Additions de parties dans $\mathbb{N}$

Gabriel Pallier (gabriel@pallier.org)

Parimaths, 26 septembre 2015

Table des matières

Motivations

Le sujet qui nous occupe aujourd'hui est l'addition de parties dans $\mathbb{N}$ et dans certains ensembles de nombres proches de $\mathbb{N}$. La sommation des parties généralise celle des éléments dans le sens suivant :

Notation 1. Soient A et B des sous-ensembles de $\mathbb{Z}$, et n un entier naturel. On appelle somme de A et B l'ensemble

$$A + B = \{a + b \mid a \in A, b \in B\}$$

On appelle n-ième somme itérée de A l'ensemble

$$n \wedge A = \underbrace{A + \cdots + A}_{n\text{fois}}$$

Attention, ceci diffère de $nA = \{n \cdot a \mid a \in A\}$ dès que A possède au moins deux éléments. Enfin, par convention (mais c'est une convention raisonnable) $0 \wedge A = \{0\}$

Bien que d'une apparente simplicité dans leur formulation, les problèmes d'addition de parties forment un sujet de recherche à part entière en mathématiques appelé théorie additive des nombres, qui appelle rapidement des preuves d'une difficulté redoutable. Voici quelques questions très vastes qui se posent naturellement, et que nous ne pourrons qu'effleurer dans la suite [1] :

Question 1. On se donne A et B deux parties, que peut-on dire sur la taille de $A+B$ en fonction de celles de A et de B ? (La notion de "taille" reste bien sûr à préciser notamment pour les parties infinies). Dans le même ordre d'idée, comment caractériser A et B telles que $A+B$ est "petit" par rapport à A et B ?

Question 2. On se donne $A \subseteq \mathbb{N}$, a-t-on pour un certain g, $g \wedge A = \mathbb{N}$? $g \wedge A = \mathbb{N}_{\geqslant m}$ pour un certain m ? Cette question avec pour A l'ensemble des puissances k-ièmes constitue le problème de Waring. Depuis Hilbert on sait qu'un tel g existe toujours, mais en général on ne sait qu'encadrer le plus petit d'entre eux, noté $g(k)$.

Question 3. Soit $\mathcal{P} \subseteq \mathbb{N}$ l'ensemble des nombres premiers. A-t-on

$$\mathcal{P} + \mathcal{P} \supset 2\mathbb{N}_{\geqslant 2} = \{4, 6, 8, \ldots\} \ ?$$

$$3 \wedge \mathcal{P} \supset 2\mathbb{N}_{\geqslant 3} + \{1\} = \{7, 9, 11, \ldots\} \ ?$$

La deuxième ligne était la conjecture de Goldbach faible et vient tout juste d'être démontrée (en 2014, par H. Helfgott) ; la première est la conjecture de Golbach forte qui tient toujours.

1 Combinatoire additive

1.1 Un zeste de combinatoire additive dans $\mathbb{N}$

On sommera ici exclusivement des ensembles finis. On désigne par $|X|$ le cardinal de X.

Exercice 1. Soient A et B deux parties finies de $\mathbb{N}$. Montrer que

$$|A+B| \leqslant |A| \cdot |B| \tag{1}$$

Puis que cette majoration est optimale. Émettre des conjectures sur une minoration de $|A+B|$ en fonction de $|A|$ et $|B|$, et essayer de les démontrer.

Théorème 1. *Soient $A, B \subseteq \mathbb{Z}$ deux ensembles finis non vides. Alors on a l'inégalité*

$$|A+B| \geqslant |A| + |B| - 1 \tag{2}$$

Avec égalité si et seulement si, $|A| = 1$ ou $|B| = 1$ ou A et B sont les ensembles sous-jacents à des progressions arithmétiques de même raison.

Démonstration. Quitte à translater les parties A et B par t et s, ce qui revient à translater leur somme de $t+s$ et ne change pas les cardinaux, on peut supposer que $A, B \subset \mathbb{N} - \{0\}$. Cette opération est profitable car on va maintenant se servir de l'ordre. Écrivons

$$A = \{a_1 \ldots a_k\}$$

1. Pour les réponses éventuelles mentionnées dans cette introduction, je ne peux d'ailleurs que faire confiance aux spécialistes...

$$B = \{b_1 \dots b_\ell\}$$

Avec $0 < a_1 < \cdots < a_k$ et $0 < b_1 < \cdots < b_\ell$. On place les éléments de $A + B$ dans un grand tableau :

	a_1	$<$	$\cdots$	$<$	a_k
b_1	$a_1 + b_1$	$<$	$\cdots$	$<$	$a_k + b_1$
$\wedge$	$\wedge$				$\wedge$
$\vdots$	$\vdots$		$a_i + b_j$		$\vdots$
$\wedge$	$\wedge$				$\wedge$
b_ℓ	$a_1 + b_\ell$	$<$	$\cdots$	$<$	$a_k + b_\ell$

Maintenant, n'importe quel chemin de directions Sud-Est allant de $a_1 + b_1$ à $a_k + b_\ell$ dans le grand tableau constitue une suite strictement croissante de $k + \ell - 1$ termes. On en déduit que

$$|A + B| \geqslant k + \ell - 1 = |A| + |B| - 1$$

De plus, il y a égalité quand toutes ces suites sont égales, c'est-à-dire quand $a_{i+1} - a_i = b_{j+1} - b_j$ pour tous i et j tels que $1 \leqslant i < k$, $1 \leqslant j < \ell$. Si k et ℓ sont $\geqslant 2$, cela impose que (a_i) et (b_j) sont des progressions arithmétiques de même raison. Si $k = 1$ ou $\ell = 1$, l'égalité est vérifiée.

Si la majoration 1 aurait toujours été possible en remplaçant $\mathbb{Z}$ par un ensemble M quelconque muni d'une loi d'addition (penser à $\mathbb{Z}/10\mathbb{Z}$ par exemple), la preuve de la minoration 2 a fait intervenir de manière cruciale l'ordre dans $\mathbb{N}$ et on s'attend à ce qu'elle soit spécifique à $\mathbb{Z}$. En fait, nous verrons vers la fin qu'il existe un énoncé analogue dans $\mathbb{Z}/p\mathbb{Z}$ quand p est premier : le théorème de Cauchy-Davenport.

