 1, 5, 9, 7, 3 ],
  [ 9, 6, 4, 1, 3, 8, 10, 7, 5, 2 ], [ 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 10 with 10 generators>
gap> IsCyclic(last);
true

n=46
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21],[3,9,15,21,19,13,7,1,5,11,17],
[5,15,21,11,1,9,19,17,7,3,13],[7,21,11,3,17,15,1,13,19,5,9],[9,19,1,17,11,7,21,3,15,13,5],
[11,13,9,15,7,17,5,19,3,21,1],[13,7,19,1,21,5,15,11,9,17,3],[15,1,17,13,3,19,11,5,21,9,7],
[17,5,7,19,15,3,9,21,13,1,11],[19,11,3,5,13,21,17,9,1,7,15],[21,17,13,9,5,1,3,7,11,15,19]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 ], [ 2, 5, 8, 11, 10, 7, 4, 1, 3, 6, 9 ]
    , [ 3, 8, 11, 6, 1, 5, 10, 9, 4, 2, 7 ],
  [ 4, 11, 6, 2, 9, 8, 1, 7, 10, 3, 5 ], [ 5, 10, 1, 9, 6, 4, 11, 2, 8, 7, 3 ]
    , [ 6, 7, 5, 8, 4, 9, 3, 10, 2, 11, 1 ],
  [ 7, 4, 10, 1, 11, 3, 8, 6, 5, 9, 2 ], [ 8, 1, 9, 7, 2, 10, 6, 3, 11, 5, 4 ]
    , [ 9, 3, 4, 10, 8, 2, 5, 11, 7, 1, 6 ],
  [ 10, 6, 2, 3, 7, 11, 9, 5, 1, 4, 8 ],
  [ 11, 9, 7, 5, 3, 1, 2, 4, 6, 8, 10 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 11 with 11 generators>
gap> IsCyclic(last);
true

n=48
gap> ct:=CanonicalCayleyTable([[1,5,7,11,13,17,19,23],[5,23,13,7,17,11,1,19],
[7,13,1,19,5,23,11,17],[11,7,19,23,1,5,17,13],[13,17,5,1,23,19,7,11],[17,11,23,5,19,1,13,7],
[19,1,11,17,7,13,23,5],[23,19,17,13,11,7,5,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8 ], [ 2, 8, 5, 3, 6, 4, 1, 7 ],
  [ 3, 5, 1, 7, 2, 8, 4, 6 ], [ 4, 3, 7, 8, 1, 2, 6, 5 ],
  [ 5, 6, 2, 1, 8, 7, 3, 4 ], [ 6, 4, 8, 2, 7, 1, 5, 3 ],
  [ 7, 1, 4, 6, 3, 5, 8, 2 ], [ 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(ct);
<group of size 8 with 8 generators>
gap> IsCyclic(last);
false
```

n=50
ct:=CanonicalCayleyTable([[1,3,7,9,11,13,17,19,21,23],[3,9,21,23,17,11,1,7,13,19],
[7,21,1,13,23,9,19,17,3,11],[9,23,13,19,1,17,3,21,11,7],[11,17,23,1,21,7,13,9,19,3],
[13,11,9,17,7,19,21,3,23,1],[17,1,19,3,13,21,11,23,7,9],[19,7,17,21,9,3,23,11,1,13],
[21,13,3,11,19,23,7,1,9,17],[23,19,11,7,3,1,9,13,17,21]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10], [2, 4, 9, 10, 7, 5, 1, 3, 6, 8],
  [3, 9, 1, 6, 10, 4, 8, 7, 2, 5], [4, 10, 6, 8, 1, 7, 2, 9, 5, 3],
  [5, 7, 10, 1, 9, 3, 6, 4, 8, 2], [6, 5, 4, 7, 3, 8, 9, 2, 10, 1],
  [7, 1, 8, 2, 6, 9, 5, 10, 3, 4], [8, 3, 7, 9, 4, 2, 10, 5, 1, 6],
  [9, 6, 2, 5, 8, 10, 3, 1, 4, 7], [10, 8, 5, 3, 2, 1, 4, 6, 7, 9]]
gap> GroupByMultiplicationTable(ct);
<group of size 10 with 10 generators>
gap> IsCyclic(last);
true

n=52
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,15,17,19,21,23,25],[3,9,15,21,25,19,7,1,5,11,17,23],
[5,15,25,17,7,3,23,19,9,1,11,21],[7,21,17,3,11,25,1,15,23,9,5,19],[9,25,7,11,23,5,21,3,15,19,1,17],
[11,19,3,25,5,17,9,21,1,23,7,15],[15,7,23,1,21,9,17,5,25,3,19,11],[17,1,19,15,3,21,5,23,11,7,25,9],
[19,5,9,23,15,1,25,11,3,17,21,7],[21,11,1,9,19,23,3,7,17,25,15,5],[23,17,11,5,1,7,19,25,21,15,9,3],
[25,23,21,19,17,15,11,9,7,5,3,1]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12],
  [2, 5, 7, 10, 12, 9, 4, 1, 3, 6, 8, 11],
  [3, 7, 12, 8, 4, 2, 11, 9, 5, 1, 6, 10],
  [4, 10, 8, 2, 6, 12, 1, 7, 11, 5, 3, 9],
  [5, 12, 4, 6, 11, 3, 10, 2, 7, 9, 1, 8],
  [6, 9, 2, 12, 3, 8, 5, 10, 1, 11, 4, 7],
  [7, 4, 11, 1, 10, 5, 8, 3, 12, 2, 9, 6],
  [8, 1, 9, 7, 2, 10, 3, 11, 6, 4, 12, 5],
  [9, 3, 5, 11, 7, 1, 12, 6, 2, 8, 10, 4],
  [10, 6, 1, 5, 9, 11, 2, 4, 8, 12, 7, 3],
  [11, 8, 6, 3, 1, 4, 9, 12, 10, 7, 5, 2],
  [12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1]]
gap> GroupByMultiplicationTable(last);
<group of size 12 with 12 generators>
gap> IsCyclic(last);
true

n=54
gap> ct:=CanonicalCayleyTable([[1,5,7,11,13,17,19,23,25],[5,25,19,1,11,23,13,7,17],
[7,19,5,23,17,11,25,1,13],[11,1,23,13,19,25,7,17,5],[13,11,17,19,7,5,23,25,1],
[17,23,11,25,5,19,1,13,7],[19,13,25,7,23,1,17,5,11],[23,7,1,17,25,13,5,11,19],
[25,17,13,5,1,7,11,19,23]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9], [2, 9, 7, 1, 4, 8, 5, 3, 6],
  [3, 7, 2, 8, 6, 4, 9, 1, 5], [4, 1, 8, 5, 7, 9, 3, 6, 2],
  [5, 4, 6, 7, 3, 2, 8, 9, 1], [6, 8, 4, 9, 2, 7, 1, 5, 3],
  [7, 5, 9, 3, 8, 1, 6, 2, 4], [8, 3, 1, 6, 9, 5, 2, 4, 7],
  [9, 6, 5, 2, 1, 3, 4, 7, 8]]
gap> GroupByMultiplicationTable(last);
<group of size 9 with 9 generators>
gap> IsCyclic(last);
true

n=56
gap> ct:=CanonicalCayleyTable([[1,3,5,9,11,13,15,17,19,23,25,27],
[3,9,15,27,23,17,11,5,1,13,19,25],[5,15,25,11,1,9,19,27,17,3,13,23],
[9,27,11,25,13,5,23,15,3,17,1,19],[11,23,1,13,9,25,3,19,15,27,5,17],
[13,17,9,5,25,1,27,3,23,19,11,15],[15,11,19,23,3,27,1,25,5,9,17,13],
[17,5,27,15,19,3,25,9,13,1,23,11],[19,1,17,3,15,23,5,13,25,11,27,9],
[23,13,3,17,27,19,9,1,11,25,15,5],[25,19,13,1,5,11,17,23,27,15,9,3],
[27,25,23,19,17,15,13,11,9,5,3,1]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12],
  [2, 4, 7, 12, 10, 8, 5, 3, 1, 6, 9, 11],
  [3, 7, 11, 5, 1, 4, 9, 12, 8, 2, 6, 10],
  [4, 12, 5, 11, 6, 3, 10, 7, 2, 8, 1, 9],
  [5, 10, 1, 6, 4, 11, 2, 9, 7, 12, 3, 8],
  [6, 8, 4, 3, 11, 1, 12, 2, 10, 9, 5, 7],
  [7, 5, 9, 10, 2, 12, 1, 11, 3, 4, 8, 6],
  [8, 3, 12, 7, 9, 2, 11, 4, 6, 1, 10, 5],
  [9, 1, 8, 2, 7, 10, 3, 6, 11, 5, 12, 4],
  [10, 6, 2, 8, 12, 9, 4, 1, 5, 11, 7, 3],
  [11, 9, 6, 1, 3, 5, 8, 10, 12, 7, 4, 2],
  [12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1]]
gap> GroupByMultiplicationTable(last);
<group of size 12 with 12 generators>
gap> IsCyclic(last);
false

n=58
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21,23,25,27],
[3,9,15,21,27,25,19,13,7,1,5,11,17,23],[5,15,25,23,13,3,7,17,27,21,11,1,9,19],
[7,21,23,9,5,19,25,11,3,17,27,13,1,15],[9,27,13,5,23,17,1,19,21,3,15,25,7,11],
[11,25,3,19,17,5,27,9,13,23,1,21,15,7],[13,19,7,25,1,27,5,21,11,15,17,9,23,3],
[15,13,17,11,19,9,21,7,23,5,25,3,27,1],[17,7,27,3,21,13,11,23,1,25,9,15,19,5],
[19,1,21,17,3,23,15,5,25,13,7,27,11,9],[21,5,11,27,15,1,17,25,9,7,23,19,3,13],
[23,11,1,13,25,21,9,3,15,27,19,7,5,17],[25,17,9,1,7,15,23,27,19,11,3,5,13,21],
[27,23,19,15,11,7,3,1,5,9,13,17,21,25]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14],
  [2, 5, 8, 11, 14, 13, 10, 7, 4, 1, 3, 6, 9, 12],
  [3, 8, 13, 12, 7, 2, 4, 9, 14, 11, 6, 1, 5, 10],
  [4, 11, 12, 5, 3, 10, 13, 6, 2, 9, 14, 7, 1, 8],
  [5, 14, 7, 3, 12, 9, 1, 10, 11, 2, 8, 13, 4, 6],
  [6, 13, 2, 10, 9, 3, 14, 5, 7, 12, 1, 11, 8, 4],
  [7, 10, 4, 13, 1, 14, 3, 11, 6, 8, 9, 5, 12, 2],
  [8, 7, 9, 6, 10, 5, 11, 4, 12, 3, 13, 2, 14, 1],
  [9, 4, 14, 2, 11, 7, 6, 12, 1, 13, 5, 8, 10, 3],
  [10, 1, 11, 9, 2, 12, 8, 3, 13, 7, 4, 14, 6, 5],
  [11, 3, 6, 14, 8, 1, 9, 13, 5, 4, 12, 10, 2, 7],
  [12, 6, 1, 7, 13, 11, 5, 2, 8, 14, 10, 4, 3, 9],
  [13, 9, 5, 1, 4, 8, 12, 14, 10, 6, 2, 3, 7, 11],
  [14, 12, 10, 8, 6, 4, 2, 1, 3, 5, 7, 9, 11, 13]]
gap> GroupByMultiplicationTable(last);
<group of size 14 with 14 generators>
gap> IsCyclic(last);
true

n=60
gap> ct:=CanonicalCayleyTable([[1,7,11,13,17,19,23,29],[7,11,17,29,1,13,19,23],
[11,17,1,23,7,29,13,19],[13,29,23,11,19,7,1,17],[17,1,7,19,11,23,29,13],[19,13,29,7,23,1,17,11],
[23,19,13,1,29,17,11,7],[29,23,19,17,13,11,7,1]]);
[[1, 2, 3, 4, 5, 6, 7, 8], [2, 3, 5, 8, 1, 4, 6, 7],
  [3, 5, 1, 7, 2, 8, 4, 6], [4, 8, 7, 3, 6, 2, 1, 5],
  [5, 1, 2, 6, 3, 7, 8, 4], [6, 4, 8, 2, 7, 1, 5, 3],
  [7, 6, 4, 1, 8, 5, 3, 2], [8, 7, 6, 5, 4, 3, 2, 1]]
gap> GroupByMultiplicationTable(last);
<group of size 8 with 8 generators>
gap> IsCyclic(last);
false

n=62
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21,23,25,27,29],
[3,9,15,21,27,29,23,17,11,5,1,7,13,19,25],[5,15,25,27,17,7,3,13,23,29,19,9,1,11,21],
[7,21,27,13,1,15,29,19,5,9,23,25,11,3,17],[9,27,17,1,19,25,7,11,29,15,3,21,23,5,13],
[11,29,7,15,25,3,19,21,1,23,17,5,27,13,9],[13,23,3,29,7,19,17,9,27,1,25,11,15,21,5],
[15,17,13,19,11,21,9,23,7,25,5,27,3,29,1],[17,11,23,5,29,1,27,7,21,13,15,19,9,25,3],
[19,5,29,9,15,23,1,25,13,11,27,3,21,17,7],[21,1,19,23,3,17,25,5,15,27,7,13,29,9,11],
[23,7,9,25,21,5,11,27,19,3,13,29,17,1,15],[25,13,1,11,23,27,15,3,9,21,29,17,5,7,19],
[27,19,11,3,5,13,21,29,25,17,9,1,7,15,23],[29,25,21,17,13,9,5,1,3,7,11,15,19,23,27]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15],
  [2, 5, 8, 11, 14, 15, 12, 9, 6, 3, 1, 4, 7, 10, 13],
  [3, 8, 13, 14, 9, 4, 2, 7, 12, 15, 10, 5, 1, 6, 11],
  [4, 11, 14, 7, 1, 8, 15, 10, 3, 5, 12, 13, 6, 2, 9],
  [5, 14, 9, 1, 10, 13, 4, 6, 15, 8, 2, 11, 12, 3, 7],
  [6, 15, 4, 8, 13, 2, 10, 11, 1, 12, 9, 3, 14, 7, 5],
  [7, 12, 2, 15, 4, 10, 9, 5, 14, 1, 13, 6, 8, 11, 3],
  [8, 9, 7, 10, 6, 11, 5, 12, 4, 13, 3, 14, 2, 15, 1],
  [9, 6, 12, 3, 15, 1, 14, 4, 11, 7, 8, 10, 5, 13, 2],
  [10, 3, 15, 5, 8, 12, 1, 13, 7, 6, 14, 2, 11, 9, 4],
  [11, 1, 10, 12, 2, 9, 13, 3, 8, 14, 4, 7, 15, 5, 6],
  [12, 4, 5, 13, 11, 3, 6, 14, 10, 2, 7, 15, 9, 1, 8],
  [13, 7, 1, 6, 12, 14, 8, 2, 5, 11, 15, 9, 3, 4, 10],
  [14, 10, 6, 2, 3, 7, 11, 15, 13, 9, 5, 1, 4, 8, 12],
  [15, 13, 11, 9, 7, 5, 3, 1, 2, 4, 6, 8, 10, 12, 14]]
gap> GroupByMultiplicationTable(last);
<group of size 15 with 15 generators>
gap> IsCyclic(last);
true

n=64
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31],
[3,9,15,21,27,31,25,19,13,7,1,5,11,17,23,29],[5,15,25,29,19,9,1,11,21,31,23,13,3,7,17,27],
[7,21,29,15,1,13,27,23,9,5,19,31,17,3,11,25],[9,27,19,1,17,29,11,7,25,21,3,15,31,13,5,23],
[11,31,9,13,29,7,15,27,5,17,25,3,19,23,1,21],[13,25,1,27,11,15,23,3,29,9,17,21,5,31,7,19],
[15,19,11,23,7,27,3,31,1,29,5,25,9,21,13,17],[17,13,21,9,25,5,29,1,31,3,27,7,23,11,19,15],
[19,7,31,5,21,17,9,29,3,23,15,11,27,1,25,13],[21,1,23,19,3,25,17,5,27,15,7,29,13,9,31,11],
[23,5,13,31,15,3,21,25,7,11,29,17,1,19,27,9],[25,11,3,17,31,19,5,9,23,27,13,1,15,29,21,7],
[27,17,7,3,13,23,31,21,11,1,9,19,29,25,15,5],[29,23,17,11,5,1,7,13,19,25,31,27,21,15,9,3],

```
[31,29,27,25,23,21,19,17,15,13,11,9,7,5,3,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 ],
  [ 2, 5, 8, 11, 14, 16, 13, 10, 7, 4, 1, 3, 6, 9, 12, 15 ],
  [ 3, 8, 13, 15, 10, 5, 1, 6, 11, 16, 12, 7, 2, 4, 9, 14 ],
  [ 4, 11, 15, 8, 1, 7, 14, 12, 5, 3, 10, 16, 9, 2, 6, 13 ],
  [ 5, 14, 10, 1, 9, 15, 6, 4, 13, 11, 2, 8, 16, 7, 3, 12 ],
  [ 6, 16, 5, 7, 15, 4, 8, 14, 3, 9, 13, 2, 10, 12, 1, 11 ],
  [ 7, 13, 1, 14, 6, 8, 12, 2, 15, 5, 9, 11, 3, 16, 4, 10 ],
  [ 8, 10, 6, 12, 4, 14, 2, 16, 1, 15, 3, 13, 5, 11, 7, 9 ],
  [ 9, 7, 11, 5, 13, 3, 15, 1, 16, 2, 14, 4, 12, 6, 10, 8 ],
  [ 10, 4, 16, 3, 11, 9, 5, 15, 2, 12, 8, 6, 14, 1, 13, 7 ],
  [ 11, 1, 12, 10, 2, 13, 9, 3, 14, 8, 4, 15, 7, 5, 16, 6 ],
  [ 12, 3, 7, 16, 8, 2, 11, 13, 4, 6, 15, 9, 1, 10, 14, 5 ],
  [ 13, 6, 2, 9, 16, 10, 3, 5, 12, 14, 7, 1, 8, 15, 11, 4 ],
  [ 14, 9, 4, 2, 7, 12, 16, 11, 6, 1, 5, 10, 15, 13, 8, 3 ],
  [ 15, 12, 9, 6, 3, 1, 4, 7, 10, 13, 16, 14, 11, 8, 5, 2 ],
  [ 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 16 with 16 generators>
gap> IsCyclic(last);
true

n=66
gap> ct:=CanonicalCayleyTable([[1,5,7,13,17,19,23,25,29,31],[5,25,31,1,19,29,17,7,13,23],
[7,31,17,25,13,1,29,23,5,19],[13,1,25,29,23,17,31,5,19,7],[17,19,13,23,25,7,5,29,31,1],
[19,29,1,17,7,31,25,13,23,5],[23,17,29,31,5,25,1,19,7,13],[25,7,23,5,29,13,19,31,1,17],
[29,13,5,19,31,23,7,1,17,25],[31,23,19,7,1,5,13,17,25,29]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 ], [ 2, 8, 10, 1, 6, 9, 5, 3, 4, 7 ],
  [ 3, 10, 5, 8, 4, 1, 9, 7, 2, 6 ], [ 4, 1, 8, 9, 7, 5, 10, 2, 6, 3 ],
  [ 5, 6, 4, 7, 8, 3, 2, 9, 10, 1 ], [ 6, 9, 1, 5, 3, 10, 8, 4, 7, 2 ],
  [ 7, 5, 9, 10, 2, 8, 1, 6, 3, 4 ], [ 8, 3, 7, 2, 9, 4, 6, 10, 1, 5 ],
  [ 9, 4, 2, 6, 10, 7, 3, 1, 5, 8 ], [ 10, 7, 6, 3, 1, 2, 4, 5, 8, 9 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 10 with 10 generators>
gap> IsCyclic(last);
true

n=68
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,19,21,23,25,27,29,31,33],
[3,9,15,21,27,33,29,23,11,5,1,7,13,19,25,31],[5,15,25,33,23,13,3,7,27,31,21,11,1,9,19,29],
[7,21,33,19,5,9,23,31,3,11,25,29,15,1,13,27],[9,27,23,5,13,31,19,1,33,15,3,21,29,11,7,25],
[11,33,13,9,31,15,7,29,5,27,19,3,25,21,1,23],[13,29,3,23,19,7,33,9,25,1,27,15,11,31,5,21],
[15,23,7,31,1,29,9,21,13,25,5,33,3,27,11,19],[19,11,27,3,33,5,25,13,21,9,29,1,31,7,23,15],
[21,5,31,11,15,27,1,25,9,33,7,19,23,3,29,13],[23,1,21,25,3,19,27,5,29,7,15,31,9,13,33,11],
[25,7,11,29,21,3,15,33,1,19,31,13,5,23,27,9],[27,13,1,15,29,25,11,3,31,23,9,5,19,33,21,7],
[29,19,9,1,11,21,31,27,7,3,13,23,33,25,15,5],[31,25,19,13,7,1,5,11,23,29,33,27,21,15,9,3],
[33,31,29,27,25,23,21,19,15,13,11,9,7,5,3,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 ],
  [ 2, 5, 8, 10, 13, 16, 14, 11, 6, 3, 1, 4, 7, 9, 12, 15 ],
  [ 3, 8, 12, 16, 11, 7, 2, 4, 13, 15, 10, 6, 1, 5, 9, 14 ],
  [ 4, 10, 16, 9, 3, 5, 11, 15, 2, 6, 12, 14, 8, 1, 7, 13 ],
  [ 5, 13, 11, 3, 7, 15, 9, 1, 16, 8, 2, 10, 14, 6, 4, 12 ],
```

