Magistère L3, 2024 : Carrés

R. Bacher

Quelques références:

La preuve de Rousseau (réciprocité quadratique):

https://stacky.net/files/115/RousseauQR.pdf

Wikipedia donne une preuve assez lisible (il faut remplir quelques trous calculatoires) du thm des quatre carrés :

https://fr.wikipedia.org/wiki/Théorème_des_quatre_carrés_de_Lagrange

????? (Je suis preneur de suggestions)

Avertissement : Ces notes sont à mon usage personnel. Elles ne sont donc pas nécessairement très complètes. Je n'ai pas extirpé toutes les erreurs par respect pour la biodiversité.

Rappels sur la réciprocité quadratique

Symbole de Legendre : p un premier impair, a dans $\mathbb{F}_p$. Le symbole de Legendre $\left(\frac{a}{p}\right)$ vaut 0 si $a = 0$, 1 si a est un carré non-nul et -1 si a est un non-carré. C'est un homomorphisme de groupe de $\mathbb{F}_p^*$ dans $\{\pm 1\}$ de noyau le sous-groupe (multiplicatif) des carrés non-nuls. On a $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. (Calcul possible par exponentiation rapide, cf. RSA).

On a la réciprocité quadratique pour le symbole de Legendre (déterminé aprs complétion par les valeurs pour $a = -1$ et $a = 2$).

Symbole de Jacobi : $\left(\frac{a}{n}\right)$ pour n impair et a dans $\mathbb{Z}$ qcque. Également un homomorphisme (de $(\mathbb{Z}/n\mathbb{Z})^*$ dans $\{\pm 1\}$, étendu par 0 aux éléments non-inversibles modulo n). Défini par les formules de la réciprocité quadratique (et la complétion pour $a = -1$ et $a = 2$).

Utilisation: Calcul rapide du symbole de Legendre (ou de Jacobi) par un algorithme similaire à l'algo d'Euclide. Exo: calculer quelques exemples, e.g. $\left(\frac{182}{257}\right)$ etc. (cet algo nécessite de passer par le symbole de Jacobi. Par contre, pas besoin de savoir factoriser effectivement.)

Interprétation en termes de signature (Lemme de **Zolotarev**) : La multiplication par un élément a inversible agit par permutation sur $(\mathbb{Z}/n\mathbb{Z})^*$. Le

symbole de Legendre (pour n premier), respectivement le symbole de Jacobi (pour n impair quelconque) est simplement la signature de cette permutation. (Preuve pour Legendre: a d'ordre $\alpha | p-1$ dans $\mathbb{F}_p^*$ agit par $(p-1)/\alpha$ cycles de longueur α. C'est donc de signature -1 si et seulement si $(p-1)/\alpha$ est impair (α est alors pairs car $p-1 = \alpha\frac{p-1}{\alpha}$ est pair). L'élément a est donc une puissance impaire d'un générateur du groupe cyclique $\mathbb{F}_p^*$. ...(Compléter la preuve!))

Rappel: Interprétation de la signature d'une permutation en termes de 'croisements' de diagrammes.

1 Une preuve (relativement) simple de la réciprocité quadratique

En simplifiant à l'extrême, on peut ranger les preuves dans un spectre se terminant par deux types (pour simplifier) de preuves particulièrement 'jolies' : D'une part, les preuves les plus accessibles ('Proofs from the book') mais qui n'expliquent généralement pas le pourquoi et preuves 'à la Grothendieck' maximisant la compréhension (preuves passant par les raisons profondes rendant inéluctable la vérité d'un énoncé, impossibles à comprendre pour le néophyte car nécessitant souvent un énorme contexte.)

La plupart des preuves sont évidemment quelque part entre ces deux extrêmes.

Remarque: Cette 'classification' est une simplification est elle est surtout valable pour l'algèbre et l'arithmétique. En analyse et en géométrie, les meilleurs preuves réunissent généralement les deux qualités.