1.2 Une louche de combinatoire additive dans $\mathbb{Z}/n\mathbb{Z}$

Rappels sur $\mathbb{Z}/n\mathbb{Z}$ On dit que deux entiers a et b sont congrus modulo un entier n, et on note $a \equiv b[n]$, si n divise $b - a$. On vérifie que l'addition et la multiplication dans $\mathbb{Z}$ sont compatibles avec les congruences ; plus précisément, pour tout $c \in \mathbb{Z}$, si $a \equiv b[n]$, alors $a + c \equiv b + c[n]$, et $ac \equiv bc[n]$. On calcule donc modulo n comme on calcule dans les entiers, en ajoutant la règle $n = 0$. On note $\overline{a}$ la classe de congruence de a modulo n, et $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes de congruence modulo n. D'après ce qui précède, on peut sommer et multiplier les classes de congruence.

Exemple 1. Dans $\mathbb{Z}/7\mathbb{Z}$, $\overline{6} + \overline{3} = \overline{2}$ et $\overline{6} \times \overline{3} = \overline{4}$. Attention, l'entier n est implicite dans la notation $\overline{a}$; on doit toujours pouvoir le déterminer à l'aide du contexte.

Remarque 1. Il est possible, et dans une certaine mesure utile, de penser à $\mathbb{Z}/n\mathbb{Z}$ (au moins du point de vue de l'addition [2] qui nous occupe ici) comme à l'ensemble des nombres disposés sur une horloge à n heures. L'opération consistant à additionner x à y revient à faire tourner l'aiguille pointée vers y de x graduations dans le sens des aiguilles de cette horloge.

On sommera ici des parties de $\mathbb{Z}/n\mathbb{Z}$, en conservant les notation précédentes. En fait, sommer les parties de $\mathbb{Z}/n\mathbb{Z}$ est instructif quand il s'agit de sommer les parties de $\mathbb{N}$ ou $\mathbb{Z}$, comme le montre l'exercice suivant :

Exercice 2. Calculer $3 \wedge \{\overline{0}, \overline{1}, \overline{4}\}$ dans $\mathbb{Z}/8\mathbb{Z}$. Quels sont les classes de congruence des carrés modulo 8 ? En déduire que 2015 n'est pas somme de trois carrés.

2. Pour la multiplication, voir `http://micmaths.com/videos.php` , la face cachée des tables de multiplication

Venons-en à la combinatoire additive proprement dite dans $\mathbb{Z}/n\mathbb{Z}$:

Proposition 1. *Soient* $A, B \subseteq \mathbb{Z}/n\mathbb{Z}$ *non-vide et tels que* $|A| + |B| > n$. *Alors* $A + B = \mathbb{Z}/n\mathbb{Z}$.

Démonstration. Soit $x \in \mathbb{Z}/n\mathbb{Z}$, alors x est dans $A + B$ si, et seulement si, $\{\{x\} - B\} \cap A$ est non vide. Or

$$|\{x\} - B| + |A| = |B| + |A| > n = |\mathbb{Z}/n\mathbb{Z}|$$

Donc nécessairement, ces deux ensembles s'intersectent (Si l'on veut, on peut voir ceci comme une conséquence du principe des tiroirs).

Exercice 3 (Important). Soit p un nombre premier. Montrer qu'il existe x et y dans $\mathbb{N}$ tels que p divise $1 + x^2 + y^2$.

Exercice 4 (Moins important). [3] On note $\mathcal{C}_n$ l'ensemble des carrés dans $\mathbb{Z}/n\mathbb{Z}$. Montrer que si aucun carré ne divise n, alors

$$\mathcal{C}_n + \mathcal{C}_n = \mathbb{Z}/n\mathbb{Z}$$

Que dire de la réciproque ?

Remarque 2. En particulier, l'exercice précédent montre qu'il est utile de regarder les sommes de deux carrés modulo 4, 8 ou 9 mais pas modulo 5 ou 6, qui n'ont pas de facteurs carrés.

Exercice 5. Soit N le nombre à 2015 chiffres $N = 333\cdots333$. Montrer que N n'est pas une somme de deux carrés.

Nous reviendrons sur la combinatoire additive dans $\mathbb{Z}/p\mathbb{Z}$ dans la dernière partie.

2 Les sommes de carrés dans $\mathbb{N}$

L'objet principal de cette section est de caractériser l'ensemble $\Sigma_2 = \mathcal{C} + \mathcal{C}$ des sommes de deux carrés. Nous savons déjà que celui-ci n'est pas égal à $\mathbb{N}$, et même qu'il ne contient aucun $\mathbb{N}_{\geqslant m}$, par exemple parce qu'il ne contient pas les nombres congrus à 3 modulo 4. Toutefois regarder modulo 4 n'est pas un critère suffisant, comme le montre le tableau des sommes de deux carrés $\leqslant 100$ suivant :

	0^2	1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2
0^2	0	1	4	9	16	25	36	49	64	81	100
1^2		2	5	10	17	26	37	50	65	82	
2^2			8	13	20	29	40	53	68	85	
3^2				18	25	34	45	58	73	90	
4^2					32	41	52	65	80	97	
5^2						50	61	74	89		
6^2							72	85	100		
7^2								98			

On peut faire un certain nombre d'observations et de conjectures à partir du tableau

Observation 1. Tous les nombres premiers congrus à 1 modulo 4 (en rouge) apparaissent. Les seuls nombres congrus à 1 modulo 4 qui n'apparaissent pas sont $21, 33, 57, 77$

3. Cet exercice nécessite de connaître le lemme chinois des restes

Observation 2. Certains nombres apparaissent plusieurs fois (on les a soulignés). Ils ne sont jamais premiers, et ils semblent tous être des multiples de 5, mais un étude plus poussée montre que

$$169 = 13 \times 13 = 13^2 + 0^2 = 12^2 + 5^2$$

$$221 = 17 \times 13 = 10^2 + 11^2 = 14^2 + 5^2$$

Observation 3. Dans les décompositions en facteur premier des nombres du tableau, les nombres premiers qui sont également dans le tableau apparaissent souvent. Les nombres premiers qui ne sont pas dans le tableau apparaissent toujours au moins au carré.