```
  [ 6, 16, 7, 5, 15, 8, 4, 14, 3, 13, 9, 2, 12, 10, 1, 11 ],
  [ 7, 14, 2, 11, 9, 4, 16, 5, 12, 1, 13, 8, 6, 15, 3, 10 ],
  [ 8, 11, 4, 15, 1, 14, 5, 10, 7, 12, 3, 16, 2, 13, 6, 9 ],
  [ 9, 6, 13, 2, 16, 3, 12, 7, 10, 5, 14, 1, 15, 4, 11, 8 ],
  [ 10, 3, 15, 6, 8, 13, 1, 12, 5, 16, 4, 9, 11, 2, 14, 7 ],
  [ 11, 1, 10, 12, 2, 9, 13, 3, 14, 4, 8, 15, 5, 7, 16, 6 ],
  [ 12, 4, 6, 14, 10, 2, 8, 16, 1, 9, 15, 7, 3, 11, 13, 5 ],
  [ 13, 7, 1, 8, 14, 12, 6, 2, 15, 11, 5, 3, 9, 16, 10, 4 ],
  [ 14, 9, 5, 1, 6, 10, 15, 13, 4, 2, 7, 11, 16, 12, 8, 3 ],
  [ 15, 12, 9, 7, 4, 1, 3, 6, 11, 14, 16, 13, 10, 8, 5, 2 ],
  [ 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 16 with 16 generators>
gap> IsCyclic(last);
true

n=70
gap> ct:=CanonicalCayleyTable([[1,3,9,11,13,17,19,23,27,29,31,33],
[3,9,27,33,31,19,13,1,11,17,23,29],[9,27,11,29,23,13,31,3,33,19,1,17],
[11,33,29,19,3,23,1,27,17,31,9,13],[13,31,23,3,29,11,33,19,1,27,17,9],
[17,19,13,23,11,9,27,29,31,3,33,1],[19,13,31,1,33,27,11,17,23,9,29,3],
[23,1,3,27,19,29,17,31,9,33,13,11],[27,11,33,17,1,31,23,9,29,13,3,19],
[29,17,19,31,27,3,9,33,13,1,11,23],[31,23,1,9,17,33,29,13,3,11,19,27],
[33,29,17,13,9,1,3,11,19,23,27,31]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ],
  [ 2, 3, 9, 12, 11, 7, 5, 1, 4, 6, 8, 10 ],
  [ 3, 9, 4, 10, 8, 5, 11, 2, 12, 7, 1, 6 ],
  [ 4, 12, 10, 7, 2, 8, 1, 9, 6, 11, 3, 5 ],
  [ 5, 11, 8, 2, 10, 4, 12, 7, 1, 9, 6, 3 ],
  [ 6, 7, 5, 8, 4, 3, 9, 10, 11, 2, 12, 1 ],
  [ 7, 5, 11, 1, 12, 9, 4, 6, 8, 3, 10, 2 ],
  [ 8, 1, 2, 9, 7, 10, 6, 11, 3, 12, 5, 4 ],
  [ 9, 4, 12, 6, 1, 11, 8, 3, 10, 5, 2, 7 ],
  [ 10, 6, 7, 11, 9, 2, 3, 12, 5, 1, 4, 8 ],
  [ 11, 8, 1, 3, 6, 12, 10, 5, 2, 4, 7, 9 ],
  [ 12, 10, 6, 5, 3, 1, 2, 4, 7, 8, 9, 11 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 12 with 12 generators>
gap> IsCyclic(last);
true

n=72
gap> ct:=CanonicalCayleyTable([[1,5,7,11,13,17,19,23,25,29,31,35],
[5,25,35,17,7,13,23,29,19,1,11,31],[7,35,23,5,19,25,11,17,31,13,1,29],
[11,17,5,23,1,29,7,35,13,31,19,25],[13,7,19,1,25,5,31,11,35,17,29,23],
[17,13,25,29,5,1,35,31,7,11,23,19],[19,23,11,7,31,35,1,5,29,25,13,17],
[23,29,17,35,11,31,5,25,1,19,7,13],[25,19,31,13,35,7,29,1,23,5,17,11],
[29,1,13,31,17,11,25,19,5,23,35,7],[31,11,1,19,29,23,13,7,17,35,25,5],
[35,31,29,25,23,19,17,13,11,7,5,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ],
  [ 2, 9, 12, 6, 3, 5, 8, 10, 7, 1, 4, 11 ],
  [ 3, 12, 8, 2, 7, 9, 4, 6, 11, 5, 1, 10 ],
```

```
  [ 4, 6, 2, 8, 1, 10, 3, 12, 5, 11, 7, 9 ],
  [ 5, 3, 7, 1, 9, 2, 11, 4, 12, 6, 10, 8 ],
  [ 6, 5, 9, 10, 2, 1, 12, 11, 3, 4, 8, 7 ],
  [ 7, 8, 4, 3, 11, 12, 1, 2, 10, 9, 5, 6 ],
  [ 8, 10, 6, 12, 4, 11, 2, 9, 1, 7, 3, 5 ],
  [ 9, 7, 11, 5, 12, 3, 10, 1, 8, 2, 6, 4 ],
  [ 10, 1, 5, 11, 6, 4, 9, 7, 2, 8, 12, 3 ],
  [ 11, 4, 1, 7, 10, 8, 5, 3, 6, 12, 9, 2 ],
  [ 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 12 with 12 generators>
gap> IsCyclic(last);
false

n=74
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35],
[3,9,15,21,27,33,35,29,23,17,11,5,1,7,13,19,25,31],
[5,15,25,35,29,19,9,1,11,21,31,33,23,13,3,7,17,27],
[7,21,35,25,11,3,17,31,29,15,1,13,27,33,19,5,9,23],
[9,27,29,11,7,25,31,13,5,23,33,15,3,21,35,17,1,19],
[11,33,19,3,25,27,5,17,35,13,9,31,21,1,23,29,7,15],
[13,35,9,17,31,5,21,27,1,25,23,3,29,19,7,33,15,11],
[15,29,1,31,13,17,27,3,33,11,19,25,5,35,9,21,23,7],
[17,23,11,29,5,35,1,33,7,27,13,21,19,15,25,9,31,3],
[19,17,21,15,23,13,25,11,27,9,29,7,31,5,33,3,35,1],
[21,11,31,1,33,9,23,19,13,29,3,35,7,25,17,15,27,5],
[23,5,33,13,15,31,3,25,21,7,35,11,17,29,1,27,19,9],
[25,1,23,27,3,21,29,5,19,31,7,17,33,9,15,35,11,13],
[27,7,13,33,21,1,19,35,15,5,25,29,9,11,31,23,3,17],
[29,13,3,19,35,23,7,9,25,33,17,1,15,31,27,11,5,21],
[31,19,7,5,17,29,33,21,9,3,15,27,35,23,11,1,13,25],
[33,25,17,9,1,7,15,23,31,35,27,19,11,3,5,13,21,29],
[35,31,27,23,19,15,11,7,3,1,5,9,13,17,21,25,29,33]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18 ],
  [ 2, 5, 8, 11, 14, 17, 18, 15, 12, 9, 6, 3, 1, 4, 7, 10, 13, 16 ],
  [ 3, 8, 13, 18, 15, 10, 5, 1, 6, 11, 16, 17, 12, 7, 2, 4, 9, 14 ],
  [ 4, 11, 18, 13, 6, 2, 9, 16, 15, 8, 1, 7, 14, 17, 10, 3, 5, 12 ],
  [ 5, 14, 15, 6, 4, 13, 16, 7, 3, 12, 17, 8, 2, 11, 18, 9, 1, 10 ],
  [ 6, 17, 10, 2, 13, 14, 3, 9, 18, 7, 5, 16, 11, 1, 12, 15, 4, 8 ],
  [ 7, 18, 5, 9, 16, 3, 11, 14, 1, 13, 12, 2, 15, 10, 4, 17, 8, 6 ],
  [ 8, 15, 1, 16, 7, 9, 14, 2, 17, 6, 10, 13, 3, 18, 5, 11, 12, 4 ],
  [ 9, 12, 6, 15, 3, 18, 1, 17, 4, 14, 7, 11, 10, 8, 13, 5, 16, 2 ],
  [ 10, 9, 11, 8, 12, 7, 13, 6, 14, 5, 15, 4, 16, 3, 17, 2, 18, 1 ],
  [ 11, 6, 16, 1, 17, 5, 12, 10, 7, 15, 2, 18, 4, 13, 9, 8, 14, 3 ],
  [ 12, 3, 17, 7, 8, 16, 2, 13, 11, 4, 18, 6, 9, 15, 1, 14, 10, 5 ],
  [ 13, 1, 12, 14, 2, 11, 15, 3, 10, 16, 4, 9, 17, 5, 8, 18, 6, 7 ],
  [ 14, 4, 7, 17, 11, 1, 10, 18, 8, 3, 13, 15, 5, 6, 16, 12, 2, 9 ],
  [ 15, 7, 2, 10, 18, 12, 4, 5, 13, 17, 9, 1, 8, 16, 14, 6, 3, 11 ],
  [ 16, 10, 4, 3, 9, 15, 17, 11, 5, 2, 8, 14, 18, 12, 6, 1, 7, 13 ],
  [ 17, 13, 9, 5, 1, 4, 8, 12, 16, 18, 14, 10, 6, 2, 3, 7, 11, 15 ],
  [ 18, 16, 14, 12, 10, 8, 6, 4, 2, 1, 3, 5, 7, 9, 11, 13, 15, 17 ] ]
gap> GroupByMultiplicationTable(last);
```

<group of size 18 with 18 generators>
gap> IsCyclic(last);
true

n=76
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,21,23,25,27,29,31,33,35,37],
[3,9,15,21,27,33,37,31,25,13,7,1,5,11,17,23,29,35],
[5,15,25,35,31,21,11,1,9,29,37,27,17,7,3,13,23,33],
[7,21,35,27,13,1,15,29,33,5,9,23,37,25,11,3,17,31],
[9,27,31,13,5,23,35,17,1,37,21,3,15,33,25,7,11,29],
[11,33,21,1,23,31,9,13,35,3,25,29,7,15,37,17,5,27],
[13,37,11,15,35,9,17,33,7,31,5,21,29,3,23,27,1,25],
[15,31,1,29,17,13,33,3,27,11,35,5,25,21,9,37,7,23],
[17,25,9,33,1,35,7,27,15,23,11,31,3,37,5,29,13,21],
[21,13,29,5,37,3,31,11,23,15,27,7,35,1,33,9,25,17],
[23,7,37,9,21,25,5,35,11,27,3,33,13,17,29,1,31,15],
[25,1,27,23,3,29,21,5,31,7,33,17,9,35,15,11,37,13],
[27,5,17,37,15,7,29,25,3,35,13,9,31,23,1,21,33,11],
[29,11,7,25,33,15,3,21,37,1,17,35,23,5,13,31,27,9],
[31,17,3,11,25,37,23,9,5,33,29,15,1,13,27,35,21,7],
[33,23,13,3,7,17,27,37,29,9,1,11,21,31,35,25,15,5],
[35,29,23,17,11,5,1,7,13,25,31,37,33,27,21,15,9,3],
[37,35,33,31,29,27,25,23,21,17,15,13,11,9,7,5,3,1]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18],
  [2, 5, 8, 10, 13, 16, 18, 15, 12, 7, 4, 1, 3, 6, 9, 11, 14, 17],
  [3, 8, 12, 17, 15, 10, 6, 1, 5, 14, 18, 13, 9, 4, 2, 7, 11, 16],
  [4, 10, 17, 13, 7, 1, 8, 14, 16, 3, 5, 11, 18, 12, 6, 2, 9, 15],
  [5, 13, 15, 7, 3, 11, 17, 9, 1, 18, 10, 2, 8, 16, 12, 4, 6, 14],
  [6, 16, 10, 1, 11, 15, 5, 7, 17, 2, 12, 14, 4, 8, 18, 9, 3, 13],
  [7, 18, 6, 8, 17, 5, 9, 16, 4, 15, 3, 10, 14, 2, 11, 13, 1, 12],
  [8, 15, 1, 14, 9, 7, 16, 2, 13, 6, 17, 3, 12, 10, 5, 18, 4, 11],
  [9, 12, 5, 16, 1, 17, 4, 13, 8, 11, 6, 15, 2, 18, 3, 14, 7, 10],
  [10, 7, 14, 3, 18, 2, 15, 6, 11, 8, 13, 4, 17, 1, 16, 5, 12, 9],
  [11, 4, 18, 5, 10, 12, 3, 17, 6, 13, 2, 16, 7, 9, 14, 1, 15, 8],
  [12, 1, 13, 11, 2, 14, 10, 3, 15, 4, 16, 9, 5, 17, 8, 6, 18, 7],
  [13, 3, 9, 18, 8, 4, 14, 12, 2, 17, 7, 5, 15, 11, 1, 10, 16, 6],
  [14, 6, 4, 12, 16, 8, 2, 10, 18, 1, 9, 17, 11, 3, 7, 15, 13, 5],
  [15, 9, 2, 6, 12, 18, 11, 5, 3, 16, 14, 8, 1, 7, 13, 17, 10, 4],
  [16, 11, 7, 2, 4, 9, 13, 18, 14, 5, 1, 6, 10, 15, 17, 12, 8, 3],
  [17, 14, 11, 9, 6, 3, 1, 4, 7, 12, 15, 18, 16, 13, 10, 8, 5, 2],
  [18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1]]
gap> GroupByMultiplicationTable(last);
<group of size 18 with 18 generators>
gap> IsCyclic(last);
true

n=78
gap> ct:=CanonicalCayleyTable([[1,5,7,11,17,19,23,25,29,31,35,37],
[5,25,35,23,7,17,37,31,11,1,19,29],[7,35,29,1,37,23,5,19,31,17,11,25],
[11,23,1,35,31,25,19,37,7,29,5,17],[17,7,37,31,23,11,1,35,25,19,29,5],
[19,17,23,25,11,29,31,7,5,35,37,1],[23,37,5,19,1,31,17,29,35,11,25,7],

[25,31,19,37,35,7,29,1,23,5,17,11],[29,11,31,7,25,5,35,23,17,37,1,19],
[31,1,17,29,19,35,11,5,37,25,7,23],[35,19,11,5,29,37,25,17,1,7,23,31],
[37,29,25,17,5,1,7,11,19,23,31,35]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12],
  [2, 8, 11, 7, 3, 5, 12, 10, 4, 1, 6, 9],
  [3, 11, 9, 1, 12, 7, 2, 6, 10, 5, 4, 8],
  [4, 7, 1, 11, 10, 8, 6, 12, 3, 9, 2, 5],
  [5, 3, 12, 10, 7, 4, 1, 11, 8, 6, 9, 2],
  [6, 5, 7, 8, 4, 9, 10, 3, 2, 11, 12, 1],
  [7, 12, 2, 6, 1, 10, 5, 9, 11, 4, 8, 3],
  [8, 10, 6, 12, 11, 3, 9, 1, 7, 2, 5, 4],
  [9, 4, 10, 3, 8, 2, 11, 7, 5, 12, 1, 6],
  [10, 1, 5, 9, 6, 11, 4, 2, 12, 8, 3, 7],
  [11, 6, 4, 2, 9, 12, 8, 5, 1, 3, 7, 10],
  [12, 9, 8, 5, 2, 1, 3, 4, 6, 7, 10, 11]]
gap> GroupByMultiplicationTable(last);
<group of size 12 with 12 generators>
gap> IsCyclic(last);
true

n=80
gap> ct:=CanonicalCayleyTable([[1,3,7,9,11,13,17,19,21,23,27,29,31,33,37,39],
[3,9,21,27,33,39,29,23,17,11,1,7,13,19,31,37],[7,21,31,17,3,11,39,27,13,1,29,37,23,9,19,33],
[9,27,17,1,19,37,7,11,29,33,3,21,39,23,13,31],[11,33,3,19,39,17,27,31,9,13,23,1,21,37,7,29],
[13,39,11,37,17,9,19,7,33,21,31,23,3,29,1,27],[17,29,39,7,27,19,31,3,37,9,21,13,33,1,11,23],
[19,23,27,11,31,7,3,39,1,37,33,9,29,13,17,21],[21,17,13,29,9,33,37,1,39,3,7,31,11,27,23,19],
[23,11,1,33,13,21,9,37,3,31,19,27,7,39,29,17],[27,1,29,3,23,31,21,33,7,19,9,17,37,11,39,13],
[29,7,37,21,1,23,13,9,31,27,17,39,19,3,33,11],[31,13,23,39,21,3,33,29,11,7,37,19,1,17,27,9],
[33,19,9,23,37,29,1,13,27,39,11,3,17,31,21,7],[37,31,19,13,7,1,11,17,23,29,39,33,27,21,9,3],
[39,37,33,31,29,27,23,21,19,17,13,11,9,7,3,1]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16],
  [2, 4, 9, 11, 14, 16, 12, 10, 7, 5, 1, 3, 6, 8, 13, 15],
  [3, 9, 13, 7, 2, 5, 16, 11, 6, 1, 12, 15, 10, 4, 8, 14],
  [4, 11, 7, 1, 8, 15, 3, 5, 12, 14, 2, 9, 16, 10, 6, 13],
  [5, 14, 2, 8, 16, 7, 11, 13, 4, 6, 10, 1, 9, 15, 3, 12],
  [6, 16, 5, 15, 7, 4, 8, 3, 14, 9, 13, 10, 2, 12, 1, 11],
  [7, 12, 16, 3, 11, 8, 13, 2, 15, 4, 9, 6, 14, 1, 5, 10],
  [8, 10, 11, 5, 13, 3, 2, 16, 1, 15, 14, 4, 12, 6, 7, 9],
  [9, 7, 6, 12, 4, 14, 15, 1, 16, 2, 3, 13, 5, 11, 10, 8],
  [10, 5, 1, 14, 6, 9, 4, 15, 2, 13, 8, 11, 3, 16, 12, 7],
  [11, 1, 12, 2, 10, 13, 9, 14, 3, 8, 4, 7, 15, 5, 16, 6],
  [12, 3, 15, 9, 1, 10, 6, 4, 13, 11, 7, 16, 8, 2, 14, 5],
  [13, 6, 10, 16, 9, 2, 14, 12, 5, 3, 15, 8, 1, 7, 11, 4],
  [14, 8, 4, 10, 15, 12, 1, 6, 11, 16, 5, 2, 7, 13, 9, 3],
  [15, 13, 8, 6, 3, 1, 5, 7, 10, 12, 16, 14, 11, 9, 4, 2],
  [16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1]]
gap> GroupByMultiplicationTable(last);
<group of size 16 with 16 generators>
gap> IsCyclic(last);
false

n=82