(Preuve de G. Rousseau, J. Austr. Math. Soc **51**, 423-425.)

p, q deux premiers impairs distincts. Posons

$$G = (\mathbb{Z}/pq\mathbb{Z})^*/\{\pm 1\} = \left((\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^*\right)/U$$

où $U = \{(1,1),(-1,-1)\}$.

Calculons le produit $\pi = \prod_{g\in G} g \pmod U$ (dans un groupe commutatif fini, le produit de tous les éléments est soit l'identité, soit un élément d'ordre 2 car tous les éléments d'ordre > 2 peuvent être regroupés avec leur inverse et les éléments d'ordre ≤ 2 forment un $\mathbb{F}_2$-espace vectoriel. Le résultat est l'unique élément d'ordre 2 si le sous-groupe des élts d'ordre 1 ou 2 a deux éléments et c'est l'identité sinon).

On va calculer π de deux façons : la première fait appaître le facteur correctif $(-1)^{(p-1)(q-1)/4}$, la deuxième fait intervenir les deux symboles de Legendre $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$.

Comme

$$\{1,\dots,p-1\}\times\{1,\dots,(q-1)/2\}$$

est un système de représentants, on a $\pi=\pi_1$ pour

$$\pi_1=\left(((p-1)!)^{(q-1)/2},(((q-1)/2)!)^{p-1}\right)\ .$$

En utilisant Wilson ($(p-1)!\equiv -1 \pmod p$ pour tout premier p) et

$$(((q-1)/2)!)^2=(-1)^{(q-1)/2}(q-1)!$$

nous avons donc

$$\begin{aligned}\pi_1&=\left((-1)^{(q-1)/2},(-(-1)^{(q-1)/2})^{(p-1)/2}\right)\\&=\left((-1)^{(q-1)/2},(-1)^{(p-1)/2}(-1)^{(p-1)(q-1)/4}\right)\end{aligned}$$

D'autre part, on peut travailler directement dans $(\mathbb{Z}/pq\mathbb{Z})^*$ (modulo le sous-groupe $\{\pm1\}$, évidemment). On doit alors considérer le produit A des entiers dans $\{1,\dots,(pq-1)/2\}$ qui sont premiers à pq. Modulo p on obtient alors

$$\begin{aligned}A&=\frac{\left(\prod_{i=1}^{p-1}i\right)\left(\prod_{i=1}^{p-1}p+i\right)\cdots\left(\prod_{i=1}^{p-1}\frac{q-3}{2}p+i\right)\left(\prod_{i=1}^{(p-1)/2}\frac{q-1}{2}p+i\right)}{q\cdot 2q\cdot 3q\cdots\frac{p-1}{2}q}\\&\equiv\frac{((p-1)!)^{(q-1)/2}((p-1)/2)!}{q^{(p-1)/2}((p-1)/2)!}\pmod p\\&\equiv(-1)^{(q-1)/2}\left(\frac{q}{p}\right)\pmod p\end{aligned}$$

(car $q^{(p-1)/2}\equiv\left(\frac{q}{p}\right) \pmod p$). En combinant avec l'expression symétrique pour $A \pmod q$ nous avons donc pour $\pi=\pi_2 \pmod U$

$$\begin{aligned}\pi_2&=(A\pmod p,A\pmod q)\\&=\left((-1)^{(q-1)/2},(-1)^{(p-1)/2}(-1)^{(p-1)(q-1)/4}\right)\\&=\left((-1)^{(q-1)/2}\Big/\left(\frac{q}{p}\right),(-1)^{(p-1)/2}\Big/\left(\frac{p}{q}\right)\right).\end{aligned}$$

Comme $\pi_1\pi_2^{-1}\in U=\pm(1,1)$ ous obtenons

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

Compléments Valeurs π selon congruence p, q modulo 4:

p	q	$\left((-1)^{(q-1)/2}, (-1)^{(p-1)/2}(-1)^{(p-1)(q-1)/4}\right)$
1	1	$(1,1)$
1	-1	$(-1,1)$
-1	1	$(1,-1)$
-1	-1	$(-1,1)$

Exo: G un groupe abélien fini noté multiplicativement.

$$\prod_{g\in G} g = \prod_{g\in \ker(\varphi_2)} g$$

pour l'homomorphisme $\varphi_2(x) = x^2$ (montrer que c'est un endomomorphisme de groupe pour un groupe abélien).

