Décomposants de Goldbach dans le groupe des unités

Denise Chemla

13 octobre 2013

1 Groupes $C3$ et $C4$

Pour $n = 14$, le groupe des unités quotienté par $\{-1, 1\}$ est le groupe cyclique $C3$. On représente ci-dessous sa table de Cayley pour la multiplication et les décomposants de Goldbach sont colorés en rouge dans les entêtes de colonnes. On met une colonne fictive pour 7 bien que 7 ne soit pas une unité (pas premier à 14 puisque diviseur de 14) (en fait, on se dit que c'est peut-être une racine qu'il faudrait adjoindre parce qu'il est un décomposant trivial de 14).

$n = 14$	1	3	5	7
1	1	3	5	–
3	3	5	1	–
5	5	1	3	–
7	–	–	–	–

Pour les nombres $n = 16$, $n = 20$ ou $n = 30$, le groupe des unités quotienté est le groupe cyclique $C4$. On modifie l'ordre croissant habituel sur les entiers de manière à bien faire apparaître la cyclicité du groupe dans les lignes des tables de Cayley.

$n = 16$	1	3	7	5
1	1	3	7	5
3	3	7	5	1
7	7	5	1	3
5	5	1	3	7

$n = 20$	1	3	9	7
1	1	3	9	7
3	3	9	7	1
9	9	7	1	3
7	7	1	3	9

$n = 30$	1	7	11	13
1	1	7	11	13
7	7	11	13	1
11	11	13	1	7
13	13	1	7	11

Passons à $n = 60$ parce qu'alors le groupe des unités quotienté est $C4 \times C2$.

$n = 60$	1	7	11	17	13	19	23	29
1	1	7	11	17	13	19	23	29
7	7	11	17	1	29	13	19	23
11	11	17	1	7	23	29	13	19
17	17	1	7	11	19	23	29	13
13	13	29	23	19	11	7	1	17
19	19	13	29	23	7	1	17	11
23	11	13	1	7	1	7	11	13
29	29	23	19	13	17	11	7	1

Voyons pour $n = 80$ dans la mesure où le groupe des unités quotienté est $C4 \times C4$.

$n = 80$	1	3	9	27	7	21	17	29	11	33	19	23	13	39	37	31
1	1	3	9	27	7	21	17	29	11	33	19	23	13	39	37	31
3	3	9	27	1	21	17	29	7	33	19	23	11	39	37	31	13
9	9	27	1	3	17	29	7	21	19	23	11	33	37	31	13	39
27	27	1	3	9	29	7	21	17	23	11	33	19	31	13	39	37
7	7	21	17	29	31	13	39	37	3	9	27	1	11	33	19	23
21	21	17	29	7	13	39	37	31	9	27	1	3	33	19	23	11
17	17	29	7	21	39	37	31	13	27	1	3	9	19	23	11	33
29	29	7	21	17	37	31	13	39	1	3	9	27	23	11	33	19
11	11	33	19	23	3	9	27	1	39	37	31	13	17	29	7	21
33	33	19	23	11	9	27	1	3	37	31	13	39	29	7	21	17
19	19	23	11	33	27	1	3	9	31	13	39	37	7	21	17	29
23	23	11	33	19	1	3	9	27	13	39	37	31	21	17	29	7
13	13	39	37	31	11	33	19	23	17	29	7	21	9	27	1	3
39	39	37	31	13	33	19	23	11	29	7	21	17	27	1	3	9
37	37	31	13	39	19	23	11	33	7	21	17	29	1	3	9	27
31	31	13	39	37	23	11	33	19	21	17	29	7	3	9	27	1

2 Groupes $C5$ et $C6$

Pour $n = 22$, le groupe des unités quotienté par $\{-1, 1\}$ est le groupe cyclique $C5$. On met une colonne fictive pour 11 décomposant de Goldbach trivial de 22.

$n = 22$	1	3	9	5	7	11
1	1	3	9	5	7	–
3	3	9	5	7	1	–
9	9	5	7	1	3	–
5	5	7	1	3	9	–
7	7	1	3	9	5	–
11	–	–	–	–	–	–

Pour les nombres $n = 26$ et $n = 28$, le groupe des unités quotienté est le groupe cyclique $C6$. Pour rappel, pour $n = 26$ existe également le décomposant de Goldbach trivial 13 premier.