```
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39],
[3,9,15,21,27,33,39,37,31,25,19,13,7,1,5,11,17,23,29,35],
[5,15,25,35,37,27,17,7,3,13,23,33,39,29,19,9,1,11,21,31],
[7,21,35,33,19,5,9,23,37,31,17,3,11,25,39,29,15,1,13,27],
[9,27,37,19,1,17,35,29,11,7,25,39,21,3,15,33,31,13,5,23],
[11,33,27,5,17,39,21,1,23,37,15,7,29,31,9,13,35,25,3,19],
[13,39,17,9,35,21,5,31,25,1,27,29,3,23,33,7,19,37,11,15],
[15,37,7,23,29,1,31,21,9,39,13,17,35,5,25,27,3,33,19,11],
[17,31,3,37,11,23,25,9,39,5,29,19,15,33,1,35,13,21,27,7],
[19,25,13,31,7,37,1,39,5,33,11,27,17,21,23,15,29,9,35,3],
[21,19,23,17,25,15,27,13,29,11,31,9,33,7,35,5,37,3,39,1],
[23,13,33,3,39,7,29,17,19,27,9,37,1,35,11,25,21,15,31,5],
[25,7,39,11,21,29,3,35,15,17,33,1,31,19,13,37,5,27,23,9],
[27,1,29,25,3,31,23,5,33,21,7,35,19,9,37,17,11,39,15,13],
[29,5,19,39,15,9,33,25,1,23,35,11,13,37,21,3,27,31,7,17],
[31,11,9,29,33,13,7,27,35,15,5,25,37,17,3,23,39,19,1,21],
[33,17,1,15,31,35,19,3,13,29,37,21,5,11,27,39,23,7,9,25],
[35,23,11,1,13,25,37,33,21,9,3,15,27,39,31,19,7,5,17,29],
[37,29,21,13,5,3,11,19,27,35,39,31,23,15,7,1,9,17,25,33],
[39,35,31,27,23,19,15,11,7,3,1,5,9,13,17,21,25,29,33,37]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 ],
  [ 2, 5, 8, 11, 14, 17, 20, 19, 16, 13, 10, 7, 4, 1, 3, 6, 9, 12, 15, 18 ],
  [ 3, 8, 13, 18, 19, 14, 9, 4, 2, 7, 12, 17, 20, 15, 10, 5, 1, 6, 11, 16 ],
  [ 4, 11, 18, 17, 10, 3, 5, 12, 19, 16, 9, 2, 6, 13, 20, 15, 8, 1, 7, 14 ],
  [ 5, 14, 19, 10, 1, 9, 18, 15, 6, 4, 13, 20, 11, 2, 8, 17, 16, 7, 3, 12 ],
  [ 6, 17, 14, 3, 9, 20, 11, 1, 12, 19, 8, 4, 15, 16, 5, 7, 18, 13, 2, 10 ],
  [ 7, 20, 9, 5, 18, 11, 3, 16, 13, 1, 14, 15, 2, 12, 17, 4, 10, 19, 6, 8 ],
  [ 8, 19, 4, 12, 15, 1, 16, 11, 5, 20, 7, 9, 18, 3, 13, 14, 2, 17, 10, 6 ],
  [ 9, 16, 2, 19, 6, 12, 13, 5, 20, 3, 15, 10, 8, 17, 1, 18, 7, 11, 14, 4 ],
  [ 10, 13, 7, 16, 4, 19, 1, 20, 3, 17, 6, 14, 9, 11, 12, 8, 15, 5, 18, 2 ],
  [ 11, 10, 12, 9, 13, 8, 14, 7, 15, 6, 16, 5, 17, 4, 18, 3, 19, 2, 20, 1 ],
  [ 12, 7, 17, 2, 20, 4, 15, 9, 10, 14, 5, 19, 1, 18, 6, 13, 11, 8, 16, 3 ],
  [ 13, 4, 20, 6, 11, 15, 2, 18, 8, 9, 17, 1, 16, 10, 7, 19, 3, 14, 12, 5 ],
  [ 14, 1, 15, 13, 2, 16, 12, 3, 17, 11, 4, 18, 10, 5, 19, 9, 6, 20, 8, 7 ],
  [ 15, 3, 10, 20, 8, 5, 17, 13, 1, 12, 18, 6, 7, 19, 11, 2, 14, 16, 4, 9 ],
  [ 16, 6, 5, 15, 17, 7, 4, 14, 18, 8, 3, 13, 19, 9, 2, 12, 20, 10, 1, 11 ],
  [ 17, 9, 1, 8, 16, 18, 10, 2, 7, 15, 19, 11, 3, 6, 14, 20, 12, 4, 5, 13 ],
  [ 18, 12, 6, 1, 7, 13, 19, 17, 11, 5, 2, 8, 14, 20, 16, 10, 4, 3, 9, 15 ],
  [ 19, 15, 11, 7, 3, 2, 6, 10, 14, 18, 20, 16, 12, 8, 4, 1, 5, 9, 13, 17 ],
  [ 20, 18, 16, 14, 12, 10, 8, 6, 4, 2, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 20 with 20 generators>
gap> IsCyclic(last);
true

n=84
gap> ct:=CanonicalCayleyTable([[1,5,11,13,17,19,23,25,29,31,37,41],
[5,25,29,19,1,11,31,41,23,13,17,37],[11,29,37,25,19,41,1,23,17,5,13,31],
[13,19,25,1,31,5,37,11,41,17,23,29],[17,1,19,31,37,13,29,5,11,23,41,25],
[19,11,41,5,13,25,17,29,37,1,31,23],[23,31,1,37,29,17,25,13,5,41,11,19],
[25,41,23,11,5,29,13,37,31,19,1,17],[29,23,17,41,11,37,5,31,1,25,19,13],
[31,13,5,17,23,1,41,19,25,37,29,11],[37,17,13,23,41,31,11,1,19,29,25,5],
```

```
[41,37,31,29,25,23,19,17,13,11,5,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ],
  [ 2, 8, 9, 6, 1, 3, 10, 12, 7, 4, 5, 11 ],
  [ 3, 9, 11, 8, 6, 12, 1, 7, 5, 2, 4, 10 ],
  [ 4, 6, 8, 1, 10, 2, 11, 3, 12, 5, 7, 9 ],
  [ 5, 1, 6, 10, 11, 4, 9, 2, 3, 7, 12, 8 ],
  [ 6, 3, 12, 2, 4, 8, 5, 9, 11, 1, 10, 7 ],
  [ 7, 10, 1, 11, 9, 5, 8, 4, 2, 12, 3, 6 ],
  [ 8, 12, 7, 3, 2, 9, 4, 11, 10, 6, 1, 5 ],
  [ 9, 7, 5, 12, 3, 11, 2, 10, 1, 8, 6, 4 ],
  [ 10, 4, 2, 5, 7, 1, 12, 6, 8, 11, 9, 3 ],
  [ 11, 5, 4, 7, 12, 10, 3, 1, 6, 9, 8, 2 ],
  [ 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 12 with 12 generators>
gap> IsCyclic(last);
false

n=86
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41],
[3,9,15,21,27,33,39,41,35,29,23,17,11,5,1,7,13,19,25,31,37],
[5,15,25,35,41,31,21,11,1,9,19,29,39,37,27,17,7,3,13,23,33],
[7,21,35,37,23,9,5,19,33,39,25,11,3,17,31,41,27,13,1,15,29],
[9,27,41,23,5,13,31,37,19,1,17,35,33,15,3,21,39,29,11,7,25],
[11,33,31,9,13,35,29,7,15,37,27,5,17,39,25,3,19,41,23,1,21],
[13,39,21,5,31,29,3,23,37,11,15,41,19,7,33,27,1,25,35,9,17],
[15,41,11,19,37,7,23,33,3,27,29,1,31,25,5,35,21,9,39,17,13],
[17,35,1,33,19,15,37,3,31,21,13,39,5,29,23,11,41,7,27,25,9],
[19,29,9,39,1,37,11,27,21,17,31,7,41,3,35,13,25,23,15,33,5],
[21,23,19,25,17,27,15,29,13,31,11,33,9,35,7,37,5,39,3,41,1],
[23,17,29,11,35,5,41,1,39,7,33,13,27,19,21,25,15,31,9,37,3],
[25,11,39,3,33,17,19,31,5,41,9,27,23,13,37,1,35,15,21,29,7],
[27,5,37,17,15,39,7,25,29,3,35,19,13,41,9,23,31,1,33,21,11],
[29,1,27,31,3,25,33,5,23,35,7,21,37,9,19,39,11,17,41,13,15],
[31,7,17,41,21,3,27,35,11,13,37,25,1,23,39,15,9,33,29,5,19],
[33,13,7,27,39,19,1,21,41,25,5,15,35,31,11,9,29,37,17,3,23],
[35,19,3,13,29,41,25,9,7,23,39,31,15,1,17,33,37,21,5,11,27],
[37,25,13,1,11,23,35,39,27,15,3,9,21,33,41,29,17,5,7,19,31],
[39,31,23,15,7,1,9,17,25,33,41,37,29,21,13,5,3,11,19,27,35],
[41,37,33,29,25,21,17,13,9,5,1,3,7,11,15,19,23,27,31,35,39]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21 ],
  [ 2, 5, 8, 11, 14, 17, 20, 21, 18, 15, 12, 9, 6, 3, 1, 4, 7, 10, 13, 16, 19 ],
  [ 3, 8, 13, 18, 21, 16, 11, 6, 1, 5, 10, 15, 20, 19, 14, 9, 4, 2, 7, 12, 17 ],
  [ 4, 11, 18, 19, 12, 5, 3, 10, 17, 20, 13, 6, 2, 9, 16, 21, 14, 7, 1, 8, 15 ],
  [ 5, 14, 21, 12, 3, 7, 16, 19, 10, 1, 9, 18, 17, 8, 2, 11, 20, 15, 6, 4, 13 ],
  [ 6, 17, 16, 5, 7, 18, 15, 4, 8, 19, 14, 3, 9, 20, 13, 2, 10, 21, 12, 1, 11 ],
  [ 7, 20, 11, 3, 16, 15, 2, 12, 19, 6, 8, 21, 10, 4, 17, 14, 1, 13, 18, 5, 9 ],
  [ 8, 21, 6, 10, 19, 4, 12, 17, 2, 14, 15, 1, 16, 13, 3, 18, 11, 5, 20, 9, 7 ],
  [ 9, 18, 1, 17, 10, 8, 19, 2, 16, 11, 7, 20, 3, 15, 12, 6, 21, 4, 14, 13, 5 ],
  [ 10, 15, 5, 20, 1, 19, 6, 14, 11, 9, 16, 4, 21, 2, 18, 7, 13, 12, 8, 17, 3 ],
  [ 11, 12, 10, 13, 9, 14, 8, 15, 7, 16, 6, 17, 5, 18, 4, 19, 3, 20, 2, 21, 1 ],
  [ 12, 9, 15, 6, 18, 3, 21, 1, 20, 4, 17, 7, 14, 10, 11, 13, 8, 16, 5, 19, 2 ],
```

```
  [ 13, 6, 20, 2, 17, 9, 10, 16, 3, 21, 5, 14, 12, 7, 19, 1, 18, 8, 11, 15, 4 ],
  [ 14, 3, 19, 9, 8, 20, 4, 13, 15, 2, 18, 10, 7, 21, 5, 12, 16, 1, 17, 11, 6 ],
  [ 15, 1, 14, 16, 2, 13, 17, 3, 12, 18, 4, 11, 19, 5, 10, 20, 6, 9, 21, 7, 8 ],
  [ 16, 4, 9, 21, 11, 2, 14, 18, 6, 7, 19, 13, 1, 12, 20, 8, 5, 17, 15, 3, 10 ],
  [ 17, 7, 4, 14, 20, 10, 1, 11, 21, 13, 3, 8, 18, 16, 6, 5, 15, 19, 9, 2, 12 ],
  [ 18, 10, 2, 7, 15, 21, 13, 5, 4, 12, 20, 16, 8, 1, 9, 17, 19, 11, 3, 6, 14 ],
  [ 19, 13, 7, 1, 6, 12, 18, 20, 14, 8, 2, 5, 11, 17, 21, 15, 9, 3, 4, 10, 16 ],
  [ 20, 16, 12, 8, 4, 1, 5, 9, 13, 17, 21, 19, 15, 11, 7, 3, 2, 6, 10, 14, 18 ],
  [ 21, 19, 17, 15, 13, 11, 9, 7, 5, 3, 1, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20 ]
 ]
gap> GroupByMultiplicationTable(last);
<group of size 21 with 21 generators>
gap> IsCyclic(last);
true

n=88
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,13,15,17,19,21,23,25,27,29,31,35,37,39,41,43],
[3,9,15,21,27,39,43,37,31,25,19,13,7,1,5,17,23,29,35,41],
[5,15,25,35,43,23,13,3,7,17,27,37,41,31,21,1,9,19,29,39],
[7,21,35,39,25,3,17,31,43,29,15,1,13,27,41,19,5,9,23,37],
[9,27,43,25,7,29,41,23,5,13,31,39,21,3,15,37,19,1,17,35],
[13,39,23,3,29,7,19,43,17,9,35,27,1,25,37,15,41,21,5,31],
[15,43,13,17,41,19,39,9,21,37,7,23,35,5,25,3,27,31,1,29],
[17,37,3,31,23,43,9,25,29,5,39,15,19,35,1,21,13,41,7,27],
[19,31,7,43,5,17,21,29,9,41,3,35,15,23,27,39,1,37,13,25],
[21,25,17,29,13,9,37,5,41,1,43,3,39,7,35,31,15,27,19,23],
[23,19,27,15,31,35,7,39,3,43,1,41,5,37,9,13,29,17,25,21],
[25,13,37,1,39,27,23,15,35,3,41,9,29,21,17,5,43,7,31,19],
[27,7,41,13,21,1,35,19,15,39,5,29,25,9,43,23,31,3,37,17],
[29,1,31,27,3,25,5,35,23,7,37,21,9,39,19,41,17,13,43,15],
[31,5,21,41,15,37,25,1,27,35,9,17,43,19,7,29,3,23,39,13],
[35,17,1,19,37,15,3,21,39,31,13,5,23,41,29,7,25,43,27,9],
[37,23,9,5,19,41,27,13,1,15,29,43,31,17,3,25,39,35,21,7],
[39,29,19,9,1,21,31,41,37,27,17,7,3,13,23,43,35,25,15,5],
[41,35,29,23,17,5,1,7,13,19,25,31,37,43,39,27,21,15,9,3],
[43,41,39,37,35,31,29,27,25,23,21,19,17,15,13,9,7,5,3,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 ],
  [ 2, 5, 7, 10, 13, 18, 20, 17, 15, 12, 9, 6, 4, 1, 3, 8, 11, 14, 16, 19 ],
  [ 3, 7, 12, 16, 20, 11, 6, 2, 4, 8, 13, 17, 19, 15, 10, 1, 5, 9, 14, 18 ],
  [ 4, 10, 16, 18, 12, 2, 8, 15, 20, 14, 7, 1, 6, 13, 19, 9, 3, 5, 11, 17 ],
  [ 5, 13, 20, 12, 4, 14, 19, 11, 3, 6, 15, 18, 10, 2, 7, 17, 9, 1, 8, 16 ],
  [ 6, 18, 11, 2, 14, 4, 9, 20, 8, 5, 16, 13, 1, 12, 17, 7, 19, 10, 3, 15 ],
  [ 7, 20, 6, 8, 19, 9, 18, 5, 10, 17, 4, 11, 16, 3, 12, 2, 13, 15, 1, 14 ],
  [ 8, 17, 2, 15, 11, 20, 5, 12, 14, 3, 18, 7, 9, 16, 1, 10, 6, 19, 4, 13 ],
  [ 9, 15, 4, 20, 3, 8, 10, 14, 5, 19, 2, 16, 7, 11, 13, 18, 1, 17, 6, 12 ],
  [ 10, 12, 8, 14, 6, 5, 17, 3, 19, 1, 20, 2, 18, 4, 16, 15, 7, 13, 9, 11 ],
  [ 11, 9, 13, 7, 15, 16, 4, 18, 2, 20, 1, 19, 3, 17, 5, 6, 14, 8, 12, 10 ],
  [ 12, 6, 17, 1, 18, 13, 11, 7, 16, 2, 19, 5, 14, 10, 8, 3, 20, 4, 15, 9 ],
  [ 13, 4, 19, 6, 10, 1, 16, 9, 7, 18, 3, 14, 12, 5, 20, 11, 15, 2, 17, 8 ],
  [ 14, 1, 15, 13, 2, 12, 3, 16, 11, 4, 17, 10, 5, 18, 9, 19, 8, 6, 20, 7 ],
  [ 15, 3, 10, 19, 7, 17, 12, 1, 13, 16, 5, 8, 20, 9, 4, 14, 2, 11, 18, 6 ],
  [ 16, 8, 1, 9, 17, 7, 2, 10, 18, 15, 6, 3, 11, 19, 14, 4, 12, 20, 13, 5 ],
```