Soit $\psi : x \longmapsto x^{-1}$. Montrer que ψ est un endomorphisme de groupe pour les groupes abéliens. Montrer que le sous-groupe $\ker(\varphi_2)$ est le sous-groupe des éléments fixes par ψ.

Montrer qu'il suffit de comprendre le sous-groupe des élements d'ordre un diviseur de 4 dans $(\mathbb{Z}/p\mathbb{Z})^* \times \mathbb{Z}/q\mathbb{Z})^*$. Remplacer le premier calcul dans la preuve par des arguments théoriques n'utilisant que les solutions de $x^4 = 1$ dans les corps $\mathbb{F}_p$ et $\mathbb{F}_q$.

Soit G un groupe tel que $x^2 = 1$ pour tout x dans G. Montrer que G est un $\mathbb{F}_2$-espace vectoriel (et donc commutatif).

$B(m,n)$ le groupe de Burnside libre avec m générateurs $x_1, \ldots, x_m$ et exposant n (i.e. $w^n = 1$ pour tout produit fini $w = x_{i_1}x_{i_2}\cdots x_{i_l}$ de générateurs dans $B(m,n)$ mais on n'impose aucune autre relation supplémentaire (on ferme cependant pour la conjugaison)). On a $B(1,n) = \mathbb{Z}/n\mathbb{Z}$ et $B(m,2) = \mathbb{F}_2^m$. On sait que $B(m,3), B(m,4)$ et $B(m,6)$ sont finis et que $B(m,n)$ est infini pour $m \geq 2$ et $n \geq 8000$ (on saît un peu plus pour n impair). Pour $B(2,5)$ (par exemple) on ne saît pas si c'est un groupe fini.

2 Infinitude des nombres premiers

(voir Paulo Ribenboim : The New Book of Prime Number Records)

Remarque sur $\mathbb{N}$: appartenance de 0 à $\mathbb{N}$:

$\mathbb{N} = \{1, 2, \ldots\}$ (souvent) chez les anglosaxons (anglais et americains) : suggère les ordinaux (von Neumann : il faudrait commencer les ordinaux également avec 0. Justification $\omega, \omega+1, \ldots$). On peut aussi dire que $\{1, 2, 3, \ldots\}$ est naturel quand on travaille avec le semi-groupe multiplicatif.

$\mathbb{N} = \{0, 1, 2, \ldots\}$ suggère plutôt les cardinaux.

Arithmétique (addition et multiplication) possible avec les cardinaux, pas naturel avec les ordinaux.

Théorie des cardinaux et ordinaux infinis très différente. (Mentionner hypothèse du continu.)

Inclusions $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$.

(quaternions et octonions, cf. plus tard (peut-être)).

$(\mathbb{N}, +)$ est le monoide libre à un générateur.

$(\mathbb{N}^*, \cdot)$ est le monoide commutative libre avec un nombre dénombrable de générateurs (les nombres premiers). (La liberté de ce monoide est l'unicité de la décomposition en premiers.)

On considére la suite définie par $s_1 = 2$ et $s_{n+1} = 1 + \prod_{j=1}^{n} s_j$.

Calculer les premiers termes.

Vérifier qu'on a $s_{n+1} = s_n^2 - s_n + 1$. Preuve?

Que peut-on dire du pgcd de s_i et s_j?

Soit p_j le plus petit nombre premier qui divise s_j. Calculer p_j pour les premières valeurs de s_j.

Est-ce que cela permet de montrer qu'il y a une infinité de nombres premiers?

Variation : Une preuve de Goldbach (C'est le Goldbach d'une célèbre conjecture affirmant que tout entier pair ≥ 4 est somme de deux premiers.) Prenons $F_0 = 3$ et $F_{n+1} = 2 + \prod_{j=0}^{n} F_j$.