Exercice 6. En observant le tableau des sommes de deux carrés précédent, émettre des conjectures sur leur caractérisation.

2.1 Le cas des nombres premiers

Pourquoi donc s'intéresser d'abord aux nombres premiers et à la décomposition en produits des sommes de deux carrés ? Notre problème relève a priori de l'addition seulement, on voit mal comment les nombres premiers et les produits peuvent avoir un rôle. Pour comprendre l'intérêt de décomposer, réfléchissez un moment à cette question voisine (mais plus facile) :

Exercice 7. Est-ce que 30 est différence de deux carrés ?

Nous partirons donc sur cette voie.

Le but de cette partie est de démontrer la

Proposition 2 (Fermat)**.** *Soit* p *un nombre premier. Alors,* p *est somme de deux carrés si et seulement si* p *n'est pas congru à* 3 *modulo* 4.

Le sens "seulement si" a déjà été démontré. Si $p = 2$ le résultat est clair, on se concentrera donc sur le cas où p est congru à 1 modulo 4. Commençons par quelques rappels :

Inversibilité modulo p Soit p un nombre premier et x dans $\mathbb{Z}$ tel que $p \nmid x$. Alors il existe y tel que $xy \equiv 1\,[p]$. En effet, x et p sont premiers entre eux ; d'après le théorème de Bezout il existe u et v tels que

$$up + vx = 1$$

De sorte qu'il suffit de prendre y égal à v. En fait, n'importe quel y congru à v modulo p convient. De plus, si y et y' sont tels que $xy \equiv xy' \equiv 1\,[p]$ alors $p \mid x(y - y')$ mais comme $p \nmid x$, nous avons que $y \equiv y'$ modulo p. On peut donc définir l'inverse de la classe $\overline{x}$ dans $\mathbb{Z}/p\mathbb{Z}$ comme la classe $\overline{y}$, notée $\overline{x}^{-1}$ (d'après ce qui précède, l'inverse existe et il est unique). Dans $\mathbb{Z}/p\mathbb{Z}$, toutes les classes non nulles sont inversibles.

Depuis la section précédente, nous savons que $\overline{-1}$ est toujours une somme de deux carrés dans $\mathbb{Z}/p\mathbb{Z}$. En fait, on a un peu mieux quand $p \equiv 1\,[4]$:

Lemme 1. *Soit* p *un nombre premier impair. Si* $p \equiv 1\,[4]$ *alors l'équation*

$$s^2 = \overline{-1}$$

admet 2 *solutions opposées l'une l'autre dans* $\mathbb{Z}/p\mathbb{Z}$. *Si* $p \equiv -1\,[4]$ *cette équation n'admet pas de solution dans* $\mathbb{Z}/p\mathbb{Z}$

Démonstration. Commençons par remarquer que $\overline{-1}$ possède au plus deux racines carrées dans $\mathbb{Z}/p\mathbb{Z}$ (voir la solution de l'exercice 3). Regroupons les éléments de $S = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$ en paquets[4] de telle manière que pour tout $x \in S$, les éléments x, $-x$ et x^{-1} sont dans le même paquet. A quoi ressemblent nos paquets ? Les éléments dans le paquet contenant x sont x, $-x$, x^{-1} et $-x^{-1} = (-x)^{-1}$. Puisque p est impair, on a toujours $x \neq -x$. Par ailleurs $x = x^{-1}$ si et seulement si $x^2 = 1$, soit encore $(x+1)(x-1) = 0$ dans $\mathbb{Z}/p\mathbb{Z}$, ce qui implique $x = \pm\overline{1}$. Il y a donc trois types de paquets

1. Le paquet $\{-1, 1\}$
2. Les paquets de la forme $\{s, -s\}$ avec $s^{-1} = -s$, soit $s^2 = \overline{-1}$
3. Les paquets contenant 4 éléments $\left\{x, -x, x^{-1}, -x^{-1}\right\}$

Si $|S| = p - 1$ est divisible par 4, il y a un nombre impair de paquets du deuxième type. Il y en a donc un seul, formé de $\{s, -s\}$ avec $s^2 = \overline{-1}$

Exercice 8. Dans $\mathbb{Z}/11\mathbb{Z}$ puis dans $\mathbb{Z}/13\mathbb{Z}$, effectuer la dissection en paquets de la preuve précédente. Dans le second cas trouver les classes s telles que $s^2 = \overline{-1}$.

Exercice 9. Montrer que

$$(p-1)! \equiv -1\ [p]$$

En déduire une nouvelle preuve que $\overline{-1}$ est un carré quand $p \equiv 1\ [4]$. Est-elle si nouvelle ?

Preuve de la proposition Considérons les paires (x', y') d'entiers tels que $0 \leqslant x', y' \leqslant \sqrt{p}$. Il y en a exactement $(1 + E(\sqrt{p}))^2$, ce qui est strictement plus grand que p, car p n'est pas un carré parfait. D'après le principe des tiroirs, on sait donc que pour tout $s \in \mathbb{Z}$ il existe deux paires distinctes, disons (x', y') et (x'', y'') telles que

$$x' - sy' \equiv x'' - sy''\ [p]$$

Posons alors $x = |x' - x''|$ et $y = |y' - y''|$; nous obtenons que

$$x \equiv \pm sy\ [p]$$

avec $0 \leqslant x, y \leqslant \sqrt{p}$. Maintenant, si l'on se donne pour s une racine carrée de $\overline{-1}$, qui existe d'après le lemme, alors $x^2 \equiv -y^2$ modulo p. Comme par ailleurs

$$0 < x^2 + y^2 < 2p$$

on obtient que $p = x^2 + y^2$, ce qu'on voulait.