$n = 26$	1	7	3	5	9	11
1	1	7	3	5	9	11
7	7	3	5	9	11	1
3	3	5	9	11	1	7
5	5	9	11	1	7	3
9	9	11	1	7	3	5
11	11	1	7	3	5	9

$n = 28$	1	5	3	13	9	11
1	1	5	3	13	9	11
5	5	3	13	9	11	1
3	3	13	9	11	1	5
13	13	9	11	1	5	3
9	9	11	1	5	3	13
11	11	1	5	3	13	9

3 Groupe $C9$

Le groupe cyclique $C9$ est celui trouvé pour $n = 38$ et $n = 54$.
On ne fournit plus la table de Cayley : pour $n = 38$, les puissances de 3 sont dans l'ordre $\{1, 3, 9, 11, 5, 15, 7, 17, 13\}$.
Pour $n = 54$, les puissances de 5 sont dans l'ordre $\{1, 5, 25, 17, 23, 7, 19, 13, 11\}$.

4 Groupe $C10$

Le groupe cyclique $C10$ est celui trouvé pour $n = 44$, $n = 50$ et $n = 66$.
Pour $n = 44$, les puissances de 3 sont dans l'ordre $\{1, 3, 9, 17, 7, 21, 19, 13, 5, 15\}$.
Pour $n = 50$, les puissances de 3 sont dans l'ordre $\{1, 3, 9, 23, 19, 7, 21, 13, 11, 17\}$.
Pour $n = 66$, les puissances de 5 sont dans l'ordre $\{1, 5, 25, 7, 31, 23, 17, 19, 29, 13\}$.

5 Note

Ci-dessous, pour $n = 36$, est présenté le procédé de quotient par $\{1, -1\}$. D'abord, la table de Cayley avec les unités dans l'ordre croissant traditionnel sur les entiers, puis la même table mais dont on a interverti certaines colonnes de manière à bien voir apparaître les sous-groupes cycliques et enfin, le quotient pour ne garder que les unités inférieures à $n/2$ dont on rappelle qu'il s'agit de ne conserver que celles qui d'une part sont des nombres premiers et d'autre part ne sont jamais congrus à n selon un module premier inférieur à $\sqrt{n}$.

Table de Cayley initiale pour la multiplication dans $\mathbb{Z}/36\mathbb{Z}$:

	1	5	7	11	13	17	19	23	25	29	31	35
1	1	5	7	11	13	17	19	23	25	29	31	35
5	5	25	35	19	29	13	23	7	17	1	11	31
7	7	35	13	5	19	11	25	17	31	23	1	29
11	11	19	5	13	35	7	29	1	23	31	17	25
13	13	29	19	35	25	5	31	11	1	17	7	23
17	17	13	11	7	5	1	35	31	29	25	23	19
19	19	23	25	29	31	35	1	5	7	11	13	17
23	23	7	17	1	11	31	5	25	35	19	29	13
25	25	17	31	23	1	29	7	35	13	5	19	11
29	29	1	23	31	17	25	11	19	5	13	35	7
31	31	11	1	17	7	23	13	29	19	35	25	5
35	35	31	29	25	23	19	17	13	11	7	5	1

Interversion de certaines colonnes pour bien "voir" $C6 \times C2$:

	1	11	13	35	25	23	5	19	29	31	17	7	
1	1	11	13	35	25	23	5	19	29	31	17	7	$a^0 = Id$
11	11	13	35	25	23	1	19	29	31	17	7	5	a^1
13	13	35	25	23	1	11	29	31	17	7	5	19	a^2
35	35	25	23	1	11	13	31	17	7	5	19	29	a^3
25	25	23	1	11	13	35	17	7	5	19	29	31	a^4
23	23	1	11	13	35	25	7	5	19	29	31	17	a^5
5	5	19	29	31	17	7	25	23	1	11	13	35	b
19	19	29	31	17	7	5	23	1	11	13	35	25	$a.b$
29	29	31	17	7	5	19	1	11	13	35	25	23	$a^2.b$
31	31	17	7	5	19	29	11	13	35	25	23	1	$a^3.b$
17	17	7	5	19	29	31	13	35	25	23	1	11	$a^4.b$
7	7	5	19	29	31	17	35	25	23	1	11	13	$a^5.b$

Quotient par $\{1,-1\}$ pour se focaliser les unités inférieures à $n/2$:

$n=36$	1	5	7	11	13	17
1	1	5	7	11	13	17
5	5	11	1	17	7	13
7	7	1	13	5	17	11
11	11	17	5	13	1	7
13	13	7	17	1	11	5
17	17	13	11	7	5	1

Interversion des colonnes pour bien reconnaître $C6$:

$n=36$	1	5	11	17	13	7
1	1	5	11	17	13	7
5	5	11	17	13	7	1
11	11	17	13	7	1	5
17	17	13	7	1	5	11
13	13	7	1	5	11	17
7	7	1	5	11	17	13