Calculer les premiers termes et verifier qu'on a $F_n = 2^{2^n} + 1$. (Le nombre F_n s'appelle parfois le n-ième nombre de Fermat. Fermat croyait, à tort, qu'ils étaient tous premiers.)

Prouver par récurrence que $F_n = 2^{2^n} + 1$. (Indication : Utiliser la récurrence $F_{n+1} - 2 = \prod_{j=0}^{n} F_j$ et l'identité remarquable $(2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1$.)

Conclure.

Autre preuve. Lemme de rappel: Le nombre de monômes de degré n en d variables est égal à $\binom{n+d-1}{d-1} = \binom{n+d-1}{n}$.

Deux preuves: Bijective: Préparer $n + d - 1$ cases alignés et choisir n cases pour y mettre une variable sans indice. L'indice (dans $\{0, \ldots, d-1\}$ est donné par le nombre de cases libre à gauche.

2. Séries génératrices: La somme de tous les monômes en $x_1, \ldots, x_d$ est obtenue en développant $\prod_{j=1}^{d} \frac{1}{1-x_j}$. Le nombre de monômes de degé n est donc donné par le coefficient de z^n dans $(1-z)^{-d} = \sum \binom{-d}{n}(-z)^n$.

Supposons qu'il n'existe que k nombres premiers distincts.

L'ensemble des entiers naturels strictement positifs serait alors en bijection (en admettant l'unicité, sinon on obtient seulement une surjection des monômes sur $\mathbb{N}^*$) avec les monômes en $p_1, \ldots, p_k$ (et $(\mathbb{N}^*, \cdot)$ serait un

semigroupe (monoide avec identité, monoide : ensemble muni d'un produit associatif) commutatif engendré par k générateurs).

Comme $p_i \geq 2$, les 2^n entiers dans $\{1, \ldots, 2^n\}$ seraient alors représentables par des monômes de degré $\leq n$ et le nombre de ces monomes, donné par

$$\sum_{m=0}^{n} \binom{m+k-1}{k-1} = \binom{m+k}{k}$$

(ajouter une variable supplémentaire pour rendre tous ces monômes de degé exactement n) croît seulement polynomialement. Une fonction polynomiale perd contre une exponentielle.

Une preuve d'Euler (18-ième, 1707-1783)

Pour p un premier utiliser l'identité

$$1 + \frac{1}{p-1} = \frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots$$

(et la factorisation unique des entiers en puissances de nombres premiers) pour formellement montrer l'égalité

$$\prod_p \frac{1}{1-\frac{1}{p}} = \sum_{n \geq 1} \frac{1}{n}.$$

Le produit à gauche est sur l'ensemble des nombres premiers. Si cet ensemble est fini, le produit est fini et donne un nombre rationnel en contradiction avec la divergence de $\sum_{n \geq 1} \frac{1}{n}$.

La jolie preuve topologique de Furstenberg : Topologie sur $\mathbb{Z}$ en définissant comme ouverts l'ensemble vide et les réunions (quelconques, finies ou infinies) de progressions arithmétiques non-constantes (de la forme $a\mathbb{Z}+b$ avec $a > 0$). (Vérifiez que cela définit une topologie : $\emptyset$ et $\mathbb{Z}$ sont ouverts, des réunions (quelconques) et des intersections finies d'ouverts sont des ouverts).

On observe que les ouverts non-vides sont des sous-ensembles infinis de $\mathbb{Z}$.

D'autre part, le complémentaire d'une progression arithmétique est une réunion (fini) de progressions arithmétiques. C'est donc un ouvert. L'ensemble fini non-vide

$$\{-1, 1\} = \bigcap_p (\mathbb{Z} \setminus p\mathbb{Z})$$

est donc une intersection d'ouverts qui n'est pas un ouvert. Ceci implique que c'est une intersection d'un ensemble infini d'ouverts.

Question : Où l'arithmétique se cache-t-elle?