```
  [ 17, 11, 5, 3, 9, 19, 13, 6, 1, 7, 14, 20, 15, 8, 2, 12, 18, 16, 10, 4 ],
  [ 18, 14, 9, 5, 1, 10, 15, 19, 17, 13, 8, 4, 2, 6, 11, 20, 16, 12, 7, 3 ],
  [ 19, 16, 14, 11, 8, 3, 1, 4, 6, 9, 12, 15, 17, 20, 18, 13, 10, 7, 5, 2 ],
  [ 20, 19, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 20 with 20 generators>
gap> IsCyclic(last);
false

n=90
gap> ct:=CanonicalCayleyTable([[1,7,11,13,17,19,23,29,31,37,41,43],
[7,41,13,1,29,43,19,23,37,11,17,31],[11,13,31,37,7,29,17,41,19,43,1,23],
[13,1,37,11,41,23,29,17,43,31,7,19],[17,29,7,41,19,37,31,43,13,1,23,11],
[19,43,29,23,37,1,13,11,41,17,31,7],[23,19,17,29,31,13,11,37,7,41,43,1],
[29,23,41,17,43,11,37,31,1,7,19,13],[31,37,19,43,13,41,7,1,29,23,11,17],
[37,11,43,31,1,17,41,7,23,19,13,29],[41,17,1,7,23,31,43,19,11,13,29,37],
[43,31,23,19,11,7,1,13,17,29,37,41]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 ],
  [ 2, 11, 4, 1, 8, 12, 6, 7, 10, 3, 5, 9 ],
  [ 3, 4, 9, 10, 2, 8, 5, 11, 6, 12, 1, 7 ],
  [ 4, 1, 10, 3, 11, 7, 8, 5, 12, 9, 2, 6 ],
  [ 5, 8, 2, 11, 6, 10, 9, 12, 4, 1, 7, 3 ],
  [ 6, 12, 8, 7, 10, 1, 4, 3, 11, 5, 9, 2 ],
  [ 7, 6, 5, 8, 9, 4, 3, 10, 2, 11, 12, 1 ],
  [ 8, 7, 11, 5, 12, 3, 10, 9, 1, 2, 6, 4 ],
  [ 9, 10, 6, 12, 4, 11, 2, 1, 8, 7, 3, 5 ],
  [ 10, 3, 12, 9, 1, 5, 11, 2, 7, 6, 4, 8 ],
  [ 11, 5, 1, 2, 7, 9, 12, 6, 3, 4, 8, 10 ],
  [ 12, 9, 7, 6, 3, 2, 1, 4, 5, 8, 10, 11 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 12 with 12 generators>
gap> IsCyclic(last);
true

n=92
gap> ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21,25,27,29,31,33,35,37,39,41,43,45],
[3,9,15,21,27,33,39,45,41,35,29,17,11,5,1,7,13,19,25,31,37,43],
[5,15,25,35,45,37,27,17,7,3,13,33,43,39,29,19,9,1,11,21,31,41],
[7,21,35,43,29,15,1,13,27,41,37,9,5,19,33,45,31,17,3,11,25,39],
[9,27,45,29,11,7,25,43,31,13,5,41,33,15,3,21,39,35,17,1,19,37],
[11,33,37,15,7,29,41,19,3,25,45,1,21,43,27,5,17,39,31,9,13,35],
[13,39,27,1,25,41,15,11,37,29,3,43,17,9,35,31,5,21,45,19,7,33],
[15,45,17,13,43,19,11,41,21,9,39,7,37,25,5,35,27,3,33,29,1,31],
[17,41,7,27,31,3,37,21,13,45,11,35,1,33,25,9,43,15,19,39,5,29],
[19,35,3,41,13,25,29,9,45,7,31,15,39,1,37,17,21,33,5,43,11,27],
[21,29,13,37,5,45,3,39,11,31,19,27,15,35,7,43,1,41,9,33,17,25],
[25,17,33,9,41,1,43,7,35,15,27,19,31,11,39,3,45,5,37,13,29,21],
[27,11,43,5,33,21,17,37,1,39,15,31,7,45,9,29,25,13,41,3,35,19],
[29,5,39,19,15,43,9,25,33,1,35,11,45,13,21,37,3,31,27,7,41,17],
[31,1,29,33,3,27,35,5,25,37,7,39,9,21,41,11,19,43,13,17,45,15],
[33,7,19,45,21,5,31,35,9,17,43,3,29,37,11,15,41,25,1,27,39,13],
[35,13,9,31,39,17,5,27,43,21,1,45,25,3,19,41,29,7,15,37,33,11],
```

[37,19,1,17,35,39,21,3,15,33,41,5,13,31,43,25,7,11,29,45,27,9],
[39,25,11,3,17,31,45,33,19,5,9,37,41,27,13,1,15,29,43,35,21,7],
[41,31,21,11,1,9,19,29,39,43,33,13,3,7,17,27,37,45,35,25,15,5],
[43,37,31,25,19,13,7,1,5,11,17,29,35,41,45,39,33,27,21,15,9,3],
[45,43,41,39,37,35,33,31,29,27,25,21,19,17,15,13,11,9,7,5,3,1]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21,
22], [2, 5, 8, 11, 13, 16, 19, 22, 20, 17, 14, 9, 6, 3, 1, 4, 7, 10,
12, 15, 18, 21],
[3, 8, 12, 17, 22, 18, 13, 9, 4, 2, 7, 16, 21, 19, 14, 10, 5, 1, 6, 11, 15,
20], [4, 11, 17, 21, 14, 8, 1, 7, 13, 20, 18, 5, 3, 10, 16, 22, 15, 9,
2, 6, 12, 19],
[5, 13, 22, 14, 6, 4, 12, 21, 15, 7, 3, 20, 16, 8, 2, 11, 19, 17, 9, 1, 10,
18], [6, 16, 18, 8, 4, 14, 20, 10, 2, 12, 22, 1, 11, 21, 13, 3, 9, 19,
15, 5, 7, 17],
[7, 19, 13, 1, 12, 20, 8, 6, 18, 14, 2, 21, 9, 5, 17, 15, 3, 11, 22, 10, 4,
16], [8, 22, 9, 7, 21, 10, 6, 20, 11, 5, 19, 4, 18, 12, 3, 17, 13, 2,
16, 14, 1, 15],
[9, 20, 4, 13, 15, 2, 18, 11, 7, 22, 6, 17, 1, 16, 12, 5, 21, 8, 10, 19, 3,
14], [10, 17, 2, 20, 7, 12, 14, 5, 22, 4, 15, 8, 19, 1, 18, 9, 11, 16,
3, 21, 6, 13],
[11, 14, 7, 18, 3, 22, 2, 19, 6, 15, 10, 13, 8, 17, 4, 21, 1, 20, 5, 16, 9,
12], [12, 9, 16, 5, 20, 1, 21, 4, 17, 8, 13, 10, 15, 6, 19, 2, 22, 3,
18, 7, 14, 11],
[13, 6, 21, 3, 16, 11, 9, 18, 1, 19, 8, 15, 4, 22, 5, 14, 12, 7, 20, 2, 17,
10], [14, 3, 19, 10, 8, 21, 5, 12, 16, 1, 17, 6, 22, 7, 11, 18, 2, 15,
13, 4, 20, 9],
[15, 1, 14, 16, 2, 13, 17, 3, 12, 18, 4, 19, 5, 11, 20, 6, 10, 21, 7, 9, 22,
8], [16, 4, 10, 22, 11, 3, 15, 17, 5, 9, 21, 2, 14, 18, 6, 8, 20, 12,
1, 13, 19, 7],
[17, 7, 5, 15, 19, 9, 3, 13, 21, 11, 1, 22, 12, 2, 10, 20, 14, 4, 8, 18, 16,
6], [18, 10, 1, 9, 17, 19, 11, 2, 8, 16, 20, 3, 7, 15, 21, 12, 4, 6,
14, 22, 13, 5],
[19, 12, 6, 2, 9, 15, 22, 16, 10, 3, 5, 18, 20, 13, 7, 1, 8, 14, 21, 17, 11,
4], [20, 15, 11, 6, 1, 5, 10, 14, 19, 21, 16, 7, 2, 4, 9, 13, 18, 22,
17, 12, 8, 3],
[21, 18, 15, 12, 10, 7, 4, 1, 3, 6, 9, 14, 17, 20, 22, 19, 16, 13, 11, 8, 5,
2], [22, 21, 20, 19, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5,
4, 3, 2, 1]]
gap> GroupByMultiplicationTable(last);
<group of size 22 with 22 generators>
gap> IsCyclic(last);
true

n=94
gap>
ct:=CanonicalCayleyTable([[1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45],
[3,9,15,21,27,33,39,45,43,37,31,25,19,13,7,1,5,11,17,23,29,35,41],
[5,15,25,35,45,39,29,19,9,1,11,21,31,41,43,33,23,13,3,7,17,27,37],
[7,21,35,45,31,17,3,11,25,39,41,27,13,1,15,29,43,37,23,9,5,19,33],
[9,27,45,31,13,5,23,41,35,17,1,19,37,39,21,3,15,33,43,25,7,11,29],
[11,33,39,17,5,27,45,23,1,21,43,29,7,15,37,35,13,9,31,41,19,3,25],
[13,39,29,3,23,45,19,7,33,35,9,17,43,25,1,27,41,15,11,37,31,5,21],

[15,45,19,11,41,23,7,37,27,3,33,31,1,29,35,5,25,39,9,21,43,13,17],
[17,43,9,25,35,1,33,27,7,41,19,15,45,11,23,37,3,31,29,5,39,21,13],
[19,37,1,39,17,21,35,3,41,15,23,33,5,43,13,25,31,7,45,11,27,29,9],
[21,31,11,41,1,43,9,33,19,23,29,13,39,3,45,7,35,17,25,27,15,37,5],
[23,25,21,27,19,29,17,31,15,33,13,35,11,37,9,39,7,41,5,43,3,45,1],
[25,19,31,13,37,7,43,1,45,5,39,11,33,17,27,23,21,29,15,35,9,41,3],
[27,13,41,1,39,15,25,29,11,43,3,37,17,23,31,9,45,5,35,19,21,33,7],
[29,7,43,15,21,37,1,35,23,13,45,9,27,31,5,41,17,19,39,3,33,25,11],
[31,1,33,29,3,35,27,5,37,25,7,39,23,9,41,21,11,43,19,13,45,17,15],
[33,5,23,43,15,13,41,25,3,31,35,7,21,45,17,11,39,27,1,29,37,9,19],
[35,11,13,37,33,9,15,39,31,7,17,41,29,5,19,43,27,3,21,45,25,1,23],
[37,17,3,23,43,31,11,9,29,45,25,5,15,35,39,19,1,21,41,33,13,7,27],
[39,23,7,9,25,41,37,21,5,11,27,43,35,19,3,13,29,45,33,17,1,15,31],
[41,29,17,5,7,19,31,43,39,27,15,3,9,21,33,45,37,25,13,1,11,23,35],
[43,35,27,19,11,3,5,13,21,29,37,45,41,33,25,17,9,1,7,15,23,31,39],
[45,41,37,33,29,25,21,17,13,9,5,1,3,7,11,15,19,23,27,31,35,39,43]]);
[[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23],
[2, 5, 8, 11, 14, 17, 20, 23, 22, 19, 16, 13, 10, 7, 4, 1, 3, 6, 9, 12, 15, 18, 21],
[3, 8, 13, 18, 23, 20, 15, 10, 5, 1, 6, 11, 16, 21, 22, 17, 12, 7, 2, 4, 9, 14, 19],
[4, 11, 18, 23, 16, 9, 2, 6, 13, 20, 21, 14, 7, 1, 8, 15, 22, 19, 12, 5, 3, 10, 17],
[5, 14, 23, 16, 7, 3, 12, 21, 18, 9, 1, 10, 19, 20, 11, 2, 8, 17, 22, 13, 4, 6, 15],
[6, 17, 20, 9, 3, 14, 23, 12, 1, 11, 22, 15, 4, 8, 19, 18, 7, 5, 16, 21, 10, 2, 13], [7, 20, 15, 2, 12, 23, 10, 4, 17, 18, 5, 9, 22, 13, 1, 14, 21, 8, 6, 19, 16, 3, 11],
[8, 23, 10, 6, 21, 12, 4, 19, 14, 2, 17, 16, 1, 15, 18, 3, 13, 20, 5, 11, 22, 7, 9],
[9, 22, 5, 13, 18, 1, 17, 14, 4, 21, 10, 8, 23, 6, 12, 19, 2, 16, 15, 3, 20, 11, 7], [10, 19, 1, 20, 9, 11, 18, 2, 21, 8, 12, 17, 3, 22, 7, 13, 16, 4, 23, 6, 14, 15, 5],
[11, 16, 6, 21, 1, 22, 5, 17, 10, 12, 15, 7, 20, 2, 23, 4, 18, 9, 13, 14, 8, 19, 3], [12, 13, 11, 14, 10, 15, 9, 16, 8, 17, 7, 18, 6, 19, 5, 20, 4, 21, 3, 22, 2, 23, 1],
[13, 10, 16, 7, 19, 4, 22, 1, 23, 3, 20, 6, 17, 9, 14, 12, 11, 15, 8, 18, 5, 21, 2],
[14, 7, 21, 1, 20, 8, 13, 15, 6, 22, 2, 19, 9, 12, 16, 5, 23, 3, 18, 10, 11, 17, 4],
[15, 4, 22, 8, 11, 19, 1, 18, 12, 7, 23, 5, 14, 16, 3, 21, 9, 10, 20, 2, 17, 13, 6], [16, 1, 17, 15, 2, 18, 14, 3, 19, 13, 4, 20, 12, 5, 21, 11, 6, 22, 10, 7, 23, 9, 8],
[17, 3, 12, 22, 8, 7, 21, 13, 2, 16, 18, 4, 11, 23, 9, 6, 20, 14, 1, 15, 19, 5, 10],
[18, 6, 7, 19, 17, 5, 8, 20, 16, 4, 9, 21, 15, 3, 10, 22, 14, 2, 11, 23, 13, 1, 12],
[19, 9, 2, 12, 22, 16, 6, 5, 15, 23, 13, 3, 8, 18, 20, 10, 1, 11, 21, 17, 7, 4, 14], [20, 12, 4, 5, 13, 21, 19, 11, 3, 6, 14, 22, 18, 10, 2, 7, 15, 23, 17, 9, 1, 8, 16],
[21, 15, 9, 3, 4, 10, 16, 22, 20, 14, 8, 2, 5, 11, 17, 23, 19, 13, 7, 1, 6,

```
    12, 18 ], [ 22, 18, 14, 10, 6, 2, 3, 7, 11, 15, 19, 23, 21, 17, 13, 9, 5,
    1, 4, 8, 12, 16, 20 ],
  [ 23, 21, 19, 17, 15, 13, 11, 9, 7, 5, 3, 1, 2, 4, 6, 8, 10, 12, 14, 16, 18,
    20, 22 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 23 with 23 generators>
gap> IsCyclic(last);
true

n=96
gap> ct:=CanonicalCayleyTable([[1,5,7,11,13,17,19,23,25,29,31,35,37,41,43,47],
[5,25,35,41,31,11,1,19,29,47,37,17,7,13,23,43],[7,35,47,19,5,23,37,31,17,11,25,43,29,1,13,41],
[11,41,19,25,47,5,17,35,13,31,43,1,23,29,7,37],[13,31,5,47,23,29,41,11,37,7,19,25,1,43,17,35],
[17,11,23,5,29,1,35,7,41,13,47,19,43,25,37,31],[19,1,37,17,41,35,23,43,5,25,13,7,31,11,47,29],
[23,19,31,35,11,7,43,47,1,5,41,37,13,17,29,25],[25,29,17,13,37,41,5,1,47,43,7,11,35,31,19,23],
[29,47,11,31,7,13,25,5,43,23,35,41,17,37,1,19],[31,37,25,43,19,47,13,41,7,35,1,29,5,23,11,17],
[35,17,43,1,25,19,7,37,11,41,29,23,47,5,31,13],[37,7,29,23,1,43,31,13,35,17,5,47,25,19,41,11],
[41,13,1,29,43,25,11,17,31,37,23,5,19,47,35,7],[43,23,13,7,17,37,47,29,19,1,11,31,41,35,25,5],
[47,43,41,37,35,31,29,25,23,19,17,13,11,7,5,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 ],
  [ 2, 9, 12, 14, 11, 4, 1, 7, 10, 16, 13, 6, 3, 5, 8, 15 ],
  [ 3, 12, 16, 7, 2, 8, 13, 11, 6, 4, 9, 15, 10, 1, 5, 14 ],
  [ 4, 14, 7, 9, 16, 2, 6, 12, 5, 11, 15, 1, 8, 10, 3, 13 ],
  [ 5, 11, 2, 16, 8, 10, 14, 4, 13, 3, 7, 9, 1, 15, 6, 12 ],
  [ 6, 4, 8, 2, 10, 1, 12, 3, 14, 5, 16, 7, 15, 9, 13, 11 ],
  [ 7, 1, 13, 6, 14, 12, 8, 15, 2, 9, 5, 3, 11, 4, 16, 10 ],
  [ 8, 7, 11, 12, 4, 3, 15, 16, 1, 2, 14, 13, 5, 6, 10, 9 ],
  [ 9, 10, 6, 5, 13, 14, 2, 1, 16, 15, 3, 4, 12, 11, 7, 8 ],
  [ 10, 16, 4, 11, 3, 5, 9, 2, 15, 8, 12, 14, 6, 13, 1, 7 ],
  [ 11, 13, 9, 15, 7, 16, 5, 14, 3, 12, 1, 10, 2, 8, 4, 6 ],
  [ 12, 6, 15, 1, 9, 7, 3, 13, 4, 14, 10, 8, 16, 2, 11, 5 ],
  [ 13, 3, 10, 8, 1, 15, 11, 5, 12, 6, 2, 16, 9, 7, 14, 4 ],
  [ 14, 5, 1, 10, 15, 9, 4, 6, 11, 13, 8, 2, 7, 16, 12, 3 ],
  [ 15, 8, 5, 3, 6, 13, 16, 10, 7, 1, 4, 11, 14, 12, 9, 2 ],
  [ 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 16 with 16 generators>
gap> IsCyclic(last);
false

n=98
gap> ct:=CanonicalCayleyTable([[1,3,5,9,11,13,15,17,19,23,25,27,29,31,33,37,39,41,43,45,47],
[3,9,15,27,33,39,45,47,41,29,23,17,11,5,1,13,19,25,31,37,43],
[5,15,25,45,43,33,23,13,3,17,27,37,47,41,31,11,1,9,19,29,39],
[9,27,45,17,1,19,37,43,25,11,29,47,33,15,3,39,41,23,5,13,31],
[11,33,43,1,23,45,31,9,13,41,19,3,25,47,29,15,37,39,17,5,27],
[13,39,33,19,45,27,1,25,47,5,31,41,15,11,37,9,17,43,29,3,23],
[15,45,23,37,31,1,29,39,9,47,17,13,43,25,5,33,3,27,41,11,19],
[17,47,13,43,9,25,39,5,29,1,33,31,3,37,27,41,23,11,45,19,15],
[19,41,3,25,13,47,9,29,31,45,15,23,37,1,39,17,43,5,33,27,11],
[23,29,17,11,41,5,47,1,45,39,13,33,19,27,25,31,15,37,9,43,3],
[25,23,27,29,19,31,17,33,15,13,37,11,39,9,41,43,5,45,3,47,1],
```

