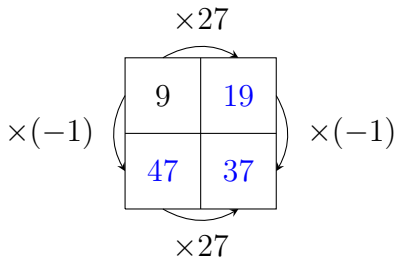
Bidominos bicolores (Denise Vella-Chemla, novembre 2023).

Cette note fait suite à celles-ci : 1, 2, 3 4 et compile le peu dont on dispose.

On va représenter certaines connaissances par des bidominos bicolores. On aura deux sortes de bidominos, les bidominos (qu'on appellera bidominos bleus) qui représentent la relation "est un décomposant de Goldbach de n" et qui vérifient certaines contraintes multiplicatives, et les bidominos (qu'on appellera bidominos verts) qui représentent la relation "est un résidu quadratique de n".

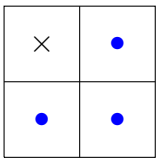
Pour n un nombre pair, une permutation de $[1, \ldots, n]$ par multiplication par k premier à n peut être représentée par la composition d'un certain nombre de transpositions, qui mettent en correspondance deux nombres et leurs opposés (leur complémentaire à n). On représentera, par exemple, une paire de telles transpositions par un bidomino bleu ainsi ($n = 56$) :



Le bidomino bleu ci-dessus représente les 4 congruences suivantes :

$$\begin{cases} 9 \times 27 & = 4 \times 56 + 19 & \equiv 19 \pmod{56} \\ 19 \times 27 & = 9 \times 56 + 9 & \equiv 9 \pmod{56} \\ 9 \times (-1) & = (-1) \times 56 + 47 & \equiv 47 \pmod{56} \\ 19 \times (-1) & = (-1) \times 56 + 37 & \equiv 37 \pmod{56} \end{cases}$$

On "résumera" un tel bidomino bleu en oubliant les nombres ainsi :



Qu'a-t-on constaté [1] également sur les permutations étudiées ? En termes de signature des permutations, on a vu (voir [6] pages 2 et 5) que pour n double d'un nombre impair, toutes les permutations engendrées par multiplication par un nombre premier à n sont de signature paire, tandis que pour n double d'un nombre pair, la parité des signatures des permutations alterne : la permutation est de signature paire pour une multiplication par m de la forme $4k+1$ et impaire pour une multiplication par m de la forme $4k + 3$.

D'autre part, on a la relation "est un résidu quadratique de". Sa table, pour les nombres premiers, est fournie par Gauss dans les Recherches arithmétiques (voir en annexe). On représentera

1. qui serait à démontrer.

cette propriété “est un résidu quadratique de n”, qui “appose” sur les nombres $[1, \ldots, n]$ un motif périodique, par des bidominos dits verts, chacun d'eux ayant comme caractéristique que les deux nombres entiers en hauts du bidomino sont des nombres entiers successifs croissants et les deux nombres entiers en bas du bidomino vert sont des nombres entiers successifs décroissants.

On dispose aussi de données sur le nombre de résidus quadratiques d'un nombre entier : Lehmer en 1913 [1] ou Stang en 1996 [2] fournissent des formules de calcul de ce nombre ; la fonction “nombre de résidus quadratiques de” est multiplicative et elle est définie par les formules suivantes sur les nombres premiers et leurs puissances :

$$\begin{cases} \text{nbRQ}(2) = 2; \\ \text{nbRQ}(p) = \dfrac{p-1}{2} & \text{pour } p \text{ premier, } p \geq 3; \\ \text{nbRQ}(2^k) = \begin{cases} \dfrac{2^{k-1}+4}{3}, & \text{pour } k \text{ pair ;} \\ \dfrac{2^{k-1}+5}{3} & \text{pour } k \text{ impair } \mathrm{k} \geq 3 \end{cases} & ; \\ \text{nbRQ}(p^k) = \begin{cases} \dfrac{p^{k+1}+p+2}{2(p+1)} & \text{pour } k \text{ pair et } p \neq 2, p \text{ premier} \\ \dfrac{p^{k+1}+2p+1}{2(p+1)} & \text{pour } k \text{ impair } \geq 3 \text{ et } p \neq 2, p \text{ premier} \end{cases} \end{cases}$$

Voyons un exemple : pour $98 = 2.7^2$, on trouve nbRQ(98) = 44. Les résidus quadratiques obéissent au motif périodique (hormis au milieu) R-R-N-R-N-N-N de longueur 7 ainsi (dans la suite des nombres, les résidus quadratiques sont verts) :

0	1	2	3	4	5	6	7
	8	9	10	11	12	13	14
	15	16	17	18	19	20	21
	22	23	24	25	26	27	28
	29	30	31	32	33	34	35
	36	37	38	39	40	41	42
	43	44	45	46	47	48	49
	50	51	52	53	54	55	56
	57	58	59	60	61	62	63
	64	65	66	67	68	69	70
	71	72	73	74	75	76	77
	78	79	80	81	82	83	84
	85	86	87	88	89	90	91
	92	93	94	95	96	97	

Remarque : pour n un nombre pair, la moitié de n est un résidu quadratique de n.