3 Infinitude des premiers de la forme $4\mathbb{N}-1$ et $4\mathbb{N}+1$

La preuve d'Euclide est un cas particulier de l'observation suivante :

Soit M un entier naturel divisant un produit AB de deux entiers naturels premiers entre eux.

Alors $A+B$ et $A-B$ (pour $A > B+1$) sont premiers à M (et ne font donc intervenir uniquement des nombres premiers qui ne divisent pas M).

Dans la preuve d'Euclide on considère $A = M$ et $B = 1$ pour M un produit fini de nombre premiers. On montre donc qu'on peut toujours agrandir strictement l'ensemble des nombres premiers.

Pour montrer qu'il y a une infinitude de premiers de la forme $4\mathbb{N}-1$ on utilise un entier $4A$ divisible par 4 et $B = 1$ pour obtenir $4A-1 \equiv 3 \pmod 4$ qui doit donc posséder un diviseur $\equiv 3 \pmod 4$.

L'infinitude des premiers de la forme $4\mathbb{N}+1$ est un peu plus subtile : On utilise le fait qu'un entier impair de la forme a^2+b^2 est soit un carré, soit divisible par un premier de la forme $4\mathbb{N}+1$ (Girard-Fermat). On considère alors

$$4A^2+1$$

pour A impair. Ceci implique que $4A^2+1 \equiv 5 \pmod 8$ ne peut pas être un carré parfait (car seuls $0, 1$ et 4 sont des carrés modulo 8). Le nombre $4A^2+1$ fait donc intervenir un diviseur premier dans $4\mathbb{N}+1$ (ou, plus précisément, dans $8\mathbb{N}+5$).

4 Pythagore

Preuves pour Pythagore (pas traité! Je les ai laissées pour le fun.)

Chapître essentiallement non traité, laissé pour les plaisirs de la procrastination.

Existe-t-il un lien entre Pythagore et l'identité $\sin^2 x + \cos^2 x = 1$?

4.1 Triplets pythagoriciens

Un triplet pythagoricien est un triplet (a, b, c) de trois entiers naturels non-nuls tel que $a^2+b^2 = c^2$. Les nombres a, b, c sont donc les trois longueurs d'un triangle rectangle.

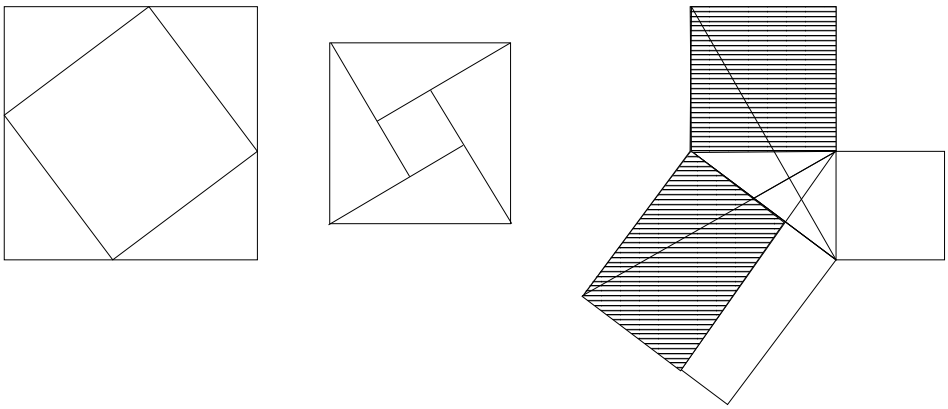

Figure 1: À gauche celle attribuée à Pythagore, à droite celle d'Euclide.

On dira qu'un triplet pythagoricien est *primitif* si le pgcd de ses entiers vaut 1.

Trouvez les 12 **triplets pyth. primitifs avec** $c \leq 75$**.**

Montrer que $a^2 + b^2 = c^2$ implique l'existence de $m + in$ dans $\mathbb{Z}[i]$ tel que $a + ib = (m + in)^2$.