```
[27,17,37,47,3,41,13,31,23,33,11,43,1,45,9,19,25,29,15,39,5],
[29,11,47,33,25,15,43,3,37,19,39,1,41,17,23,5,45,13,27,31,9],
[31,5,41,15,47,11,25,37,1,27,9,45,17,19,43,29,33,3,39,23,13],
[33,1,31,3,29,37,5,27,39,25,41,9,23,43,11,45,13,19,47,15,17],
[37,13,11,39,15,9,33,41,17,31,43,19,5,29,45,3,27,47,23,1,25],
[39,19,1,41,37,17,3,23,43,15,5,25,45,33,13,27,47,31,11,9,29],
[41,25,9,23,39,43,27,11,5,37,45,29,13,3,19,47,31,15,1,17,33],
[43,31,19,5,17,29,41,45,33,9,3,15,27,39,47,23,11,1,13,25,37],
[45,37,29,13,5,3,11,19,27,43,47,39,31,23,15,1,9,17,25,33,41],
[47,43,39,31,27,23,19,15,11,3,1,5,9,13,17,25,29,33,37,41,45]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21 ],
  [ 2, 4, 7, 12, 15, 17, 20, 21, 18, 13, 10, 8, 5, 3, 1, 6, 9, 11, 14, 16, 19 ],
  [ 3, 7, 11, 20, 19, 15, 10, 6, 2, 8, 12, 16, 21, 18, 14, 5, 1, 4, 9, 13, 17 ],
  [ 4, 12, 20, 8, 1, 9, 16, 19, 11, 5, 13, 21, 15, 7, 2, 17, 18, 10, 3, 6, 14 ],
  [ 5, 15, 19, 1, 10, 20, 14, 4, 6, 18, 9, 2, 11, 21, 13, 7, 16, 17, 8, 3, 12 ],
  [ 6, 17, 15, 9, 20, 12, 1, 11, 21, 3, 14, 18, 7, 5, 16, 4, 8, 19, 13, 2, 10 ],
  [ 7, 20, 10, 16, 14, 1, 13, 17, 4, 21, 8, 6, 19, 11, 3, 15, 2, 12, 18, 5, 9 ],
  [ 8, 21, 6, 19, 4, 11, 17, 3, 13, 1, 15, 14, 2, 16, 12, 18, 10, 5, 20, 9, 7 ],
  [ 9, 18, 2, 11, 6, 21, 4, 13, 14, 20, 7, 10, 16, 1, 17, 8, 19, 3, 15, 12, 5 ],
  [ 10, 13, 8, 5, 18, 3, 21, 1, 20, 17, 6, 15, 9, 12, 11, 14, 7, 16, 4, 19, 2 ],
  [ 11, 10, 12, 13, 9, 14, 8, 15, 7, 6, 16, 5, 17, 4, 18, 19, 3, 20, 2, 21, 1 ],
  [ 12, 8, 16, 21, 2, 18, 6, 14, 10, 15, 5, 19, 1, 20, 4, 9, 11, 13, 7, 17, 3 ],
  [ 13, 5, 21, 15, 11, 7, 19, 2, 16, 9, 17, 1, 18, 8, 10, 3, 20, 6, 12, 14, 4 ],
  [ 14, 3, 18, 7, 21, 5, 11, 16, 1, 12, 4, 20, 8, 9, 19, 13, 15, 2, 17, 10, 6 ],
  [ 15, 1, 14, 2, 13, 16, 3, 12, 17, 11, 18, 4, 10, 19, 5, 20, 6, 9, 21, 7, 8 ],
  [ 16, 6, 5, 17, 7, 4, 15, 18, 8, 14, 19, 9, 3, 13, 20, 2, 12, 21, 10, 1, 11 ],
  [ 17, 9, 1, 18, 16, 8, 2, 10, 19, 7, 3, 11, 20, 15, 6, 12, 21, 14, 5, 4, 13 ],
  [ 18, 11, 4, 10, 17, 19, 12, 5, 3, 16, 20, 13, 6, 2, 9, 21, 14, 7, 1, 8, 15 ],
  [ 19, 14, 9, 3, 8, 13, 18, 20, 15, 4, 2, 7, 12, 17, 21, 10, 5, 1, 6, 11, 16 ],
  [ 20, 16, 13, 6, 3, 2, 5, 9, 12, 19, 21, 17, 14, 10, 7, 1, 4, 8, 11, 15, 18 ],
  [ 21, 19, 17, 14, 12, 10, 9, 7, 5, 2, 1, 3, 4, 6, 8, 11, 13, 15, 16, 18, 20 ]
 ]
gap> GroupByMultiplicationTable(last);
<group of size 21 with 21 generators>
gap> IsCyclic(last);
true

n=100
gap> ct:=CanonicalCayleyTable([[1,3,7,9,11,13,17,19,21,23,27,29,31,33,37,39,41,43,47,49],
[3,9,21,27,33,39,49,43,37,31,19,13,7,1,11,17,23,29,41,47],
[7,21,49,37,23,9,19,33,47,39,11,3,17,31,41,27,13,1,29,43],
[9,27,37,19,1,17,47,29,11,7,43,39,21,3,33,49,31,13,23,41],
[11,33,23,1,21,43,13,9,31,47,3,19,41,37,7,29,49,27,17,39],
[13,39,9,17,43,31,21,47,27,1,49,23,3,29,19,7,33,41,11,37],
[17,49,19,47,13,21,11,23,43,9,41,7,27,39,29,37,3,31,1,33],
[19,43,33,29,9,47,23,39,1,37,13,49,11,27,3,41,21,17,7,31],
[21,37,47,11,31,27,43,1,41,17,33,9,49,7,23,19,39,3,13,29],
[23,31,39,7,47,1,9,37,17,29,21,33,13,41,49,3,43,11,19,27],
[27,19,11,43,3,49,41,13,33,21,29,17,37,9,1,47,7,39,31,23],
[29,13,3,39,19,23,7,49,9,33,17,41,1,43,27,31,11,47,37,21],
[31,7,17,21,41,3,27,11,49,13,37,1,39,23,47,9,29,33,43,19],
[33,1,31,3,37,29,39,27,7,41,9,43,23,11,21,13,47,19,49,17],
```