2.2 La multiplicativité de Σ_2 et le théorème des deux carrés.

La proposition suivante est assez miraculeuse.

Proposition 3 (Multiplicativité des sommes de carrés)**.** *Pour tous* $\sigma, \tau \in \Sigma_2$, $\sigma\tau \in \Sigma_2$

Démonstration. Voici une démonstration bien peu éclairante en une ligne : pour tous $x, y, z, t \in \mathbb{Z}$

$$(x^2 + y^2)(z^2 + t^2) = (xz - yt)^2 + (xt + yz)^2$$

En fait, cette identité possède une interprétation géométrique liée aux propriétés de la multiplication des entiers de Gauss.

4. Le mot "paquet" est utilisé pour dissimuler que nous formons des classes de classes.

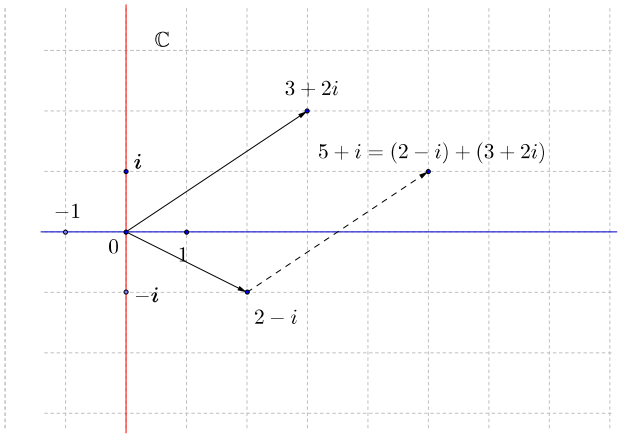

FIGURE 1 – addition des entiers de Gauss

Digression non essentielle sur les entiers de Gauss (pour les parimatheux qui n'ont pas trop froid aux yeux) On note $\mathbb{Z}[i]$ l'ensemble $\mathbb{Z} \times \mathbb{Z}$ muni des lois suivantes

$$(x, y) + (x', y') = (x + x', y + y')$$

$$(x, y) \times (x', y') = (xx' - yy', xy' + x'y)$$

On appelle i l'élément $(0, 1)$. On peut voir $\mathbb{Z}$ comme un sous-ensemble dans $\mathbb{Z}[i]$ des éléments de la forme $(x, 0), x \in \mathbb{Z}$. De plus, on peut réaliser géométriquement $\mathbb{Z}[i]$ comme l'ensemble des points à coordonnées entières du plan muni d'un repère orthonormé $(0, 1, i)$. Comment interpréter alors géométriquement ces deux opérations ? Nous renvoyons aux figures 2.2 et 2.2.

Remarque 3. La multiplication des nombres complexe (et en particulier des entiers de Gauss, que l'on peut voir comme des nombres complexes) est sur Youtube : voici la vidéo (chapitre 5).

Tout comme $\mathbb{Z}$, $\mathbb{Z}[i]$ possède une arithmétique intéressante ; il y existe une division euclidienne (la "grandeur" des éléments étant mesurée par leur norme), une notion de pgcd, un théorème de Bezout et un lemme de Gauss. Certains éléments appelés irréductibles jouent un rôle analogue aux nombres premiers dans $\mathbb{Z}$: il existe une unique décomposition en produit d'irréductibles (tout ces résultats se déduisent dans cet ordre, comme dans $\mathbb{Z}$). Ainsi par exemple, 11 est irréductible mais $13 = (3 + 2i)(3 - 2i)$ ne l'est pas dans $\mathbb{Z}[i]$. Tout ceci est très lié au théorème des deux carrés pour la raison suivante : décomposer n en deux carrés, c'est écrire n sous la forme

$$n = x^2 + y^2 = (x + iy)(x - iy)$$

Ceci doit éclairer légèrement le lien avec l'introduction de 2.1. Nous n'en dirons pas plus ici.

Nous avons à présent tous les ingrédients à notre disposition pour démontrer le

Théorème 2. *Soit n un entier naturel. Alors n est une somme de deux carrés si et seulement si, n est nul ou il se décompose en produit de facteurs premiers sous la forme*

$$n = 2^{\alpha} p_1^{\beta_1} \cdots p_r^{\beta_r} q_1^{2\gamma_1} \cdots q_s^{2\gamma_s} \tag{3}$$

Avec les $p_i \equiv 1$ et les $q_j \equiv -1$ modulo 4.

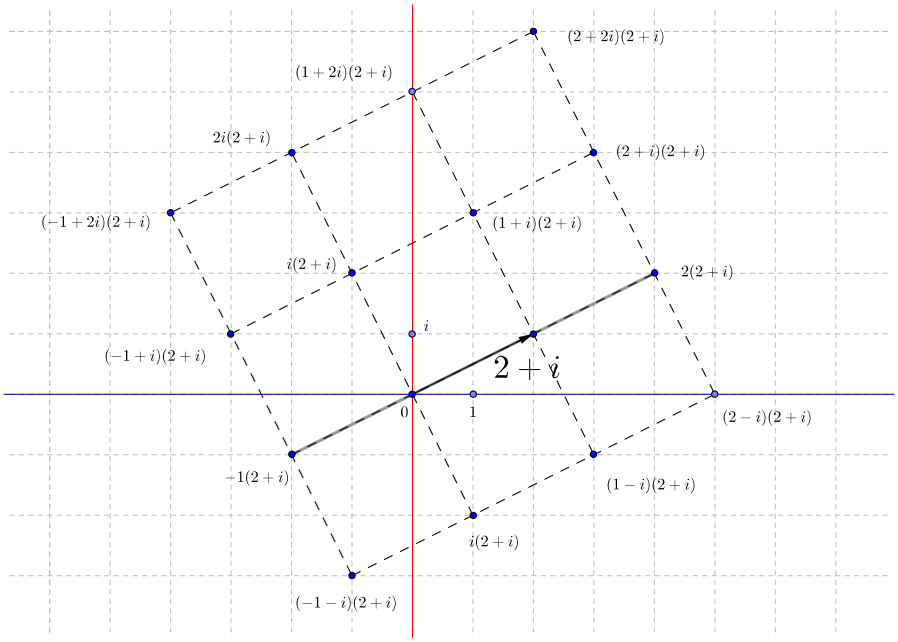

FIGURE 2 – Quelques entiers de Gauss multipliés par le nombre $2+i$. En particulier, leur norme (distance à l'origine) est multipliée par $\|2+i\| = \sqrt{5}$

Il y a deux parties dans ce théorème : le "si" et le "seulement si".