Proof. On se ramène à un triplet primitif. On a alors $c \equiv 1 \pmod 2$ et on peut supposer a impair et $b = 2\beta$ pair. On a $b^2 = 4\beta^2 = (c + a)(c - a)$ et

$$\beta^2 = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right)$$

et $\frac{c+a}{2}, \frac{c-a}{2}$ sont deux entiers premiers entre eux (car leur somme c et leur différence a le sont). Ce sont donc deux carrés parfaits m^2 et n^2 et on a $a = m^2 - n^2, b = 2mn, c = m^2 + n^2$. □

Tout triplet pythagoricien est donc de la forme $(m^2 - n^2, 2mn, m^2 + n^2)$ pour m, n dans $\mathbb{N}$.

Soit $\mathbb{S}^1$ le cercle unité de $\mathbb{C}$. Décrire les éléments de $\mathbb{S}^1 \cap \mathbb{Q}[i]$. Montrer que ces éléments forment un groupe et décrire les éléments d'ordre fini (de torsion) de ce groupe.

Vérifiez l'identité $(m^2 + n^2)^2 = (m^2 - n^2)^2 + (2mn)^2$ **et cherchez des valeurs pour** m **et** n **correspondant à vos triplets.**

Calculez z^2 **et les normes des nombres complexes** z **et** z^2 **pour** $z = m + in$**.**

Exprimez le plus grand entier c **(la longueur de l'hypothénuse) de vos triplets pythagoriciens comme une somme de deux carrés.**

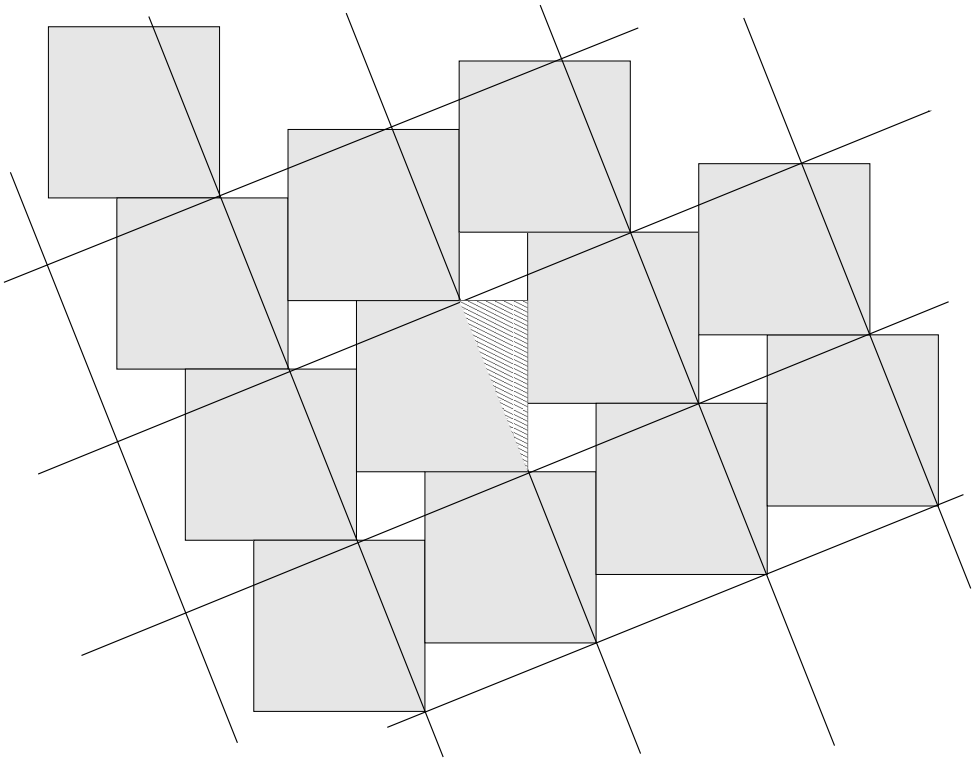

Figure 2: Une preuve observable sous l'effet de la poussée d'Archimède.