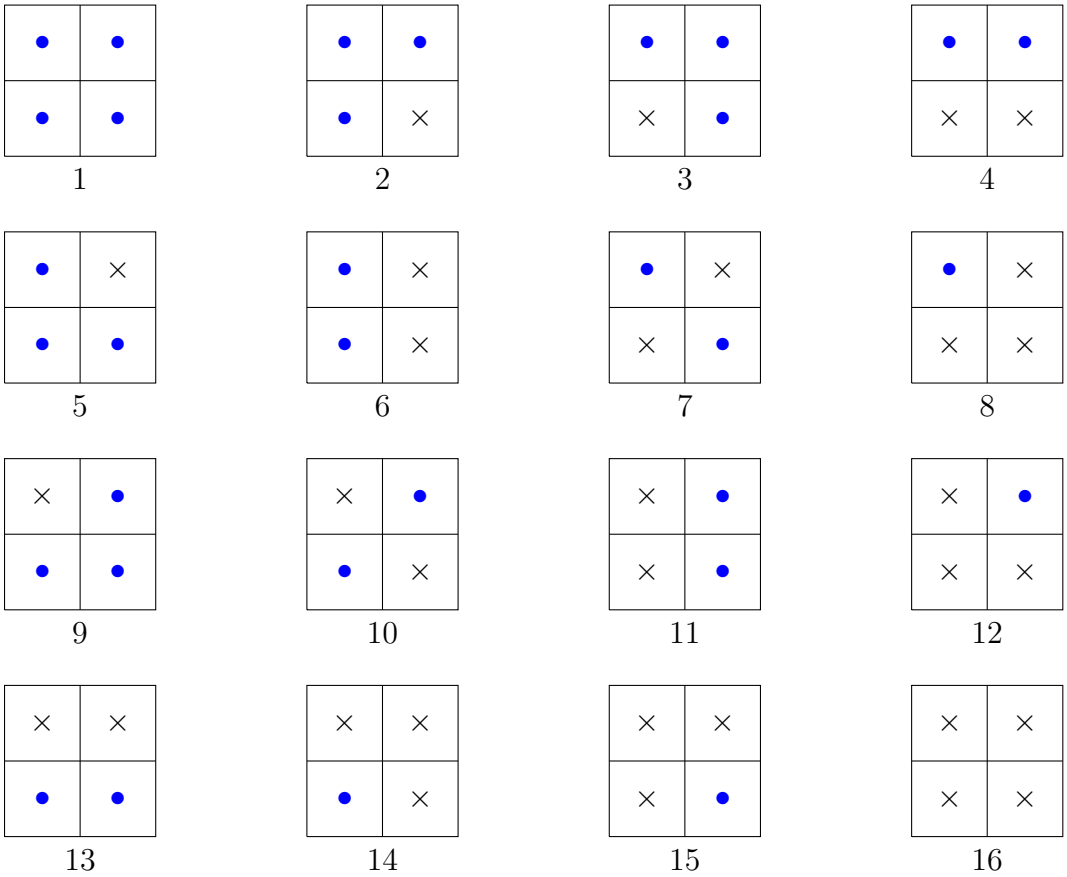
On représentera un tel bidomino vert, de connaissance de certaines relations “est un résidu quadratique de n” ainsi :

29	30
69	68

et on le résumera par :

•	•
×	×

On rappelle qu'un bidomino bicolore bleu (selon la multiplication vue plus haut) a 16 configurations possibles :



Les possibilités 1, 2, 3, 5, 6, 9 et 11 contiennent une décomposition de Goldbach au moins (un nombre premier (•) au-dessus d'un autre nombre premier (•)).

Notre but est de montrer qu'on a toujours pour n un bidomino bleu qui contient deux nombres premiers complémentaires à n, mais on ne sait pas comment établir un lien entre les bidominos

bleus des transpositions, obtenus par les multiplications dans $(\mathbb{Z}/n\mathbb{Z})^\times$, et les bidominos verts pour la relation "est un résidu quadratique de".