Démonstration (Du "si"). Soit n sous la forme donnée dans l'énoncé du théorème. 2 est somme de deux carrés. Par une récurrence utilisant la proposition 3, 2^α est dans Σ_2. D'après les propositions 2 et 3, $p_1^{\beta_1} \cdots p_r^{\beta_r}$ est une somme de deux carrés. Pour finir, $q_1^{2\gamma_1} \cdots q_s^{2\gamma_s}$ est égal à $(q_1^{\gamma_1} \cdots q_s^{\gamma_s})^2$, c'est donc un carré et en particulier, une somme de deux carrés.

Démonstration (Du "seulement si"). Nous utilisons le principe de la descente, cher à Fermat. Soit donc n une somme de deux carrés, et p premier divisant n congru à 3 modulo 4. Si $n = x^2 + y^2$ alors modulo p nous avons que

$$\overline{x^2} + \overline{y^2} \equiv 0$$

Si par l'absurde $p \nmid x$ et $p \nmid y$, posons u la classe $\overline{xy}^{-1}$; alors $u^2 = \overline{-1}$ dans $\mathbb{Z}/p\mathbb{Z}$, ce qui est exclu d'après un lemme précédent. Donc $p \mid x$ (par exemple) mais comme $p \mid n$, $p \mid y$ également. On en déduit que p^2 divise n. De plus

$$\frac{n}{p^2} = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$$

Donc n/p^2 est somme de deux carrés. Si par l'absurde le plus grand exposant e tel que $p^e \mid n$ était impair de la forme $2e'+1$, alors on aboutirait à une absurdité en réitérant ce raisonnement $e'+1$ fois.

2.3 Quelques friandises à base de sommes de carrés (à consommer sans modération)

Exercice 10. Résoudre dans $\mathbb{Z}^3$ l'équation

$$x^2 + y^2 = 7z^2$$

Exercice 11. Montrer que le 5ème nombre de Fermat

$$F_5 = 2^{2^5} + 1 = 62264^2 + 20449^2$$

n'est pas premier.

Remarque 4. Historiquement, c'est Euler qui a remarqué que F_5 n'est pas premier, mais il n'a pas utilisé cette technique. Euler a remarqué que l'on pouvait chercher des diviseurs éventuels sous la forme $64k + 1$, et 641 convient.

On définit $r_2(n)$ comme le nombre de décomposition en sommes de deux carrés $x, y \in \mathbb{Z}$. Ainsi, par exemple, $r_2(13) = 8$ puisque

$$13 = (\pm 3)^2 + (\pm 2)^2 = (\pm 2)^2 + (\pm 3)^2$$

Le principe de l'exercice précédent est que si p est premier, alors $r_2(p)$ est égal à 8 au plus. Il existe une expression de $r_2(n)$ en fonction du nombre de diviseurs de n congrus à 1 et à 3 modulo 4, que nous ne donnerons pas ici.

Si la fonction $r_2(n)$ est localement erratique, son comportement en moyenne peut être appréhendé par un argument géométrique. En effet, d'après le théorème de Pythagore $r_2(n)$ est exactement le nombre de points à coordonnées entières à distance n de l'origine, de sorte que :

$$R_2(N) = 1 + \sum_{n=1}^{N} r_2(n)$$

est exactement le nombre de points à coordonnées entières dans le disque de rayon $\sqrt{N}$. On en déduit que $R_2(N) \simeq \pi N$ (On pourrait rendre plus rigoureux ce signe $\simeq$ mais ce n'est pas l'essentiel) puis

$$\frac{1}{N} \sum_{n=1}^{N} r_2(n) \to \pi$$

Autrement dit, "en moyenne"[5], un nombre entier naturel possède $\pi/4$ décompositions en sommes de deux carrés d'entiers naturels.

2.4 Quatre carrés et bicarrés

Nous avons à peu près couvert le sujet des sommes de deux carrés (mis à part le nombre de décomposition). Tout entier n'est pas somme de trois carrés (cf. plus haut) mais pour quatre carrés, on n'arrive plus (essayez !) à trouver des restrictions dans les congruences (cf. l'exercice 17 pour un début d'explication), et pour cause :

5. On pourrait voir ceci comme une espérance, mais il faut préciser quelle loi de probabilité placer sur $\mathbb{N}$, ce qui n'est pas si évident.

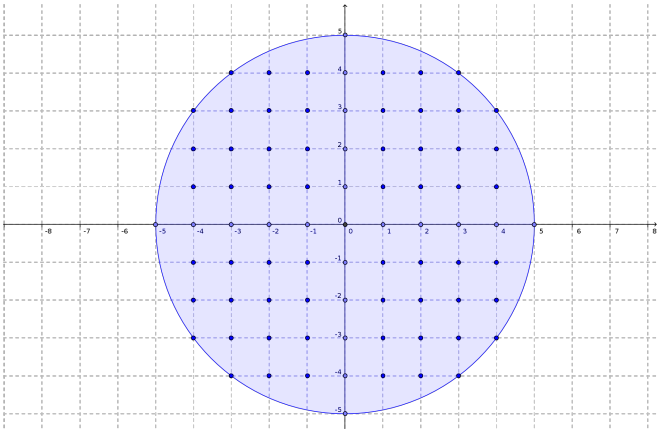

FIGURE 3 – Les 81 points à coordonnées entières dans le disque de rayon 5. Pour comparaison, $25\pi \simeq 78$