Soit $A = m^2 + n^2$ et $B = s^2 + t^2$ deux sommes de deux carrés. Que peut-on dire du produit AB? (Indication: la norme $|x + iy| = \sqrt{x^2 + y^2}$ est multiplicative : La norme d'un produit est le produit des normes.)

Faites la liste des nombres premiers jusqu'à 100. (Par exemple en utilisant le crible d'Eratosthène.)

Lequels de ces nombres premiers s'écrivent comme somme de deux carrés?

Utilisation des carrés (mod 4) pour montrer que $n \equiv 3 \pmod 4$ n'est jamais somme de deux carrés.

Preuve de Dolan que tout premier $\equiv 1 \pmod 4$ est somme de deux carrés.

Utiliser ce que vous avez appris pour compter le nombre de triplets pythagoricien primitifs avec $c \leq 200$.

Monter que $a + ib$ admet une racine carré dans $\mathbb{Z} + i\mathbb{Z}$ si (a, b, c) est un triplet pythagoricien primitif.

Thm de Fermat (ou Girard-Fermat) sur les sommes de deux carrés.

En déduire qu'un entier c est la longueur de l'hypothénuse associée à un triplet pythagoricien primitif si et seulement si c ne fait intervenir que des facteurs premiers de la forme $1 + 4\mathbb{N}$. Le nombre de triplets pythagoriciens

primitifs distincts, normalisés par $a < b < c$, est alors donné par 2^{e-1} où e est le nombre de facteurs premiers distinct (tous dans $1 + 4\mathbb{N}$) de c.

Trouver les deux triplets (pyth. prim.) associés à $c = 65$ et à $c = 85$. Trouver les quatre triplets (pyth. prim.) associés à $c = 5 \cdot 13 \cdot 17 = 1105$.

Mentionner le thm de Lagrange (somme de quatre carrés).

éventuellement, mentionner la preuve de Don Quichotte.

5 Un point de vue géométrique

Montrer l'identité

$$1 = \left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 .$$

Montrer que les trois points

$$(-1,0), \frac{1}{1+t^2}(1-t^2, 2t), (1, 2t)$$

sont alignés. En déduire une bijection entre points rationnels de l'interval ouvert $(0,1)$ et les points entiers rationnels à coordonnées strictement positives sur le cercle unité (centré à l'origine) du plan euclidien.

Poser $t = \frac{n}{m}$ pour en déduire que les trois points rationnels

$$(-1,0), (a/c, b/c), (1, 2n/m)$$

sont alignés pour le triplet pythagoricien

$$a = m^2 - n^2, b = 2mn, c = m^2 + n^2 .$$

6 La preuve de A. Christopher

Soit p un nombre premier impair.

On considére deux rectangles avec des largeurs $L > l$ entières différentes, de hauteurs H, h entières (pas nécessairement différentes) avec somme des aires $LH + lh = p$.

On considère le diagramme de Young associé pour définir les 'rectangles conjugués' de largeurs $L' = H + h > l' = H$ et de hauteurs $H' = L - l$ et $h' = l$. Ceci définit une involution avec unique point fixe donné par $((p+1)/2) \times 1$ et $1 \times ((p-1/2)$ (car p est premier).

On peut aussi considérer le quart de tour qui échange largeurs et hauteurs et qui est bien défini sauf pour $H = h$. Ce dernier cas implique $H = h = 1$

par primalité de p. Il existe alors $(p-1)/2$ telles paires de rectangles et comme $(p-1)/2 \equiv 0 \pmod 2$ pour $p \equiv 1 \pmod 4$, le quart de tour sur le nombre impair de (pairs de rectangles) définit une involution avec un point fixe donné par deux carrés.

7 La preuve de Liouville-(Heath-Brown)-Zagier-A.Spivak-Northshield

Version de Sam Northshield (Am. Math. Monthly 97(2),144)

Ici, $\{a, a\}$ est considéré comme le multi-ensemble (ensemble avec multiplicités) contenant l'élément a deux fois.