Il faudrait :

— soit démontrer qu'il est impossible, compte-tenu des contraintes qui doivent être vérifiées par les transpositions (i.e. on multiplie horizontalement par un nombre et cette opération de multiplication s'avère être une involution modulo n tandis que verticalement, on multiplie par -1 modulo n puisqu'un nombre se transpose verticalement en son opposé) et compte-tenu des contraintes de résiduosité quadratique qui lient les nombres selon leur factorisation et leur forme $4k+1$ ou $4k+3$, que les seules paires de transpositions (bidominos bleus) possibles soient toutes des seules formes 4, 7, 8, 10, 12, 13, 14, 15 et 16 énumérées ci-dessus ;

— soit démontrer par récurrence que si les bidominos sont "agréables" jusqu'à n, on a un bidomino contenant une paire de nombres premiers complémentaires pour $n+2$ (qui est le nombre pair suivant n pair).

Annexe : table de la relation "est un résidu quadratique de" fournie par Gauss dans ses Recherches arithmétiques

On colore en cyan les entête de lignes et de colonnes correspondant aux nombres premiers de la forme $4k+1$ (qui sont sommes de 2 carrés de manière unique) pour souligner la symétrie de la relation "est résidu quadratique de" qu'ils amènent (pour eux, ligne=colonne). On a omis la colonne correspondant au nombre premier 2 car un nombre impair est toujours congru à un carré modulo 2 puisqu'il est congru à 1 modulo 2, et que 1 est son propre carré.

	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
2			×			×		×		×		×		×					×	×	×		×	×
3	×			×	×			×			×			×		×	×		×	×		×		×
5		×		×			×		×	×		×				×	×		×		×		×	
7	×		×				×		×	×	×			×	×	×						×		
11		×	×	×			×				×		×		×						×	×	×	×
13	×				×	×		×	×				×		×		×				×			
17					×	×	×						×	×	×	×		×				×	×	
19	×	×				×	×			×						×	×	×	×	×	×			
23			×	×	×		×	×	×			×	×					×		×	×	×		
29		×	×		×			×	×						×	×		×	×			×		
31	×	×		×				×		×		×	×								×	×		×
37	×		×	×							×	×		×	×			×	×	×		×		
41		×						×		×	×	×	×			×	×			×		×		
43	×		×		×	×	×					×	×		×				×					×
47				×		×	×	×		×	×		×	×	×		×	×					×	×
53			×	×	×	×			×		×		×	×	×	×							×	×
59		×		×		×		×	×	×		×	×	×	×	×		×				×		
61	×	×			×		×					×		×			×			×		×		×
67	×		×	×		×			×	×	×		×					×		×	×		×	
71		×	×	×				×	×	×	×			×		×		×	×	×			×	
73	×						×	×			×	×					×	×	×	×	×		×	×
79	×	×	×		×								×	×		×			×	×	×		×	×
83						×	×		×		×	×	×	×			×	×	×		×	×		
89		×		×		×								×	×			×	×	×	×		×	×
97	×			×						×			×	×	×		×			×	×		×	×

On vérifie que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

La relation "est résidu quadratique de" est réflexive, symétrique si l'un au moins de p ou q est de la forme $4k+1$ et anti-symétrique sinon (si p et q sont tous les deux de la forme $4k+3$).

Références

[1] Lehmer D. N., *Certain Theorems in the Theory of Quadratic Residues*, The American Mathematical Monthly, Vol. 20, No. 5 (May, 1913), pp. 151-157, https://www.jstor.org/stable/2972413. Traduction http://denise.vella.chemla.free.fr/trad-Lehmer-nb-RQ.pdf.

[2] Stangl W. D., *Counting squares in* $\mathbb{Z}_n$, Mathematics magazine, vol. 69, n° 4, octobre 1996, p. 285. Traduction http://denise.vella.chemla.free.fr/trad-Stangl.pdf.

[3] Denise Vella-Chemla, *Des nombres qui en permutent d'autres*, http://denise.vella.chemla.free.fr/permutations.pdf, octobre 2023.

[4] Denise Vella-Chemla, *Annexe 2 : permutations associées aux nombres premiers à n (sauf 1 et $n-1$) pour n compris entre 64 et 100 et non double d'un nombre premier*, http://denise.vella.chemla.free.fr/permutations-annexe-2.pdf, octobre 2023.

[5] Denise Vella-Chemla, *Annexe 3 : permutations associées aux nombres premiers à n (sauf 1 et $n-1$) pour n compris entre 14 et 100 et n double d'un nombre premier de la note Des nombres qui en permutent d'autres*, http://denise.vella.chemla.free.fr/permutations-doubles-de-premiers.pdf, octobre 2023.

[6] Denise Vella-Chemla, *Utilisation de permutations à la recherche de décompositions de Goldbach*, http://denise.vella.chemla.free.fr/indu.pdf, novembre 2023.