Théorème 3 (Lagrange)**.** *Tout entier est somme de quatres carrés.*

Il existe de nombreuses preuves du théorème des quatres carrés. Une preuve très élégante s'appuie sur la géométrie des nombres, qui a été exposée par Diego Izquierdo à Parimaths en 2014. En voici une autre en exercice :

Exercice 12 (Preuve du théorème de Lagrange - Difficile). On utilisera le résultat de l'exercice 3, ainsi que l'identité doublement miraculeuse[6] suivante :

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)\\ =&(ax+by+cz+dt)^2+(ay-bx+ct-dz)^2+(az-cx-bt+dy)^2+(at-dx+bz-cy)^2\end{aligned}$$

1. On se donne p un nombre premier et on cherche à montrer qu'il est somme de quatres carrés. Pourquoi cela suffit-il pour démontrer le théorème ?
2. Soit m le plus petit entier tel que l'équation
$$pm = a^2+b^2+c^2+d^2$$
admet une solution. Montrer que m existe, puis qu'il est impair.
3. En supposant par l'absurde $m \neq 1$ et en regardant les classes des a_i modulo m, contredire la minimalité de m. Conclure.

L'exercice suivant nous permet d'avancer (d'un petit pas) dans le problème de Waring :

Exercice 13 (D'après Liouville). Un bicarré est un entier de la forme x^4. En s'appuyant sur l'identité

$$6\left(\sum_{i=1}^{4} x_i^2\right)^2 = \sum_{1\leqslant i<j\leqslant 4}\left[(x_i+x_j)^4+(x_i-x_j)^4\right]$$

et en utilisant le théorème de Lagrange, montrer que tout entier est somme d'au plus 53 bicarrés.

6. De même que $\mathbb{Z}[i]$ est la raison du miracle de la multiplicativité de Σ_2, il existe un objet qui généralise les entiers de Gauss et explique cette identité

Exercice 14 (Nombres triangulaires). Les nombres triangulaires sont les nombre de la forme

$$T_n = \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$$

En utilisant le théorème de Lagrange, montrer que tout nombre entier est somme de trois nombres triangulaires.

En ce qui concerne les sommes de trois carrés, il existe également une caractérisation :

Théorème 4 (Legendre, Gauss). *$n \in \mathbb{N}$ est somme de trois carrés si et seulement si il n'est pas de la forme $4^\ell \cdot m$ avec $m \equiv 7\,[8]$.*

Les preuves ne sont pas plus longues, mais conceptuellement un peu plus difficiles, que celles des théorèmes des deux et des quatres carrés et il ne serait pas très raisonnable d'en donner une ici. Quoi qu'il en soit, il n'est d'ailleurs pas très difficile de voir que le théorème de Legendre implique celui de Lagrange : Tout $n \in \mathbb{N}$ peut s'écrire sous la forme $n = 4^\ell m$ avec m impair. Si m n'est pas congru à -1 modulo 8, n est somme de trois carrés ; sinon $4^\ell(m-1)$ est somme de trois carrés et

$$n = 4^\ell(m-1) + 4^\ell = 4^\ell(m-1) + (2^\ell)^2$$

3 Théorème de Cauchy-Davenport et applications

On reprend ici la discussion laissée en 1.2 ; Si $A, B \subseteq \mathbb{Z}/n\mathbb{Z}$, il reste à comprendre ce qui se passe pour $A + B$ quand $|A| + |B| \leqslant n$. Voici enfin le théorème promis à la fin de 1.1.

Théorème 5 (Cauchy ~ 1830, Davenport 1935). *Soit p un nombre premier, A et B deux parties non-vides de $\mathbb{Z}/p\mathbb{Z}$. Alors*

$$|A + B| \geqslant \min(p, |A| + |B| - 1) \tag{4}$$

Remarque 5. Suite à la proposition 1, certains enthousiastes auraient peut-être aimé écrire (voir carrément écrit) la généralisation suivante : si les $A_i \subseteq \mathbb{Z}/p\mathbb{Z}$ sont non-vides et si $|A_1|+\cdots+|A_m| > p$ alors $A_1 + \cdots + A_m = \mathbb{Z}/p\mathbb{Z}$. Ceci est faux (penser à ce qui se passe quand $A_i = \{a_i\}$) mais le théorème de Cauchy Davenport assure quand même que la même conclusion tient si

$$|A_1| + \cdots + |A_m| \geqslant p + m - 1$$

Par ailleurs il existe une description du cas d'égalité dans 4 qui permet de montrer que le pronostic des enthousiastes est "souvent" valide (essentiellement, dès que les A_i ne sont pas des images de progressions arithmétiques dans $\mathbb{Z}/p\mathbb{Z}$).

Preuve du théorème de Cauchy-Davenport Voici une définition préalable

Définition 1. *Soient $A, B \subseteq \mathbb{Z}/n\mathbb{Z}$ et $e \in \mathbb{Z}/n\mathbb{Z}$. On définit la e-transformée de Dyson de (A, B) comme le couple $(A(e), B(e))$ avec*

$$A(e) = A \cup (B + e)$$

$$B(e) = B \cap (A - e)$$

La transformée de Dyson vérifie les propriétés suivantes :

1. Si $e \in A - B$ alors $B(e) \neq \emptyset$
2. $A(e) + B(e) \subseteq A + B$
3. $|A(e)| + |B(e)| = |A| + |B|$

Exercice 15. Vérifier les propriétés de la transformation de Dyson.