```
[37,11,41,33,7,19,29,3,23,49,1,27,47,21,31,43,17,9,39,13],
[39,17,27,49,29,7,37,41,19,3,47,31,9,13,43,21,1,23,33,11],
[41,23,13,31,49,33,3,21,39,43,7,11,29,47,17,1,19,37,27,9],
[43,29,1,13,27,41,31,17,3,11,39,47,33,19,9,23,37,49,21,7],
[47,41,29,23,17,11,1,7,13,19,31,37,43,49,39,33,27,21,9,3],
[49,47,43,41,39,37,33,31,29,27,23,21,19,17,13,11,9,7,3,1]]);
[ [ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20 ],
  [ 2, 4, 9, 11, 14, 16, 20, 18, 15, 13, 8, 6, 3, 1, 5, 7, 10, 12, 17, 19 ],
  [ 3, 9, 20, 15, 10, 4, 8, 14, 19, 16, 5, 2, 7, 13, 17, 11, 6, 1, 12, 18 ],
  [ 4, 11, 15, 8, 1, 7, 19, 12, 5, 3, 18, 16, 9, 2, 14, 20, 13, 6, 10, 17 ],
  [ 5, 14, 10, 1, 9, 18, 6, 4, 13, 19, 2, 8, 17, 15, 3, 12, 20, 11, 7, 16 ],
  [ 6, 16, 4, 7, 18, 13, 9, 19, 11, 1, 20, 10, 2, 12, 8, 3, 14, 17, 5, 15 ],
  [ 7, 20, 8, 19, 6, 9, 5, 10, 18, 4, 17, 3, 11, 16, 12, 15, 2, 13, 1, 14 ],
  [ 8, 18, 14, 12, 4, 19, 10, 16, 1, 15, 6, 20, 5, 11, 2, 17, 9, 7, 3, 13 ],
  [ 9, 15, 19, 5, 13, 11, 18, 1, 17, 7, 14, 4, 20, 3, 10, 8, 16, 2, 6, 12 ],
  [ 10, 13, 16, 3, 19, 1, 4, 15, 7, 12, 9, 14, 6, 17, 20, 2, 18, 5, 8, 11 ],
  [ 11, 8, 5, 18, 2, 20, 17, 6, 14, 9, 12, 7, 15, 4, 1, 19, 3, 16, 13, 10 ],
  [ 12, 6, 2, 16, 8, 10, 3, 20, 4, 14, 7, 17, 1, 18, 11, 13, 5, 19, 15, 9 ],
  [ 13, 3, 7, 9, 17, 2, 11, 5, 20, 6, 15, 1, 16, 10, 19, 4, 12, 14, 18, 8 ],
  [ 14, 1, 13, 2, 15, 12, 16, 11, 3, 17, 4, 18, 10, 5, 9, 6, 19, 8, 20, 7 ],
  [ 15, 5, 17, 14, 3, 8, 12, 2, 10, 20, 1, 11, 19, 9, 13, 18, 7, 4, 16, 6 ],
  [ 16, 7, 11, 20, 12, 3, 15, 17, 8, 2, 19, 13, 4, 6, 18, 9, 1, 10, 14, 5 ],
  [ 17, 10, 6, 13, 20, 14, 2, 9, 16, 18, 3, 5, 12, 19, 7, 1, 8, 15, 11, 4 ],
  [ 18, 12, 1, 6, 11, 17, 13, 7, 2, 5, 16, 19, 14, 8, 4, 10, 15, 20, 9, 3 ],
  [ 19, 17, 12, 10, 7, 5, 1, 3, 6, 8, 13, 15, 18, 20, 16, 14, 11, 9, 4, 2 ],
  [ 20, 19, 18, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1 ] ]
gap> GroupByMultiplicationTable(last);
<group of size 20 with 20 generators>
gap> IsCyclic(last);
true
```

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 $\left\lfloor \frac{500}{12} \right\rfloor$ 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 $1, 2, 3, 4, \ldots, n$*, 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."*

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 $\frac{a(a+1)(a+2)(a+3)\ldots(a+n-1)}{1.2.3\ldots n}$ 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* $1, 2, 3 \ldots n$*."*

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.

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

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.

Minorer le nombre de décomposants de Goldbach

Denise Vella-Chemla

16/3/13

La conjecture de Goldbach stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.

Les décomposants de Goldbach d'un nombre pair peuvent être caractérisés ainsi : un entier $m_i \in]\sqrt{n}, n/2]$ qui n'est divisible par aucun des nombres premiers $p_j < \sqrt{n}$ et dont le complémentaire à n qui est $n - m_i$ n'est pas non-plus divisible par p_j est un décomposant de Goldbach de n.
Notons DG_n l'ensemble contenant de tels entiers* et $dg(n) = |DG_n|$ le nombre de décompositions de Goldbach de n.
Considérons un entier $m_i \leqslant r$, non divisible, ainsi que son complémentaire à n, par tout nombre premier inférieur ou égal à r. Soit $dg(n, r)$ l'ensemble de ces nombres.
Dans la mesure où $dg(n, \sqrt{n})$ ne comptabilise pas les décompositions de Goldbach dont l'un des sommants serait $< \sqrt{n}$, $dg(n) \geqslant dg(n, \sqrt{n})$

Soit $r \geqslant 2$ entier.

- on note $idh(n, p_j)$ le nombre d'entiers impairs $m_i \leqslant \dfrac{n}{2}$ qui sont divisibles par le nombre premier p_j ;†
- on note $icdh(n, p_j)$ le nombre d'entiers impairs $m_i \leqslant \dfrac{n}{2}$ dont le complémentaire à n qui est $n - m_i$ est divisible par p_j‡.

On va exprimer $dg(n, r)$ en fonction des $idh(n, p_i)$ et des $icdh(n, p_i)$.

Pour estimer $dg(n, r)$, nous utilisons un outil emprunté à l'analyse combinatoire : le *principe d'inclusion-exclusion.*

Lemme : *Dans l'ensemble des entiers $\{1, 2, \ldots, n\}$, soient m relations $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m$ portant sur ces entiers et $W(r)$ le nombre des entiers qui satisfont à r relations P_i. Alors, le nombre des entiers qui ne satisfont aucune des relations P_i est donné par la formule*

$$n + \sum_{k=1}^{m} (-1)^k W(k)$$

Par le *principe d'inclusion-exclusion*, l'égalité $min(a, b) = a + b - max(a, b)$ se généralise en :

$$\begin{aligned} min(a_1, \ldots, a_r) = \quad & a_1 + a_2 + a_3 + \ldots + a_r \\ & -max(a_1, a_2) - \ldots - max(a_{r-1}, a_r) \\ & +max(a_1, a_2, a_3) + \ldots + max(a_{r-2}, a_{r-1}, a_r) \\ & - \ldots \\ & \pm max(a1, \ldots, a_r). \end{aligned}$$

Fournissons quelques valeurs de $icdh(n, p_j)$ qui nous permettront de l'estimer aisément :

- les valeurs de $icdh(n, 3)$ pour $n \geqslant 18$ sont $2, 1, 1, 2, 2, 2,\ 3, 2, 2, 3, 3, 3, \ldots$ tandis que les valeurs de $idh(n, 3)$ pour les mêmes n sont $2, 2, 2, 2, 2, 2,\ 3, 3, 3, 3, 3, 3, \ldots$;

*Les lettres *DG* sont acronymes de décomposant de Goldbach.
†Les lettres *id* sont acronymes de "impair divisible par".
‡Les lettres *icd* sont acronymes de "impair dont le complémentaire est divisible par".

- les valeurs de $icdh(n,5)$ pour $n \geqslant 30$ sont $2,1,1,1,1,2,2,2,2,2,\ 3,2,2,2,2,3,3,3,3,3,\ldots$ tandis que les valeurs de $idh(n,5)$ pour les mêmes n sont $2,2,2,2,2,2,2,2,2,2,\ 3,3,3,3,3,3,3,3,3,3,\ldots$.

On voit qu'on a toujours :

$$icdh(n,p_j) \leqslant idh(n,p_j)$$

avec

$$idh(n,p_j) = \left\lfloor \frac{n+2p_j}{4p_j} \right\rfloor$$

Appelons $dp(n)$ le nombre $\left\lfloor \frac{\frac{n}{2}-1}{2} \right\rfloor$[§].

Appelons $id(n,p_j)$ la fraction $\dfrac{idh(n,p_j)}{dp(n)}$.

L'application du *principe d'inclusion-exclusion* permet d'obtenir[¶] :

$$\begin{aligned} dg(n,r) = dp(n)\Big(1 \quad & -\sum_{p\leqslant r} id(n,p) - \sum_{p\leqslant r} icd(n,p) \\ & + \sum_{p_1<p_2\leqslant r} id(n,p_1)id(n,p_2) + \sum_{p_1<p_2\leqslant r} id(n,p_1)icd(n,p_2) \\ & \quad + \sum_{p_1<p_2\leqslant r} icd(n,p_1)id(n,p_2) + \sum_{p_1<p_2\leqslant r} icd(n,p_1)icd(n,p_2) \\ & - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)icd(n,p_3) \\ & \quad - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)icd(n,p_2)id(n,p_3) - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)icd(n,p_2)icd(n,p_3) \\ & \quad - \sum_{p_1<p_2<p_3\leqslant r} icd(n,p_1)id(n,p_2)id(n,p_3) - \sum_{p_1<p_2<p_3\leqslant r} icd(n,p_1)id(n,p_2)icd(n,p_3) \\ & \quad - \sum_{p_1<p_2<p_3\leqslant r} icd(n,p_1)icd(n,p_2)id(n,p_3) - \sum_{p_1<p_2<p_3\leqslant r} icd(n,p_1)icd(n,p_2)icd(n,p_3) \\ & + \ldots\Big) \end{aligned}$$

Serait-il possible de minorer $dg(n,r)$ en remplaçant dans cette formule tous les $icd(n,p_j)$ par des $id(n,p_j)$.

La formule devient :

$$\begin{aligned} dg(n,r) \quad \overset{?}{\geqslant} \quad dp(n)\Big(1 \quad & -\sum_{p\leqslant r} id(n,p) - \sum_{p\leqslant r} id(n,p) \\ & + \sum_{p_1<p_2\leqslant r} id(n,p_1)id(n,p_2) + \sum_{p_1<p_2\leqslant r} id(n,p_1)id(n,p_2) \\ & \quad + \sum_{p_1<p_2\leqslant r} id(n,p_1)id(n,p_2) + \sum_{p_1<p_2\leqslant r} id(n,p_1)id(n,p_2) \\ & - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) \\ & \quad - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) \\ & \quad - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) \\ & \quad - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) - \sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) \\ & + \ldots\Big) \end{aligned}$$

[§]Les lettres *dp* sont acronymes de décomposants potentiels, $dp(n)$ est le nombre d'impairs compris entre 3 et $n/2$.

[¶]Dans les grilles, multiplier un $id(n,p_i)$ par un $id(n,p_j)$ correspond au fait qu'une case grise d'une ligne se trouve dans la même colonne qu'une case grise d'une autre ligne, multiplier un $icd(n,p_i)$ par un $id(n,p_j)$ correspond au fait qu'une case bleue d'une ligne se trouve dans la même colonne qu'une case grise d'une autre ligne, tandis que multiplier un $icd(n,p_i)$ par un $icd(n,p_j)$ correspond au fait qu'une case bleue d'une ligne se trouve dans la même colonne qu'une case bleue d'une autre ligne.

$$dg(n,r) \overset{?}{\geqslant} dp(n)\Big(1 \quad -2\sum_{p\leqslant r} id(n,p) \\ +4\sum_{p_1<p_2\leqslant r} id(n,p_1)id(n,p_2) \\ -8\sum_{p_1<p_2<p_3\leqslant r} id(n,p_1)id(n,p_2)id(n,p_3) \\ +\dots\Big)$$

Cette dernière formule se réécrit en :

$$dg(n,r) \overset{?}{\geqslant} dp(n)\prod_{p_j\leqslant r}\left(1-\frac{2\ idh(n,p_j)}{dp(n)}\right)$$

Cependant, très rapidement, (à partir de $n = 992$), le nombre obtenu par cette formule est supérieur au nombre de décompositions de Goldbach.

Les idées de minoration fournies ci-après, bien que semblant effectives par tests informatiques, ne sont pas satisfaisantes parce qu'elles ne découlent pas suffisamment de la méthode qui a été présentée ci-dessus.

Fournissons cependant de ces minorations une justification heuristique : dans la mesure où l'application du principe d'inclusion-exclusion semble correspondre au fait d'éliminer de l'ensemble des nombres premiers ceux appartenant à une classe de congruence particulière pour chaque module premier inférieur ou égal à $\sqrt{n}$ (en fait, cela n'est le cas que pour les modules ne divisant pas n) , il semble naturel de minorer $dg(n,r)$, et donc $dg(n)$ de la façon suivante :

$$dg(n) \geqslant dg(n,\sqrt{n}) \overset{?}{\geqslant} (\pi(n/2)-\pi(\sqrt{n}))\prod_{p\leqslant\sqrt{n}}\left(1-\frac{1}{p}\right)$$

L'utilisation de la minoration de Tchebychev ($\pi(x) > \dfrac{x}{2ln\ x}$) dans l'inégalité précédente devrait permettre que soit toujours vérifiée :

$$dg(n) \overset{?}{\geqslant} \left(\frac{n\ ln\ 2}{2(ln\ n + ln\ 0.5)} - \frac{2\ \sqrt{n}\ ln\ 2}{ln\ n}\right)\prod_{p\leqslant\sqrt{n},p\nmid n}\left(1-\frac{1}{p}\right)$$

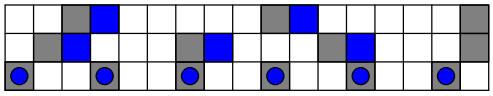
On vérifie cette minoration par programme pour tout $n \leqslant 2.10^8$. On vérifie également par programme dans les mêmes limites que :

$$dg(n) \geqslant \frac{n}{4ln^2 n}$$

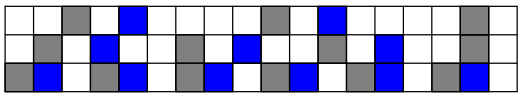
Annexe : valeurs des $id(n, p_i)$ et $icd(n, p_i)$ pour n compris entre 24 et 100

n	$dp(n)$	$idh(n,3)$	$icdh(n,3)$	$idh(n,5)$	$icdh(n,5)$	$idh(n,7)$	$icdh(n,7)$
24	5	2	2	–	–	–	–
26	6	2	2	1	1	–	–
28	6	2	2	1	1	–	–
30	7	3	3	2	2	–	–
32	7	3	2	2	1	–	–
34	8	3	2	2	1	–	–
36	8	3	3	2	1	–	–
38	9	3	3	2	1	–	–
40	9	3	3	2	2	–	–
42	10	4	4	2	2	–	–
44	10	4	3	2	2	–	–
46	11	4	3	2	2	–	–
48	11	4	4	2	2	–	–
50	12	4	4	3	3	2	1
52	12	4	4	3	2	2	1
54	13	5	5	3	2	2	1
56	13	5	4	3	2	2	2
58	14	5	4	3	2	2	2
60	14	5	5	3	3	2	2
62	15	5	5	3	3	2	2
64	15	5	5	3	3	2	2
66	16	6	6	3	3	2	2
68	16	6	5	3	3	2	2
70	17	6	5	4	4	3	3
72	17	6	6	4	3	3	2
74	18	6	6	4	3	3	2
76	18	6	6	4	3	3	2
78	19	7	7	4	3	3	2
80	19	7	6	4	4	3	2
82	20	7	6	4	4	3	2
84	20	7	7	4	4	3	3
86	21	7	7	4	4	3	3
88	21	7	7	4	4	3	3
90	22	8	8	5	5	3	3
92	22	8	7	5	4	3	3
94	23	8	7	5	4	3	3
96	23	8	8	5	4	3	3
98	24	8	8	5	4	4	4
100	24	8	8	5	5	4	3

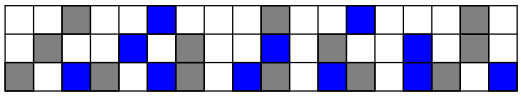
69 67 65 63 61 59 57 55 53 51 49 47 45 43 41 39 37
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35



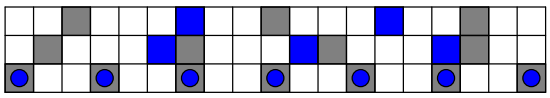
71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41 39 37
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37



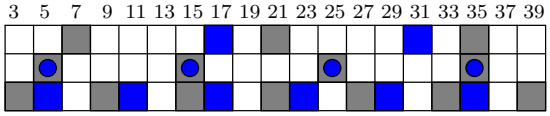
73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41 39
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37



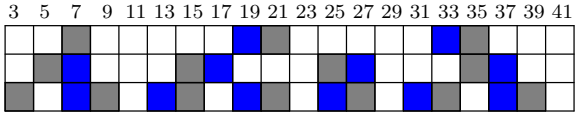
75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41 39
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39



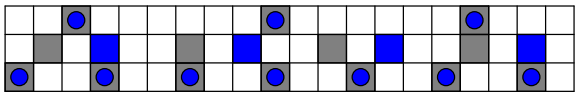
77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39



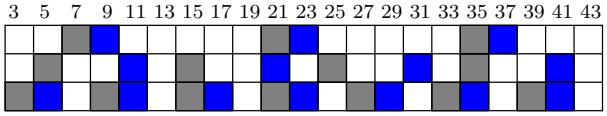
79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43 41
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41



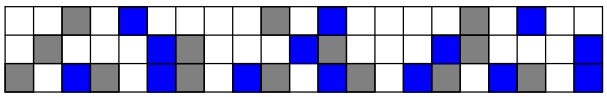
81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41



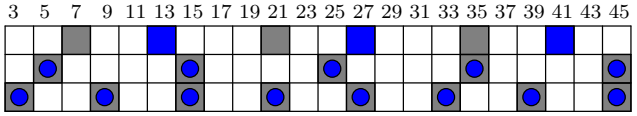
83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45 43
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43



85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43



87 85 83 81 79 77 75 73 71 69 67 65 63 61 59 57 55 53 51 49 47 45
3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45



- $n = 144$ $(DG : 5, 7, 13, 17, 31, 37, 41, 43, 47, 61, 71)$

  $n = 2^4.3^2$.
  $n/2 = 72$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		139 (p)	
11 (p)	0 $(mod\ 11)$	0 $(mod\ 7)$	133	
17 (p)			127 (p)	$17 + 127$
23 (p)		0 $(mod\ 11)$	121	
29 (p)		0 $(mod\ 5)$	115	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		109 (p)	
41 (p)			103 (p)	$41 + 103$
47 (p)			97 (p)	$47 + 97$
53 (p)		0 $(mod\ 7)$	91	
59 (p)		0 $(mod\ 5)$	85	
65	0 $(mod\ 5)$		79 (p)	
71 (p)			73 (p)	$71 + 73$

7 (p)	0 $(mod\ 7)$		137 (p)	
13 (p)			131 (p)	$13 + 131$
19 (p)		0 $(mod\ 5)$	125	
25	0 $(mod\ 5)$	0 $(mod\ 7)$	119	
31 (p)			113 (p)	$31 + 113$
37 (p)			107 (p)	$37 + 107$
43 (p)			101 (p)	$43 + 101$
49	0 $(mod\ 7)$	0 $(mod\ 5)$	95	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		89 (p)	
61 (p)			83 (p)	$61 + 83$
67 (p)		0 $(mod\ 7)$ et 0 $(mod\ 11)$	77	

- $n = 142$ $(DG : 3, 5, 11, 29, 41, 53, 59, 71)$

  $n = 2.71$.
  $n/2 = 71$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 10\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		137 (p)	
11 (p)	0 $(mod\ 11)$		131 (p)	
17 (p)		0 $(mod\ 5)$	125	
23 (p)		0 $(mod\ 7)$	119	
29 (p)			113 (p)	$29 + 113$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		107 (p)	
41 (p)			101 (p)	$41 + 101$
47 (p)		0 $(mod\ 5)$	95	
53 (p)			89 (p)	$53 + 89$
59 (p)			83 (p)	$59 + 83$
65	0 $(mod\ 5)$	0 $(mod\ 7)$ et0 $(mod\ 11)$	77	
71 (p)			71 (p)	$71 + 71$

- $n = 140$ $(DG : 3, 13, 31, 37, 43, 61, 67)$

  $n = 2^2.5.7.$
  $n/2 = 70.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 8\ (mod\ 11).$

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	133	
13 (p)			127 (p)	$13 + 127$
19 (p)		0 $(mod\ 11)$	121	
25	0 $(mod\ 5)$	0 $(mod\ 5)$	115	
31 (p)			109 (p)	$31 + 109$
37 (p)			103 (p)	$37 + 103$
43 (p)			97 (p)	$43 + 97$
49	0 $(mod\ 7)$	0 $(mod\ 7)$	91	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	85	
61 (p)			79 (p)	$61 + 79$
67 (p)			73 (p)	$67 + 73$

- $n = 138$ $(DG : 7, 11, 29, 31, 37, 41, 59, 67)$

  $n = 2.3.23.$
  $n/2 = 69.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 6\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$	0 $(mod\ 7)$	133	
11 (p)	0 $(mod\ 11)$		127 (p)	
17 (p)		0 $(mod\ 11)$	121	
23 (p)		0 $(mod\ 5)$	115	
29 (p)			109 (p)	$29 + 109$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		103 (p)	
41 (p)			97 (p)	$41 + 97$
47 (p)		0 $(mod\ 7)$	91	
53 (p)		0 $(mod\ 5)$	85	
59			79 (p)	$59 + 79$
65	0 $(mod\ 5)$		73 (p)	

7 (p)	0 $(mod\ 7)$		131 (p)	
13 (p)		0 $(mod\ 5)$	125	
19 (p)		0 $(mod\ 7)$	119	
25	0 $(mod\ 5)$		113 (p)	
31 (p)			107 (p)	$31 + 107$
37 (p)			101 (p)	$37 + 101$
43 (p)		0 $(mod\ 5)$	95	
49	0 $(mod\ 7)$		89 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		83 (p)	
61 (p)		0 $(mod\ 7)$ et 0 $(mod\ 11)$	77	
67			71 (p)	$67 + 71$

- $n = 136$ $(DG : 5, 23, 29, 47, 53)$

  $n = 2^3.17.$
  $n/2 = 68.$
  $11 < \sqrt{n} < 13.$ Les modules à considérer sont 5, 7 et 11.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 4\ (mod\ 11).$

5 (p)	0 $(mod\ 5)$		131 (p)	
11 (p)	0 $(mod\ 11)$	0 $(mod\ 5)$	125	
17 (p)		0 $(mod\ 7)$	119	
23 (p)			113 (p)	$23 + 113$
29 (p)			107 (p)	$29 + 107$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		101 (p)	
41 (p)		0 $(mod\ 5)$	95	
47 (p)			89 (p)	$47 + 89$
53 (p)			83 (p)	$53 + 83$
59 (p)		0 $(mod\ 7)$ et 0 $(mod\ 11)$	77	
65	0 $(mod\ 5)$		71 (p)	

- $n = 134$ $(DG : 3, 7, 31, 37, 61, 67)$

  $n = 2.67$.
  $n/2 = 67$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7), n \equiv 2\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$		127 (p)	
13 (p)		0 $(mod\ 11)$	121	
19 (p)		0 $(mod\ 5)$	115	
25	0 $(mod\ 5)$		109 (p)	
31 (p)			103 (p)	$31 + 103$
37 (p)			97 (p)	$37 + 97$
43 (p)		0 $(mod\ 7)$	91	
49	0 $(mod\ 7)$	0 $(mod\ 5)$	85	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		79 (p)	
61 (p)			73 (p)	$61 + 73$
67 (p)			67 (p)	$67 + 67$

- $n = 132$ $(DG : 5, 19, 23, 29, 31, 43, 53, 59, 61)$

  $n = 2^2.3.11$.
  $n/2 = 66$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7), n \equiv 0\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$		127 (p)	
11 (p)	0 $(mod\ 11)$	0 $(mod\ 11)$	121	
17 (p)		0 $(mod\ 5)$	115	
23 (p)			109 (p)	$23 + 109$
29 (p)			103 (p)	$29 + 103$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		97 (p)	
41 (p)		0 $(mod\ 7)$	91	
47 (p)		0 $(mod\ 5)$	85	
53 (p)			79 (p)	$53 + 79$
59 (p)			73 (p)	$59 + 73$
65	0 $(mod\ 5)$		67 (p)	

7 (p)	0 $(mod\ 7)$	0 $(mod\ 5)$	125	
13 (p)		0 $(mod\ 7)$	119	
19 (p)			113 (p)	$19 + 113$
25	0 $(mod\ 5)$		107 (p)	
31 (p)			101 (p)	$31 + 101$
37 (p)		0 $(mod\ 5)$	95	
43 (p)			89 (p)	$43 + 89$
49	0 $(mod\ 7)$		83 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 7)$ et 0 $(mod\ 11)$	77	
61 (p)			71 (p)	$61 + 71$

- $n = 130$ $(DG : 3, 17, 23, 29, 41, 47, 59)$

  $n = 2.5.13$.
  $n/2 = 65$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7), n \equiv 9\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	125	
11 (p)	0 $(mod\ 11)$	0 $(mod\ 7)$	119	
17 (p)			113 (p)	$17 + 113$
23 (p)			107 (p)	$23 + 107$
29 (p)			101 (p)	$29 + 101$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	95	
41 (p)			89 (p)	$41 + 89$
47 (p)			83 (p)	$47 + 83$