Démonstration (Du théorème de Cauchy-Davenport). On peut d'ores et déjà exclure les cas où $|A + B| > p$ ou bien $|A| = 1$ ou $|B| = 1$ à la lumière de tout ce qui précède. Par l'absurde, considérons un contre-exemple, où B est pris de cardinal minimal $\geqslant 2$. Soient b_1 et b_2 distincts dans B. Choisissons $a \in A$; alors $a - b_1 \notin A - b_2$. Puisque $b_2 - b_1$ est non nul, ses multiples parcourent tout $\mathbb{Z}/p\mathbb{Z}$ (ceci parce que p est premier). Posons $e = a - b_1$ et considérons la e-transformée de (A, B). b_1 est dans $B(e)$ qui n'est donc pas vide. De plus, si par l'absurde on avait $b_2 \in B(e)$ alors $b_2 + e$ serait dans A ; donc il existerait $a' \in A$ tel que $a + b_2 - b_1 = a'$, ce qui constitue une contradiction. Puisque $B(e)$ est inclus dans B et ne contient pas b_2, le couple $(A(e), B(e))$ constitue un nouveau contre-exemple avec $B(e)$ strictement plus petit. Ceci est absurde.

Applications du théorème de Cauchy-Davenport

Exercice 16 (Théorème d'Erdös-Ginzburg-Ziv). On cherche à démontrer le théorème suivant : de toute suite $(a_1, \ldots, a_{2n-1})$ d'éléments de $\mathbb{Z}$, on peut extraire n termes $a_{i_1}, a_{i_2}, \ldots a_{i_n}$ telle que

$$n \mid a_{i_1} + a_{i_2} + \cdots + a_{i_n}$$

1. On suppose que $n = p$ est premier. On ordonne les a_i dans l'ordre croissant et on pose $A_i = \{a_i, a_{i+p-1}\}$. Pourquoi peut-on supposer $|A_i| \geqslant 2$ pour tout i ? A l'aide du théorème de Cauchy-Davenport, montrer que dans ce cas

$$A_1 + \cdots + A_{p-1} = \mathbb{Z}/p\mathbb{Z}$$

2. Conclure le cas où $n = p$ est premier
3. En procédant par récurrence forte, déduire le cas général

Remarque 6. On peut vérifier que $2n - 1$ est optimal dans l'exercice précédente. En effet soient a_i les $2n-2$ éléments définis par $a_i = 0$ pour $1 \leqslant i < n$ et $a_i = 1$ pour $n \leqslant i \leqslant 2n-2$; alors on vérife que l'on ne peut pas extraire de somme nulle des a_i.

Exercice 17 (Retour sur le problème de Waring). Soit p un nombre premier. Pour cet exercice on pourra admettre le fait suivant, qui peut être vu comme un raffinement du petit théorème de Fermat : Il existe un[7] élément h non nul dit générateur dans $\mathbb{Z}/p\mathbb{Z}$ d'ordre exactement $p - 1$, c'est à dire que

$$\forall m \in \mathbb{Z},\ h^m = \overline{1} \implies p - 1 \mid m$$

Un tel élément est dit générateur. Pour tout $k \geqslant 2$ un entier, on considère $\mathcal{P}(k)$ l'ensemble des puissances k-ièmes dans $\mathbb{Z}/p\mathbb{Z}$, et on note $g_p(k)$ l'entier minimal tel que

$$g_p(k) \wedge \mathcal{P}(k) = \mathbb{Z}/p\mathbb{Z}$$

1. Montrer que $|\mathcal{P}(k)| = \frac{p-1}{(k,p-1)} + 1$ où (a, b) désigne le pgcd de a et b. [On pourra s'inspirer de l'exercice 3]

7. On peut montrer qu'il y en a $\varphi(p-1)$ tels éléments, où φ est l'indicatrice d'Euler

2. A l'aide du théorème de Cauchy-Davenport, montrer que si $g > k$ alors $g \wedge \mathcal{P}(k) = \mathbb{Z}/p\mathbb{Z}$. En déduire

$$g_p(k) \leqslant k+1 \tag{5}$$

Ainsi dans $\mathbb{Z}/p\mathbb{Z}$ pour p arbitrairement grand tout élément est somme de quatre cubes. Pour comparaison, dans $\mathbb{N}$ il en faut 9. En fait, il a été démontré que 7 cubes suffisent pour les nombres assez grands, et on conjecture que 4 cubes suffisent pour les nombres assez grands [8].

Pour conclure, voici le tableau des premières valeurs et estimations de $g(k)$ et de $G(k)$ du problème de Waring (ce dernier étant le nombre minimal pour que tout entier assez grand soit somme de $G(k)$ puissance de k).

k	$g(k)$	$G(k)$
1	1	1
2	4	4
3	9	$4 \leqslant G(3) \leqslant 7$
4	19	16

La détermination de $G(4) = 16$ est dûe à Davenport. Tout entier est somme de 19 bicarré, le résultat de l'exercice 13 (53 bicarrés) peut donc être considérablement amélioré.

On peut vérifier que l'inégalité de l'exercice 17 est quasiment optimale, ce qui indique que l'on ne peut pas vraiment aller plus loin dans la minoration de $G(k)$ seulement à l'aide de restrictions obtenues par des congruences. De fait, les meilleures minoration de $G(k)$ dont l'on dispose sont souvent (mais pas toujours) proches de $k+1$. La majoration est un tout autre problème. Les mathématiciens l'ont attaquée à l'aide de la théorie analytique des nombres, en particulier à l'aide de la *méthode du cercle*, initiée par Hardy et Littlewood, qui a connu de nombreux raffinements depuis.

4 Solutions des exercices

Solution (1). Soit $A \times B$ le produit cartésien de A et B, c'est-à-dire l'ensemble des couples (a, b) avec $a \in A$ et $b \in B$. On a une application surjective

$$\begin{aligned} A \times B &\longrightarrow A + B \\ (a, b) &\mapsto a + b \end{aligned}$$

De sorte que $|A + B| \leqslant |A \times B| = |A| \cdot |B|$. Pour l'optimalité, pensons à une situation de division euclidienne : $A = \{0, 1, \ldots, k-1\}$ et $B = \{0, k, 2k, \ldots, (\ell-1)k\}$ alors $A + B = \{0, 1, \ldots \ell k - 1\}$ qui est de cardinal ℓk donc cette inégalité ne peut pas être améliorée. En ce qui concerne la minoration, voir le théorème suivant.

Solution. 2 On vérifie que dans $\mathbb{Z}/8\mathbb{Z}$, $3 \wedge \{\overline{0}, \overline{1}, \overline{4}\} = \{\overline{0}, \overline{1}, \ldots \overline{6}\}$; $\overline{7}$ n'est pas dedans. Or $2015 \equiv 2000 + 15 \equiv 7\,[8]$, et on a clairement que $\overline{3 \wedge \mathcal{C}} = 3 \wedge \overline{\mathcal{C}}$

8. Au passage, 2015 est somme de quatre cubes et ceci d'une unique manière. Saurez-vous trouvez lesquels ?

Solution (3). Si $p = 2$, c'est clair ; on supposera p impair dans ce qui suit. Reformulons, il s'agit de montrer que $\overline{-1}$ est somme de deux carrés dans $\mathbb{Z}/p\mathbb{Z}$. En vertu de la proposition il suffit de montrer que si $\mathcal{C}_p$ est l'ensemble des carrés dans $\mathbb{Z}/p\mathbb{Z}$, alors $2|\mathcal{C}_p| > p$. Considérons l'application f de $\mathbb{Z}/p\mathbb{Z}$ dans $\mathcal{C}_p$ qui à x associe x^2. Puisque

$$f(x) = f(y) \iff p \mid x^2 - y^2 \iff p \mid (x+y)(x-y) \iff x \equiv \pm y\,[p]$$

les éléments de $\mathbb{Z}/p\mathbb{Z}$ ont 0, 1 ou 2 antécédent par f, et $\bar{0}$ est le seul à avoir un unique antécédent. Finalement

$$|\mathcal{C}_p| = 1 + \frac{p-1}{2} = \frac{p+1}{2} \tag{6}$$

Et on a ce que l'on souhaitait.

Solution (4). D'après l'exercice précédent, ceci est vrai quand $n = p$ est un nombre premier. Maintenant, écrivons

$$n = p_1 p_2 \cdots p_r$$

Pour tout k dans $\mathbb{Z}$, pour tout $i \in \{1 \dots r\}$ il existe x_i, y_i dans $\mathbb{Z}$ tels que

$$x_i^2 + y_i^2 \equiv k\,[p_i]$$

D'après le lemme chinois des restes, il existe x, y dans $\mathbb{Z}$ tels que pour tout i

$$x \equiv x_i\,[p_i]$$

$$y \equiv y_i\,[p_i]$$

On a alors

$$x^2 + y^2 \equiv k\,[p]$$

Solution (5). Le reste de N modulo 9 est aisément accessible via la somme de ses chiffres : on trouve

$$N \equiv 6[9]$$

Or $6 \equiv -3$ n'est pas somme de deux carrés modulo 9. Ceci conclut.

Solution (6). On renvoie au théorème des deux carrés.

Solution (10). Deux méthode : soit on invoque le théorème des deux carrés et on remarque que la valuation[9] $\nu_7(7z^2)$ est toujours impaire si z est non nul (donc il n'y a pas de solution non nulle) ou bien on remarque que si z est une solution éventuelle non nulle, alors soit $7 \mid x$ et $7 \mid y$, soit $\overline{xy}^{-1}$ est racine carrée de $\overline{-1}$ dans $\mathbb{Z}/7\mathbb{Z}$, ce qui n'est pas possible. Ceci amorce un raisonnement de type descente. Conclusion : l'unique solution est $(0, 0, 0)$

Solution (16). (Théorème d'Erdös-Ginzburg-Ziv)

1. Puisque les a_i sont dans l'ordre croissant, si $a_{i+p-1} = a_i$ alors il y a égalité de tous les a_j entre ces deux termes. En particulier

   $$a_i + \cdots + a_{i+p-1} = p a_i$$

   et il ne reste plus rien à démontrer. Supposons donc $|A_i| \geqslant 2$; nous avons

   $$|A_1| + \cdots + |A_{p-1}| = 2(p-1) \geqslant p + p - 2$$

9. C'est-à-dire le plus grand entier α tel que $7^\alpha \mid 7z^2$

2. Le nombre $-a_{2p-1}$ s'écrit est congru modulo p à une somme de $p-1$ nombres a_i qui le précèdent, d'après la question 1. On a démontré le théorème pour p premier.
3. On procède par récurrence forte. Supposons la propriété montrée pour $2, \dots, n-1$. Si n est premier il n'y a rien à montrer, sinon $n = pn'$ avec p premier et $n' < n$. On écrit alors

$$2n - 1 = p\,(2n' - 1) + p - 1$$

Soient $a_1, \dots a_{2n-1}$ dans $\mathbb{Z}/n\mathbb{Z}$. Par application répétée de la proposition pour p, il existe $E_1, \dots E_{2n'-1}$ dans $\{1, \dots 2n-1\}$ disjoints et de cardinaux p tels que pour tout i,

$$\sum_{x \in E_i} x \in p\mathbb{Z}/n\mathbb{Z}$$

D'après l'hypothèse de récurrence sur n', il existe $E_{i_1}, \dots E_{i_{n'}}$ tels que la somme des éléments dans les E_{i_k} est 0. On a ainsi $pn' = n$ éléments de somme nulle parmi les a_i.

Sources

Une partie du matériel présent ici (la combinatoire additive) m'a été inspirée par un exposé d'Eric Ballandreau à l'IHES le 3 septembre 2015. Voici deux ouvrages qui m'ont été utiles :

– *Proofs from the Book*, M. Aigner, G.M. Ziegler (pour le théorème des deux carrés)

– *Additive Number Theory, Inverse Problems and the Geometry of Sumsets*, M.B. Nathanson

Le premier consacre l'un de ses chapitres au théorème des deux carrés et il est accessible. Le second est spécialisé, mais la lecture des deux premiers chapitres ne demande pas plus de prérequis que la compréhension de ce texte. Le théorème de Cauchy-Davenport ainsi que des généralisations y sont démontrés.