53 (p)		0 $(mod\ 7)$ et 0 $(mod\ 11)$	77	
59 (p)			71 (p)	$59 + 71$
65	0 $(mod\ 5)$	0 $(mod\ 5)$	65	

- $n = 128$ $(DG : 19, 31, 61)$

  $n = 2^7$.
  $n/2 = 64$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7), n \equiv 7\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 11)$	121	
13 (p)		0 $(mod\ 5)$	115	
19 (p)			109 (p)	$19 + 109$
25	0 $(mod\ 5)$		103 (p)	
31 (p)			97 (p)	$31 + 97$
37 (p)		0 $(mod\ 7)$	93	
43 (p)		0 $(mod\ 5)$	87	
49	0 $(mod\ 7)$		81	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		75	
61			69 (p)	$61 + 69$

- $n = 126$ $(DG : 13, 17, 19, 23, 29, 37, 43, 47, 53, 59)$

  $n = 2.3^2.7$.
  $n/2 = 63$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7), n \equiv 5\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 11)$	121	
11 (p)	0 $(mod\ 11)$	0 $(mod\ 5)$	115	
17 (p)			109 (p)	$17 + 109$
23 (p)			103 (p)	$23 + 103$
29 (p)			97 (p)	$29 + 97$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	91	
41 (p)		0 $(mod\ 5)$	85	
47 (p)			79 (p)	$47 + 79$
53 (p)			73 (p)	$53 + 73$
59 (p)			67 (p)	$59 + 67$

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	119	
13 (p)			113 (p)	$13 + 113$
19 (p)			107 (p)	$19 + 107$
25	0 $(mod\ 5)$		101 (p)	
31 (p)		0 $(mod\ 5)$	95	
37 (p)			89 (p)	$37 + 89$
43 (p)			83 (p)	$43 + 83$
49	0 $(mod\ 7)$	0 $(mod\ 7)$ et 0 $(mod\ 11)$	77	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		71 (p)	
61 (p)		0 $(mod\ 5)$	65	

- $n = 124$ $(DG : 11, 17, 23, 41, 53)$

  $n = 2^2.31$.
  $n/2 = 62$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7), n \equiv 3\ (mod\ 11)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 7)$	119	
11 (p)	0 $(mod\ 11)$		113 (p)	
17 (p)			107 (p)	$17 + 107$
23 (p)			101 (p)	$23 + 101$
29 (p)		0 $(mod\ 5)$	95	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		89 (p)	
41 (p)			83 (p)	$41 + 83$
47 (p)		0 $(mod\ 7)$ *et* 0 $(mod\ 11)$	77	
53 (p)			71 (p)	$53 + 71$
59 (p)		0 $(mod\ 5)$	65	

- $n = 122$ $(DG : 13, 19, 43, 61)$

  $n = 2.61$.
  $n/2 = 61$.
  $11 < \sqrt{n} < 13$. Les modules à considérer sont 5, 7 et 11.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7), n \equiv 1\ (mod\ 11)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 5)$	115	
13 (p)			109 (p)	$13 + 109$
19 (p)			103 (p)	$19 + 103$
25	0 $(mod\ 5)$		97 (p)	
31 (p)		0 $(mod\ 7)$	91	
37 (p)		0 $(mod\ 5)$	85	
43 (p)			79 (p)	$43 + 79$
49	0 $(mod\ 7)$		73 (p)	
55	0 $(mod\ 5)$		67 (p)	
61 (p)			61 (p)	$61 + 61$

- $n = 120$ $(DG : 7, 11, 13, 17, 19, 23, 31, 37, 41, 47, 53, 59)$

  $n = 2^3.3.5$.
  $n/2 = 60$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	115	
11 (p)			109 (p)	$11 + 109$
17 (p)			103 (p)	$17 + 103$
23 (p)			97 (p)	$23 + 97$
29 (p)		0 $(mod\ 7)$	91	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	85	
41 (p)			79 (p)	$41 + 79$
47 (p)			73 (p)	$47 + 73$
53 (p)			67 (p)	$53 + 67$
59 (p)			61 (p)	$59 + 61$

7 (p)	0 $(mod\ 7)$		113 (p)	
13 (p)			107 (p)	$13 + 107$
19 (p)			101 (p)	$19 + 101$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	95	
31 (p)			89 (p)	$31 + 89$
37 (p)			83 (p)	$37 + 83$
43 (p)		0 $(mod\ 7)$	77 (p)	
49	0 $(mod\ 7)$		71 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	65	

- $n = 118$ $(DG : 5, 11, 17, 29, 47, 59)$

  $n = 2.59$.
  $n/2 = 59$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		113 (p)	
11 (p)			107 (p)	$11 + 107$
17 (p)			101 (p)	$17 + 101$
23 (p)		0 $(mod\ 5)$	95	
29 (p)			89 (p)	$29 + 89$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		83 (p)	
41 (p)		0 $(mod\ 7)$	77	
47 (p)			71 (p)	$47 + 71$
53 (p)		0 $(mod\ 5)$	65	
59 (p)			59 (p)	$59 + 59$

- $n = 116$ $(DG : 3, 7, 13, 19, 37, 43)$

  $n = 2^2.29$.
  $n/2 = 58$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		109 (p)	
13 (p)			103 (p)	$13 + 103$
19 (p)			97 (p)	$19 + 97$
25	0 $(mod\ 5)$	0 $(mod\ 7)$	91	
31 (p)		0 $(mod\ 5)$	85	
37 (p)			79 (p)	$37 + 79$
43 (p)			73 (p)	$43 + 73$
49	0 $(mod\ 7)$		67	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		61 (p)	

- $n = 114$ $(DG : 5, 7, 11, 13, 17, 31, 41, 43, 47, 53)$

  $n = 2.3.19$.
  $n/2 = 57$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		109 (p)	
11 (p)			103 (p)	$11 + 103$
17 (p)			97 (p)	$17 + 97$
23 (p)		0 $(mod\ 7)$	91	
29 (p)		0 $(mod\ 5)$	85	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		79 (p)	
41 (p)			73 (p)	$41 + 73$
47 (p)			67 (p)	$47 + 67$
53 (p)			61 (p)	$53 + 61$

7 (p)	0 $(mod\ 7)$		107 (p)	
13 (p)			101 (p)	$13 + 101$
19 (p)		0 $(mod\ 5)$	95	
25	0 $(mod\ 5)$		89 (p)	
31 (p)			83 (p)	$31 + 83$
37 (p)		0 $(mod\ 7)$	77	
43 (p)			71 (p)	$43 + 71$
49	0 $(mod\ 7)$	0 $(mod\ 5)$	65	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$		59 (p)	

- $n = 112$ $(DG : 3, 5, 11, 23, 29, 41, 53)$

  $n = 2^4.7$.
  $n/2 = 56$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		107 (p)	
11 (p)			101 (p)	$11 + 101$
17 (p)		0 $(mod\ 5)$	95	
23 (p)			89 (p)	$23 + 89$
29 (p)			83 (p)	$29 + 83$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	77	
41 (p)			71 (p)	$41 + 71$
47 (p)		0 $(mod\ 5)$	65	
53 (p)			59 (p)	$53 + 59$

- $n = 110$ $(DG : 3, 7, 13, 31, 37, 43)$

  $n = 2.5.11$.
  $n/2 = 55$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		103 (p)	
13 (p)			97 (p)	$13 + 97$
19 (p)		0 $(mod\ 7)$	91	
25	0 $(mod\ 5)$	0 $(mod\ 5)$	85	
31 (p)			79 (p)	$31 + 79$
37 (p)			73 (p)	$37 + 73$
43 (p)			67 (p)	$43 + 67$
49	0 $(mod\ 7)$		61 (p)	
55	0 $(mod\ 5)$ et 0 $(mod\ 11)$	0 $(mod\ 5)$	55	

- $n = 108$ $(DG : 5, 7, 11, 19, 29, 37, 41, 47)$

  $n = 2^2.3^3$.
  $n/2 = 54$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		103 (p)	
11 (p)			97 (p)	$11 + 97$
17 (p)		0 $(mod\ 7)$	91	
23 (p)		0 $(mod\ 5)$	85	
29 (p)			79 (p)	$29 + 79$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		73 (p)	
41 (p)			67 (p)	$41 + 67$
47 (p)			61 (p)	$47 + 61$
53 (p)		0 $(mod\ 5)$	55	

7 (p)	0 $(mod\ 7)$		101 (p)	
13 (p)		0 $(mod\ 5)$	95	
19 (p)			89 (p)	$19 + 89$
25	0 $(mod\ 5)$		83 (p)	
31 (p)		0 $(mod\ 7)$	77	
37 (p)			71 (p)	$37 + 71$
43 (p)		0 $(mod\ 5)$	65	
49	0 $(mod\ 7)$		59 (p)	

- $n = 106$ $(DG : 3, 5, 17, 23, 47, 53)$

  $n = 2.53$.
  $n/2 = 53$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		101 (p)	
11 (p)		0 $(mod\ 5)$	95	
17 (p)			89 (p)	$17 + 89$
23 (p)			83 (p)	$23 + 83$
29 (p)		0 $(mod\ 7)$	77	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		71 (p)	
41 (p)		0 $(mod\ 5)$	65	
47 (p)			59 (p)	$47 + 59$
53 (p)			53 (p)	$53 + 53$

- $n = 104$ $(DG : 3, 7, 31, 37, 43)$

  $n = 2^3.13$.
  $n/2 = 52$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		97 (p)	
13 (p)		0 $(mod\ 7)$	91	
19 (p)		0 $(mod\ 5)$	85	
25	0 $(mod\ 5)$		79 (p)	
31 (p)			73 (p)	$31 + 73$
37 (p)			67 (p)	$37 + 67$
43 (p)			61 (p)	$43 + 61$
49	0 $(mod\ 7)$	0 $(mod\ 5)$	55	

- $n = 102$ $(DG : 5, 13, 19, 23, 29, 31, 41, 43)$

  $n = 2.3.17$.
  $n/2 = 51$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		97 (p)	
11 (p)		0 $(mod\ 7)$	91	
17 (p)		0 $(mod\ 5)$	85	
23 (p)			79 (p)	$23 + 79$
29 (p)			73 (p)	$29 + 73$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		67 (p)	
41 (p)			61 (p)	$41 + 61$
47 (p)		0 $(mod\ 5)$	55	

7 (p)	0 $(mod\ 7)$	0 $(mod\ 5)$	95	
13 (p)			89 (p)	$13 + 89$
19 (p)			83 (p)	$19 + 83$
25	0 $(mod\ 5)$	0 $(mod\ 7)$	77	
31 (p)			71 (p)	$31 + 71$
37 (p)		0 $(mod\ 5)$	65	
43 (p)			59 (p)	$43 + 59$
49	0 $(mod\ 7)$		53 (p)	

- $n = 100$ $(DG : 3, 11, 17, 29, 41, 47)$

  $n = 2^2.5^2$.
  $n/2 = 50$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	95	
11 (p)			89 (p)	$11 + 89$
17 (p)			83 (p)	$17 + 83$
23 (p)		0 $(mod\ 7)$	77	
29 (p)			71 (p)	$29 + 71$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	65	
41 (p)			59 (p)	$41 + 59$
47 (p)			53 (p)	$47 + 53$

- $n = 98$ $(DG : 19, 31, 37)$

  $n = 2.7^2$.
  $n/2 = 49$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	91	
13 (p)		0 $(mod\ 5)$	85	
19 (p)			79 (p)	$19 + 79$
25	0 $(mod\ 5)$		73	
31 (p)			67 (p)	$31 + 67$
37 (p)			61 (p)	$37 + 61$
43 (p)		0 $(mod\ 5)$	55	
49	0 $(mod\ 7)$	0 $(mod\ 7)$	49	

- $n = 96$ $(DG : 7, 13, 17, 23, 29, 37, 43)$

  $n = 2^5.3$.
  $n/2 = 48$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 7)$	91	
11 (p)		0 $(mod\ 5)$	85	
17 (p)			79 (p)	$17 + 79$
23 (p)			73 (p)	$23 + 73$
29 (p)			67 (p)	$29 + 67$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		61 (p)	
41 (p)		0 $(mod\ 5)$	55	
47 (p)		0 $(mod\ 7)$	49	

7 (p)	0 $(mod\ 7)$		89 (p)	
13 (p)			83 (p)	$13 + 83$
19 (p)		0 $(mod\ 7)$	77	
25	0 $(mod\ 5)$		71 (p)	
31 (p)		0 $(mod\ 5)$	65	
37 (p)			59 (p)	$37 + 59$
43 (p)			53 (p)	$43 + 53$

- $n = 94$ $(DG : 5, 11, 23, 41, 47)$

  $n = 2.47$.
  $n/2 = 47$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		89 (p)	
11 (p)			83 (p)	$11 + 83$
17 (p)		0 $(mod\ 7)$	77	
23 (p)			71 (p)	$23 + 71$
29 (p)		0 $(mod\ 5)$	65	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		59 (p)	
41 (p)			53 (p)	$41 + 53$
47 (p)			47 (p)	$47 + 47$

- $n = 92$ $(DG : 3, 13, 19, 31)$

  $n = 2^2.23$.
  $n/2 = 46$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 5)$	87	
13 (p)			81 (p)	$13 + 81$
19 (p)			75 (p)	$19 + 75$
25	0 $(mod\ 5)$		69	
31 (p)			63 (p)	$31 + 63$
37 (p)		0 $(mod\ 5)$	57 (p)	
43 (p)		0 $(mod\ 7)$	51	

- $n = 90$ $(DG : 7, 11, 17, 19, 23, 29, 31, 37, 43)$

  $n = 2.3^2.5$.
  $n/2 = 45$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	85	
11 (p)			79 (p)	$11 + 79$
17 (p)			73 (p)	$17 + 73$
23 (p)			67 (p)	$23 + 67$
29 (p)			61 (p)	$29 + 61$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$	55	
41 (p)		0 $(mod\ 7)$	49	

7 (p)	0 $(mod\ 7)$		83 (p)	
13 (p)		0 $(mod\ 7)$	77	
19 (p)			71 (p)	$19 + 71$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	65	
31 (p)			59 (p)	$31 + 59$
37 (p)			53 (p)	$37 + 53$
43 (p)			47 (p)	$43 + 47$

- $n = 88$ $(DG : 5, 17, 29, 41)$

  $n = 2^3.11$.
  $n/2 = 44$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		83 (p)	
11 (p)		0 $(mod\ 7)$	77	
17 (p)			71 (p)	$17 + 71$
23 (p)		0 $(mod\ 5)$	65	
29 (p)			59 (p)	$29 + 59$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		53 (p)	
41 (p)			47 (p)	$41 + 47$

- $n = 86$ $(DG : 3, 7, 13, 19, 43)$

  $n = 2.43$.
  $n/2 = 43$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		79 (p)	
13 (p)			73 (p)	$13 + 73$
19 (p)			67 (p)	$19 + 67$
25	0 $(mod\ 5)$		61 (p)	
31 (p)		0 $(mod\ 5)$	55	
37 (p)		0 $(mod\ 7)$	49	
43 (p)			43 (p)	$43 + 43$

- $n = 84$ $(DG : 5, 11, 13, 17, 23, 31, 37, 41)$

  $n = 2^2.3.7$.
  $n/2 = 42$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		79 (p)	
11 (p)			73 (p)	$11 + 73$
17 (p)			67 (p)	$17 + 67$
23 (p)			61 (p)	$23 + 61$
29 (p)		0 $(mod\ 5)$	55	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 7)$	49	
41 (p)			43 (p)	$41 + 43$

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	77	
13 (p)			71 (p)	$13 + 71$
19 (p)		0 $(mod\ 5)$	65	
25	0 $(mod\ 5)$		59 (p)	
31 (p)			53 (p)	$31 + 53$
37 (p)			47 (p)	$37 + 47$

- $n = 82$ $(DG : 3, 11, 23, 29, 41)$

  $n = 2.41$.
  $n/2 = 41$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 7)$	77	
11 (p)			71 (p)	$11 + 71$
17 (p)		0 $(mod\ 5)$	65	
23 (p)			59 (p)	$23 + 59$
29 (p)			53 (p)	$29 + 53$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		47 (p)	
41 (p)			41 (p)	$41 + 41$

- $n = 80$ $(DG : 7, 13, 19, 37)$

  $n = 2^4.5$.
  $n/2 = 40$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		73 (p)	
13 (p)			67 (p)	$13 + 67$
19 (p)			61 (p)	$19 + 61$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	55	
31 (p)		0 $(mod\ 7)$	49	
37 (p)			43 (p)	$37 + 43$

- $n = 78$ $(DG : 5, 7, 11, 17, 19, 31, 37)$

  $n = 2.3.13$.
  $n/2 = 39$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		73 (p)	
11 (p)			67 (p)	$11 + 67$
17 (p)			61 (p)	$17 + 61$
23 (p)		0 $(mod\ 5)$	55	
29 (p)		0 $(mod\ 7)$	49	
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		43 (p)	

7 (p)	0 $(mod\ 7)$		71 (p)	
13 (p)		0 $(mod\ 5)$	65	
19 (p)			59 (p)	$19 + 59$
25	0 $(mod\ 5)$		53 (p)	
31 (p)			47 (p)	$31 + 47$
37 (p)			41 (p)	$37 + 41$

- $n = 76$ $(DG : 3, 5, 17, 23, 29)$

  $n = 2^2.19$.
  $n/2 = 38$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		71 (p)	
11 (p)		0 $(mod\ 5)$	65	
17 (p)			59 (p)	$17 + 59$
23 (p)			53 (p)	$23 + 53$
29 (p)			47 (p)	$29 + 47$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		41 (p)	

- $n = 74$ $(DG : 3, 7, 13, 31, 37)$

  $n = 2.37$.
  $n/2 = 37$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		67 (p)	
13 (p)			61 (p)	$13 + 61$
19 (p)		0 $(mod\ 5)$	55	
25	0 $(mod\ 5)$	0 $(mod\ 7)$	49	
31 (p)			43 (p)	$31 + 43$
37 (p)			37 (p)	$37 + 37$

- $n = 72$ $(DG : 5, 11, 13, 19, 29, 31)$

  $n = 2^3.3^2$.
  $n/2 = 36$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		67 (p)	
11 (p)			61 (p)	$11 + 61$
17 (p)		0 $(mod\ 5)$	55	
23 (p)		0 $(mod\ 7)$	49	
29 (p)			43 (p)	$29 + 43$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$		37 (p)	

7 (p)	0 $(mod\ 7)$	0 $(mod\ 5)$	65	
13 (p)			59 (p)	$13 + 59$
19 (p)			53 (p)	$19 + 53$
25	0 $(mod\ 5)$		47 (p)	
31 (p)			41 (p)	$31 + 41$

- $n = 70$ $(DG : 3, 11, 17, 23, 29)$

  $n = 2.5.7$.
  $n/2 = 35$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	65	
11 (p)			59 (p)	$11 + 59$
17 (p)			53 (p)	$17 + 53$
23 (p)			47 (p)	$23 + 47$
29 (p)			41 (p)	$29 + 41$
35	0 $(mod\ 5)$ et 0 $(mod\ 7)$	0 $(mod\ 5)$ et 0 $(mod\ 7)$	35	

- $n = 68$ $(DG : 7, 31)$

  $n = 2^2.17$.
  $n/2 = 34$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		61 (p)	
13 (p)		0 $(mod\ 5)$	55	
19 (p)		0 $(mod\ 7)$	49	
25	0 $(mod\ 5)$		43 (p)	
31 (p)			37 (p)	$31 + 37$

- $n = 66$ $(DG : 5, 7, 13, 19, 23, 29)$

  $n = 2.3.11$.
  $n/2 = 33$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		61 (p)	
11 (p)		0 $(mod\ 5)$	55	
17 (p)		0 $(mod\ 7)$	49	
23 (p)			43 (p)	$23 + 43$
29 (p)			37 (p)	$29 + 37$

7 (p)	0 $(mod\ 7)$		59 (p)	
13 (p)			53 (p)	$13 + 53$
19 (p)			47 (p)	$19 + 47$
25	0 $(mod\ 5)$		41 (p)	
31 (p)		0 $(mod\ 5)$ et 0 $(mod\ 7)$	35	

- $n = 64$ $(DG : 3, 5, 11, 17, 23)$

  $n = 2^6$.
  $n/2 = 32$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		59 (p)	
11 (p)			53 (p)	$11 + 53$
17 (p)			47 (p)	$17 + 47$
23 (p)			41 (p)	$23 + 41$
29 (p)		0 $(mod\ 5)$ *et* 0 $(mod\ 7)$	35	

- $n = 62$ $(DG : 3, 19, 31)$

  $n = 2.31$.
  $n/2 = 31$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 6\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 5)$	55	
13 (p)		0 $(mod\ 7)$	49	
19 (p)			43 (p)	$19 + 43$
25	0 $(mod\ 5)$		37 (p)	
31 (p)			31 (p)	$31 + 31$

- $n = 60$ $(DG : 7, 13, 17, 19, 23, 29)$

  $n = 2^2.3.5$.
  $n/2 = 30$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 4\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	55	
11 (p)		0 $(mod\ 7)$	49	
17 (p)			43 (p)	$17 + 43$
23 (p)			37 (p)	$23 + 37$
29 (p)			31 (p)	$29 + 31$

7 (p)	0 $(mod\ 7)$		53 (p)	
13 (p)			47 (p)	$13 + 47$
19 (p)			41 (p)	$19 + 41$
25	0 $(mod\ 5)$	0 $(mod\ 7)$ et 0 $(mod\ 5)$	35	

- $n = 58$ $(DG : 5, 11, 17, 29)$

  $n = 2.29$.
  $n/2 = 29$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 3\ (mod\ 5), n \equiv 2\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		53 (p)	
11 (p)			47 (p)	$11 + 47$
17 (p)			41 (p)	$17 + 41$
23 (p)		0 $(mod\ 5)$ *et* 0 $(mod\ 7)$	35	
29 (p)			29 (p)	$29 + 29$

- $n = 56$ $(DG : 3, 13, 19)$

  $n = 2^3.7$.
  $n/2 = 28$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 1\ (mod\ 5), n \equiv 0\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$	0 $(mod\ 7)$	49	
13 (p)			43 (p)	$13 + 43$
19 (p)			37 (p)	$19 + 37$
25	0 $(mod\ 5)$		31	

- $n = 54$ $(DG : 7, 11, 13, 17, 23)$

  $n = 2.3^3$.
  $n/2 = 27$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 4\ (mod\ 5), n \equiv 5\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 7)$	49	
11 (p)			43 (p)	$11 + 43$
17 (p)			37 (p)	$17 + 37$
23 (p)			31 (p)	$23 + 31$

7 (p)	0 $(mod\ 7)$		47 (p)	
13 (p)			41 (p)	$13 + 41$
19 (p)		0 $(mod\ 5)$ et 0 $(mod\ 7)$	35	
25	0 $(mod\ 5)$		29	

- $n = 52$ $(DG : 5, 11, 23)$

  $n = 2^2.13$.
  $n/2 = 26$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 2\ (mod\ 5), n \equiv 3\ (mod\ 7)$.

5 (p)	0 $(mod\ 5)$		47 (p)	
11 (p)			41 (p)	$11 + 41$
17 (p)		0 $(mod\ 5)$ *et* 0 $(mod\ 7)$	35	
23 (p)			29 (p)	$23 + 29$

- $n = 50$ $(DG : 3, 7, 13, 19)$

  $n = 2.5^2$.
  $n/2 = 25$.
  $7 < \sqrt{n} < 11$. Les modules à considérer sont 5 et 7.
  $n \equiv 0\ (mod\ 5), n \equiv 1\ (mod\ 7)$.

7 (p)	0 $(mod\ 7)$		43 (p)	
13 (p)			37 (p)	$13 + 37$
19 (p)			31 (p)	$19 + 31$
25	0 $(mod\ 5)$	0 $(mod\ 5)$	25	

- $n = 48$ $(DG : 5, 7, 11, 17, 19)$

  $n = 2^4.3$.
  $n/2 = 24$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		43 (p)	
11 (p)			37 (p)	$11 + 37$
17 (p)			31 (p)	$17 + 31$
23 (p)		0 $(mod\ 5)$	25	

7 (p)			41 (p)	$7 + 41$
13 (p)		0 $(mod\ 5)$	35	
19 (p)			29 (p)	$19 + 29$

- $n = 46$ $(DG : 3, 5, 17, 23)$

  $n = 2.23$.
  $n/2 = 23$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		41 (p)	
11 (p)		0 $(mod\ 5)$	35	
17 (p)			29 (p)	$17 + 29$
23 (p)			23 (p)	$23 + 23$

- $n = 44$ $(DG : 3, 7, 13)$

  $n = 2^2.11$.
  $n/2 = 22$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 4\ (mod\ 5)$.

7 (p)			37 (p)	
13 (p)			31 (p)	$13 + 31$
19 (p)		0 $(mod\ 5)$	25	

- $n = 42$ $(DG : 5, 11, 13, 19)$

  $n = 2.3.7$.
  $n/2 = 21$.
  $5 < \sqrt{n} < 5$. Le module à considérer est 5.
  $n \equiv 2\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		37 (p)	
11 (p)			31 (p)	$11 + 31$
17 (p)		0 $(mod\ 5)$	25	
7 (p)		0 $(mod\ 5)$	35	
13 (p)			29 (p)	$13 + 29$
19 (p)			23 (p)	$19 + 23$

- $n = 40$ $(DG : 3, 11, 17)$

  $n = 2^3.5$.
  $n/2 = 20$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	35	
11 (p)			29 (p)	$11 + 29$
17 (p)			23 (p)	$17 + 23$

- $n = 38$ $(DG : 7, 19)$

  $n = 2.19$.
  $n/2 = 19$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

7 (p)			31 (p)	
13 (p)		0 $(mod\ 5)$	25	
19			19 (p)	$19 + 19$

- $n = 36$ $(DG : 5, 7, 13, 17)$

  $n = 2^2.3^2$.
  $n/2 = 18$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		31 (p)	
11 (p)		0 $(mod\ 5)$	25	
17 (p)			19 (p)	$17 + 19$
7 (p)			29 (p)	$7 + 29$
13 (p)			23 (p)	$13 + 23$

- $n = 34$ $(DG : 3, 5, 11, 17)$

  $n = 2.17$.
  $n/2 = 17$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 4\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		29 (p)	
11 (p)			23 (p)	$11 + 23$
17 (p)			17 (p)	$17 + 17$

- $n = 32$ $(DG : 3, 13)$

  $n = 2^5$.
  $n/2 = 16$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 2\ (mod\ 5)$.

7 (p)		0 $(mod\ 5)$	25	
13			19 (p)	$13 + 19$

- $n = 30$ $(DG : 7, 11, 13)$

  $n = 2.3.5$.
  $n/2 = 15$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 0\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$	0 $(mod\ 5)$	25	
11 (p)			19 (p)	$11 + 19$
7 (p)			23 (p)	$7 + 23$
13 (p)			17 (p)	$13 + 17$

- $n = 28$ $(DG : 5, 11)$

  $n = 2^2.7$.
  $n/2 = 14$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 3\ (mod\ 5)$.

5 (p)	0 $(mod\ 5)$		23	
11 (p)			17 (p)	$11 + 17$

- $n = 26$ $(DG : 3, 7, 13)$

  $n = 2.13$.
  $n/2 = 13$.
  $5 < \sqrt{n} < 7$. Le module à considérer est 5.
  $n \equiv 1\ (mod\ 5)$.

7 (p)			19 (p)	
13			13 (p)	$13 + 13$

Tentative inaboutie de démonstration par récurrence de la conjecture de Goldbach

Denise Vella-Chemla

1/12/12

1 Introduction

On cherche à démontrer que la conjecture de Goldbach est vérifiée par tout nombre pair supérieur à 6. Cette conjecture stipule que tout nombre pair supérieur à 2 est la somme de deux nombres premiers.
Un décomposant de Goldbach d'un nombre pair donné x doit vérifier deux propriétés : la première est qu'il doit être premier, la seconde est qu'il ne doit être congru à x selon aucun nombre premier inférieur ou égal à $\sqrt{x}$, ce qui garantit que son complémentaire à x est premier également.
Notons $\mathbb{P}$ l'ensemble des nombres premiers :

$$\mathbb{P} = \{p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots\}$$

remarque : $1 \notin \mathbb{P}$
Notons certaines parties de l'ensemble des nombres premiers de la façon suivante :

$$\mathbb{P}(y) = \{x \in \mathbb{P} / x \leq y\}$$

La conjecture de Goldbach est équivalente à :

$$\begin{array}{l} \forall n \in 2\mathbb{N}, n > 4, \exists p \in \mathbb{P}(n/2), \forall m \in \mathbb{P}(\sqrt{n}), \\ \quad p \not\equiv n \ (mod\ m) \end{array}$$

Car :

$$\begin{array}{l} \forall n \in 2\mathbb{N}, n > 4, \exists p \in \mathbb{P}(n/2), \forall m \in \mathbb{P}(\sqrt{n}), \\ \quad p \not\equiv n \ (mod\ m) \Leftrightarrow n - p \not\equiv 0 \ (mod\ m) \Leftrightarrow n - p \ premier \end{array}$$

On se servira dans la démonstration du fait que x et $x + 6$ ont les mêmes restes (sont congrus) selon les modules 2 et 3.

Remarques peut-être utiles :
On peut considérer trois sortes de nombres pairs : les $6k$, les $6k+2$ et les $6k+4$. Un $6k$ ne peut être un $2p$ avec p premier ; les $2p$ présentent la particularité qu'ils vérifient trivialement la conjecture de Goldbach.
Un $6k$ est la somme d'un $6k' + 1$ et d'un $6k'' - 1$.
Un $6k + 2$ est la somme d'un $6k' + 1$ et d'un $6k'' + 1$.
Un $6k + 4$ est la somme d'un $6k' - 1$ et d'un $6k'' - 1$.
Les nombres de la progression arithmétique $6k+1$ sont alternativement de la forme $4n+1$ et $4n+3$. Il en est de même des nombres de la progression arithmétique $6k - 1$. Le produit de deux nombres de la forme $4n + 3$ est un $4n + 1$. De même du produit de deux nombres de la forme $4n + 1$.
Le produit d'un nombre de la forme $4n + 1$ par un nombre de la forme $4n + 3$ est un $4n + 3$.
Les considérations ci-dessus pour les formes selon le module 4 peuvent être intéressantes en cas d'utilisation de la loi de réciprocité quadratique.

2 Démonstration par récurrence

On doit noter que le nombre de modules inférieurs ou égaux à $\sqrt{x}$ est égal au nombre de modules inférieurs ou égaux à $\sqrt{x+6}$ dans la plupart des cas. Il y a cependant trois possibilités de nombres pour lesquels cela n'est pas le cas, lorsque $x+6$ est de la forme $p^2+1,\ p^2+3$ *ou encore* p^2+5.

1) *Premier cas* : il y a autant de modules inférieurs ou égaux à $\sqrt{x}$ que de modules inférieurs ou égaux à $\sqrt{x+6}$.
Hypothèse : on a trouvé une décomposition de Goldbach de x, i.e. on a trouvé pour x un nombre premier p tel que $x = p+q$ avec q premier également. p vérifie donc les deux propriétés d'être premier et de n'être congru à x selon aucun des modules premiers inférieurs ou égaux à $\sqrt{x}$ (peut-être vaut-il mieux considérer qu'on a trouvé une décomposition de Goldbach pour chaque entier compris entre 6 et x, ces décompositions pouvant ou non partager leur premier décomposant.)
Mais alors p est également incongru à $x+6$ selon tout module inférieur ou égal à $\sqrt{x+6}$ (faux : cela n'est vrai que pour les modules 2 et 3 et il faut réfléchir pour les modules plus grands car x et $x+6$ ne partagent pas leurs restes selon les modules premiers supérieurs ou égaux à 5 et donc p peut très bien n'être congru à x selon aucun module inférieur à $\sqrt{x}$ mais l'être à $x+6$ selon les modules en question).
Conclusion : on a donc trouvé une décomposition de $x+6$, i.e. on a trouvé pour $x+6$ un nombre premier p tel que $x+6 = p+q'$ avec q' premier également.

1) *Deuxième, troisième et quatrième cas* : il y a un module de plus à considérer car $x+6$ est de la forme $p^2+1,\ p^2+3$ *ou encore* p^2+5.

Annexe : les partages des décomposants de Goldbach entre les nombres pairs x et $x+6$ pour les nombres de 8 à 100

Faisons apparaître dans le tableau ci-dessous les trois progressions arithmétiques de 6 en 6 à partir de 8, 10 ou 12 dont les nombres x partagent systématiquement un décomposant de Goldbach avec $x+6$. Les premières lignes du tableau concernent la première progression arithmétique contenant les nombres de la forme $8+6k$ (ou $6k+2$) et les décomposants partagés par un nombre et son successeur dans cette progression dans les lignes qui suivent. Les lignes 5 et suivantes concernent les nombres de la progression arithmétique $10+6k$ (ou $6k+4$) et les lignes 8 et suivantes concernent ceux de la progression $12+6k$ (ou $6k$).

8	14	20	26	32	38	44	50	56	62	68	74	80	86	92	98
3	3	3	3	3		3	3	3	3		3		3	3	
				7	7	7			31	31	31			19	19
											7	7	7		
10	16	22	28	34	40	46	52	58	64	70	76	82	88	94	100
3	3	3		3	3	3			3	3	3	3			3
		5	5	5		5	5	5	5			41	41	41	41
12	18	24	30	36	42	48	54	60	66	72	78	84	90	96	
5	5	5		5	5	5			5	5	5	5			
		7	7	7		7	7	7	7			17	17	17	

La conjecture : "x supérieur à 6 partage toujours un décomposant de Goldbach avec $x+6$" (i.e. $x = p+q, x+6 = p+q'$ *avec* $p,\ q$ *et* q' *premiers*) a été vérifiée par ordinateur jusqu'à 16.10^8. Elle s'explique par le fait qu'un des nombres premiers décomposants de Goldbach de x étant non congru à x selon tout module inférieur à $\sqrt{x}$, aura vraiment toutes les chances d'être également non congru à $x+6$ selon tout module inférieur à $\sqrt{x+6}$.

Conjecture de Goldbach (7 juin 1742)

- On note $\mathbb{P}$ l'ensemble des nombres premiers.
  $\mathbb{P} = \{p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots\}$
- *remarque* : $1 \notin \mathbb{P}$
- **Énoncé :**
  Tout entier pair supérieur à 2 est la somme de deux nombres premiers.
  $\forall n \in 2\mathbb{N}, n > 2, \exists p, q \in \mathbb{P}, n = p + q$
- La conjecture de Goldbach a été vérifiée par ordinateur jusqu'à 4.10^{18}
  (Oliveira e Silva, 4.4.2012)
- On appelle *décomposition de Goldbach* de n une telle somme $p + q$.
  p et q sont dits *décomposants de Goldbach* de n.

Reformulation

- Notons $\mathbb{P}(y) = \{x \in \mathbb{P} / x \leq y\}$
- La conjecture de Goldbach est équivalente à l'énoncé suivant :

$$\forall n \in 2\mathbb{N}, n > 4, \exists p \in \mathbb{P}(n/2), \forall m \in \mathbb{P}(\sqrt{n}), \\ p \not\equiv n \ (mod\ m)$$

- En effet,

$$\forall n \in 2\mathbb{N}, n > 4, \exists p \in \mathbb{P}(n/2), \forall m \in \mathbb{P}(\sqrt{n}), \\ p \not\equiv n \ (mod\ m) \Leftrightarrow n - p \not\equiv 0 \ (mod\ m) \Leftrightarrow n - p \ premier$$

Étude d'un exemple

- *Pourquoi 19 est-il le plus petit décomposant de Goldbach de 98 ?*

$$98 \equiv 3 \pmod 5$$
$$98 \equiv 5 \pmod 3$$
$$98 \equiv 7 \pmod 7$$
$$98 \equiv 11 \pmod 3$$
$$98 \equiv 13 \pmod 5$$
$$98 \equiv 17 \pmod 3$$

$$98 \not\equiv 19 \pmod 3$$
$$98 \not\equiv 19 \pmod 5$$
$$98 \not\equiv 19 \pmod 7$$

- *Conclusion* : $\forall m \in \mathbb{P}(\sqrt{98}),\ 19 \not\equiv 98\ (mod\ m)$
  19 est un décomposant de Goldbach de 98.
  En effet, $98 = 19 + 79$ avec 19 et 79 premiers.

Une seconde façon de représenter l'exemple proposé

- *Pourquoi 19 est-il un décomposant de Goldbach de 98 ?*

$\mathbb{Z}/3\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$			
$\mathbb{Z}/5\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	
$\mathbb{Z}/7\mathbb{Z}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$

Classe d'appartenance de 19,

Classe d'appartenance de 98.

- *Conclusion* : $\forall m \in \mathbb{P}(\sqrt{98}),\ 19 \not\equiv 98\ (mod\ m)$
  19 est un décomposant de Goldbach de 98.
  En effet, $98 = 19 + 79$ avec 19 et 79 premiers.

On cherche à démontrer l'impossibilité de l'existence d'un entier pair qui ne vérifie pas la conjecture de Goldbach

$(\exists x \in 2\mathbb{N},\ x \geq 20, x$ *ne vérifie pas la conjecture de Goldbach*$)$
$\Rightarrow$ *false*

mais
$\exists x \in 2\mathbb{N},\ x \geq 20, x$ *ne vérifie pas la conjecture de Goldbach*

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),$
x-p composé

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),\ \exists m \in \mathbb{P}(\sqrt{x}),$
x-p $\equiv 0\ (mod\ m)$

$\Leftrightarrow \exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),\ \exists m \in \mathbb{P}(\sqrt{x}),$
$x \equiv p\ (mod\ m)$

On cherche à démontrer l'impossibilité de l'existence d'un entier pair qui ne vérifie pas la conjecture de Goldbach.

- Un nombre pair x ne vérifie pas la conjecture de Goldbach si et seulement si tout nombre premier impair p inférieur à sa moitié lui est congru selon un module premier impair m inférieur à sa racine.

- $\exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),\ \exists m \in \mathbb{P}(\sqrt{x}),$
  $x \equiv p\ (mod\ m)$

Descente infinie de Fermat

- Elle consiste à démontrer que si un nombre ne vérifiait pas la conjecture de Goldbach, il y en aurait un plus petit qui ne la vérifierait pas non plus

  (et ainsi de proche en proche, jusqu'à atteindre des nombres si petits qu'on sait qu'ils vérifient la conjecture).

- La descente infinie repose sur le fait qu'il n'existe pas de suite infinie strictement décroissante d'entiers naturels.

- Raisonnement par l'absurde :
  - on suppose que x est le plus petit entier tel que $P(x)$.
  - on montre qu'alors $P(x')$ avec $x' < x$.
  - on a abouti à une contradiction.

  (Si $P(n)$ pour un entier naturel n donné, il existe une partie non vide de $\mathbb{N}$ contenant un élément qui vérifie la propriété P. Cette partie admet un plus petit élément. En l'occurrence, la propriété P consiste à ne pas vérifier la conjecture de Goldbach)

On cherche à démontrer l'impossibilité de l'existence d'un entier pair qui ne vérifie pas la conjecture de Goldbach.

- x est le nombre pair dont on considère au début de la démonstration qu'il est le plus entier naturel ne vérifiant pas la conjecture de Goldbach ;

- $\exists x \in 2\mathbb{N},\ x \geq 20,\ \forall p \in \mathbb{P}(x/2),\ \exists m \in \mathbb{P}(\sqrt{x}),$
  $x \equiv p\ (mod\ m)$

- x ne peut de toute façon être congru à aucun nombre premier selon tout module qui divise x donc $m \nmid x$.

- x est congru à un certain nombre (éventuellement nul) de nombres premiers selon le module 3, à un certain nombre (éventuellement nul) de nombres premiers selon le module 5, etc.

Descente infinie de Fermat

- x est congru à chaque nombre premier impair inférieur à sa moitié selon un certain module premier impair inférieur à sa racine.
- On partage l'ensemble des nombres premiers impairs $\mathbb{P}(x/2)$ en sous-ensembles disjoints dont l'union est l'ensemble total et tels que chaque sous-ensemble contient des nombres premiers impairs congrus à x selon un même module premier impair.
- $\mathbb{P}(x/2) = E_{x,m_1} \cup E_{x,m_2} \cup \ldots \cup E_{x,m_i}$
- où $E_{i,j} = \{p \text{ premier impair},\ p \leq i/2 \text{ et } p \equiv i \ (mod\ j)\}$

Descente infinie de Fermat

- Considérons maintenant un nombre pair $x' = x - 2.\prod m_i$ inférieur strictement à x et congru à x selon tous les modules premiers impairs m_i inférieurs à $\sqrt{x}$.

- Il faudrait être capable de démontrer que par soustraction d'une primorielle, si x ne vérifiait pas Goldbach, x' ne la vérifierait pas non plus.

Conclusion

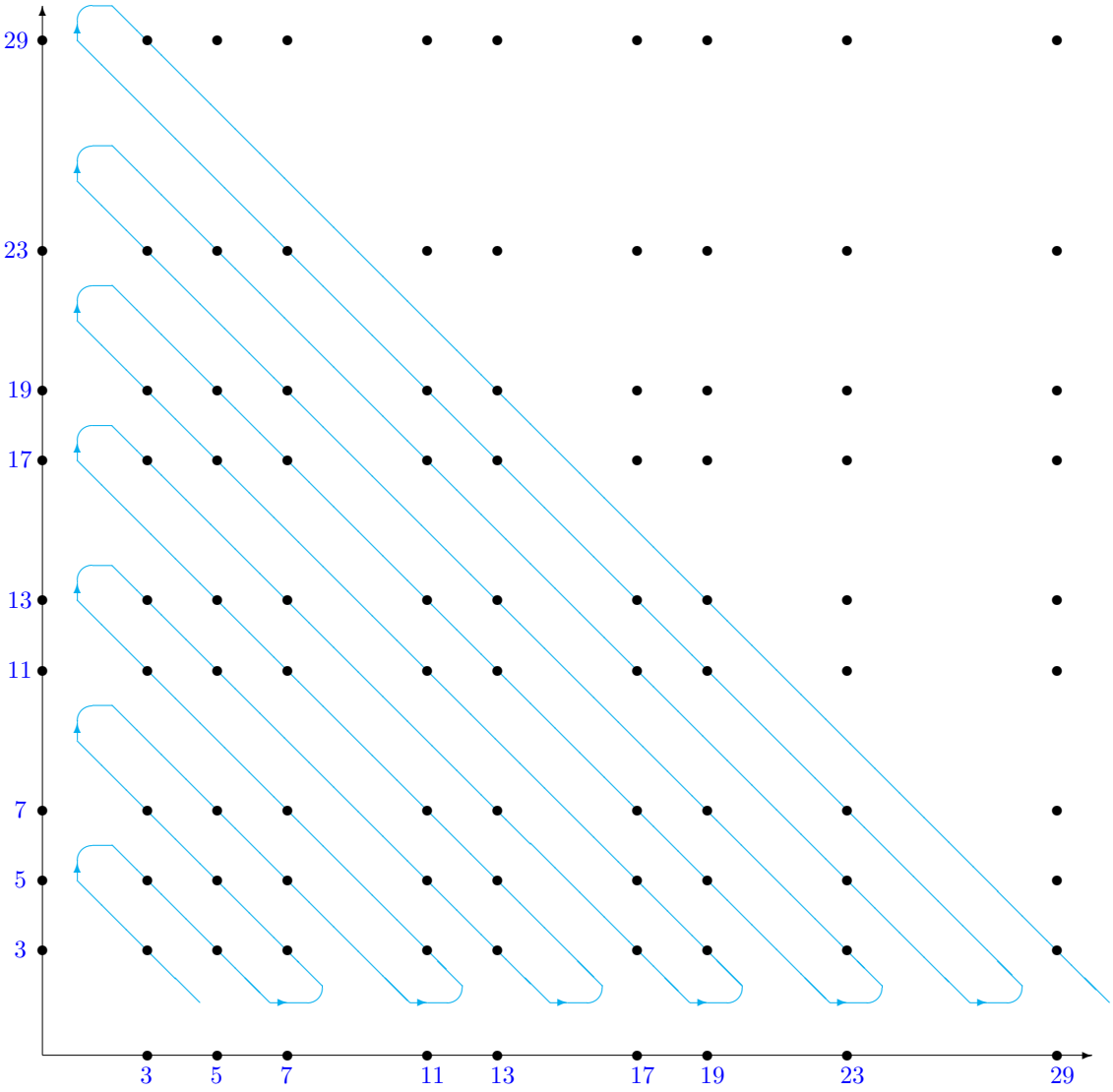
- On a utilisé un *Système de NUmération par les Restes dans les Parties Finies de* $\mathbb{N}$.
- On se situe dans le cadre d'une *théorie lexicale des nombres*, qui associe à un nombre un mot dont les lettres sont certains de ses restes modulaires selon des modules premiers.

Bijection de Cantor et Conjecture de Goldbach

Denise Vella-Chemla

24 janvier 2013

La conjecture de Goldbach stipule que tout nombre pair n plus grand que 2 est la somme de deux nombres premiers.



Cantor a exhibé une bijection de $\mathbb{N} \times \mathbb{N}$ dans $\mathbb{N}$.

Un argument similaire permet de mettre en bijection l'ensemble des sommes de deux nombres premiers et l'ensemble des entiers naturels, comme visualisé sur le graphique ci-dessus.

On peut également mettre en bijection l'ensemble des décompositions de Goldbach de la forme $3 + p_j$, avec p_j premier impair avec $\mathbb{N}$ ou bien avec l'ensemble des décompositions de Goldbach de la forme $p_i + 7$, avec p_i premier impair.

On peut aussi en procédant à un double comptage par ligne ou par colonne mettre en bijection un ensemble tel que $\{3+3, 3+5, 3+7, 5+5, 5+7, 7+7\}$ avec lui-même selon la bijection suivante, par exemple :

$$\begin{aligned}
3+3 &\mapsto 3+7 \\
3+5 &\mapsto 5+7 \\
3+7 &\mapsto 7+7 \\
5+5 &\mapsto 3+5 \\
5+7 &\mapsto 5+5 \\
7+7 &\mapsto 3+3
\end{aligned}$$

Mais cela ne semble pas permettre d'aboutir à quoi que ce soit au sujet de la conjecture de Golbach.

Un algorithme d'obtention des décomposants de Goldbach d'un nombre pair

Denise Vella-Chemla

Décembre 2012

1 Introduction

La conjecture de Goldbach stipule que tout nombre pair n plus grand que 2 est la somme de deux nombres premiers. Ces nombres premiers p et q sont appelés décomposants de Goldbach de n. Assumons ici que la conjecture de Goldbach est vraie.

Rappelons quatre faits :

1) Les nombres premiers plus grands que 3 sont de la forme $6k \pm 1$.

2) n étant un nombre pair plus grand que 2 ne peut être le carré d'un nombre premier qui est impair. Si $p_1, p_2, \ldots, p_r$ sont des nombres premiers plus grands que $\sqrt{n}$, l'un d'entre eux au plus (peut-être aucun) appartient à la décomposition euclidienne de n en facteurs premiers puisque le produit de deux d'entre eux est supérieur à n.

3) Les décomposants de Goldbach de n sont à trouver parmi les unités du groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z}, \times)$. Ces unités sont premières à n, elles sont en nombre pair et la moitié d'entre elles sont inférieures ou égales à $n/2$.

4) Si un nombre premier $p \leq n/2$ est congru à n modulo un nombre premier $m_i < \sqrt{n}$ ($n = p + \lambda m_i$), son complémentaire à n, q, 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 être un décomposant de Goldbach de n.

2 Algorithme

Prendre en compte ces faits élémentaires amène une procédure qui permet d'obtenir 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.

3 Etude d'un exemple

Appliquons la procédure au nombre pair $n = 500$.

Notons d'abord que $500 \equiv 2\ (mod\ 3)$. 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 $\left\lfloor \frac{500}{12} \right\rfloor$ nombres de la forme $6k+1$ inférieurs ou égaux à $500/2$. Ils sont compris entre 7 et 247 (première colonne du tableau).

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

La seconde colonne du tableau fournit le résultat de la première passe du crible : elle élimine les nombres congrus à 0 ($mod\ m_i$) quelque soit i.

La troisième colonne du tableau fournit le résultat de la deuxième passe du crible : elle élimine les nombres congrus à n $(mod\ m_i)$ quelque soit i.

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).

$500 = 2^2.5^3$. Le module 5 n'apparaît pas en troisième colonne.

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

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

$a_k = 6k+1$	*congruence(s) à 0 éliminant* a_k	*congruence(s) à* r $\neq 0$ *éliminant* a_k (*i.e. congruence(s) à* n)	n-a_k	*nombres restants*
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	

Remarque : revenons sur la première partie de l'algorithme, qui 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 $n/4+1$.

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). La seconde partie de l'algorithme élimine 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 $n \equiv p \ (mod\ m_i)$ *or* $n - p \equiv 0 \ (mod\ m_i)$.

Les deux passes de l'algorithme peuvent être menées indépendamment l'une de l'autre.

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.