$p \equiv 1 \pmod 4$ un nombre premier. On considère

$$\mathcal{S} = \{\{a, b\}, a, b \in \mathbb{N}, \exists n \in \mathbb{N}, p - 4ab = n^2\}.$$

$\{1, (p-1)/4\}$ est dans $\mathcal{S}$ (pour $n = 1$). (Observation : n est toujours impair.)

Lemme Si $\{a, b\}$ appartient à $\mathcal{S}$, alors exactement deux parmi les quatre expressions (pas nécessairement toutes distinctes) sont dans $\mathcal{S}$:

$$\{a, b - a \pm n\}, \{b, a - b \pm n\} \ .$$

Preuve: On vérifie que les quatre expressions correspondent à des solutions de $p-4xy = z^2$ avec x, y, z dans $\mathbb{Z}$. On utilise la primalité pour montrer que $|a - b| \neq n$ et on distingue les cas $|b - a| \gtrless n$ en tenant compte du signe de $b - a$ dans le cas $|b - a| > n$.$\square$

On relie chaque élément $\{a, b\}$ de $\mathcal{S}$ par une arête orientée à ses deux images donné par la correspondance du Lemme. (Une correspondance de A vers B est un sous-ensemble $\mathcal{C}$ quelconque de $A \times B$. Elle fait correspondre à un élément a de A le sous-ensemble $\{b \in B, (a, b) \in \mathcal{C}\}$ de B et on peut donc la voir comme une sorte de "multifonction".)

On obtient une unique (pour $p > 5$) boucle en $\{1, (p-1)/4\}$ (l'autre image est $\{1, (p-9)/4\}$). On vérifie que l'existence d'une arête orientée de s_1 vers s_2 dans $\mathcal{S}$ implique l'existence d'une arête orientée de s_2 vers s_1. La composante connexe de $\{1, (p-1)/4\}$ est donc essentiellement un chemin fini qui doit s'arêter sur un sommet $s_\omega \in \mathcal{S}$ de la forme $\{a, a\}$ car les deux arêtes issues de s_ω doivent revenir en arrière sur l'unique prédécesseur $\{a, \sqrt{p - 4a^2}\}$ de s_ω. Le sommet s_ω donne alors l'identité $p-(2a)^2 = n^2$ (pour $n = \sqrt{p - 4a^2}$).

Exo: Construire ce graphe de sommets $\mathcal{S} = \mathcal{S}_p$ (avec ses arêtes orientées) pour quelques nombres premiers $p \equiv 1 \pmod 4$. Construire ce graphe pour $p = 229$.

Cette preuve est en principe constructive mais malheureusement pas très efficace: Le graphe $\mathcal{S}$ est énorme (choisir un entier impair $n < \sqrt{p}$ et factoriser $a \cdot b = (p - n^2)/4$ pour obtenir une solution $\{a, b\}$.

Le graphe $\mathcal{S}$ possède un unique 'chemin linéaire' (ressemblant à un segment) et peut-être plusieurs 'cycles', cf. l'exemple $p = 229$ ci-dessus.

Où a-t-on utilisé la primalité de p, la congruence modulo 4 de p?

8 Une preuve de Stan Dolan (pas faite et pas relue!)

Theorem 8.1. *Tout nombre premier de la forme* $1 + 4\mathbb{N}$ *est somme de deux carrés.*

La preuve suivante (pas si simple en fait) est une retranscription de "S.Dolan: A very simple proof of the two-squares theorem. The Mathematical Gazette, Vol. 105, Issue 564 (November 2021), page 511". C'est probablement encore une version déguisée de la preuve de Zagier.

Proof. Soit p un premier de la forme $1 + 4\mathbb{N}$.

$$p = (x + y + z)^2 - 4xz = (x - z)^2 + y(2x + y + 2z) \tag{1}$$

n'a qu'un nombre fini de solutions (x, y, z) à valeurs dans $\mathbb{N} = \{0, 1, 2, \ldots\}$. En effet, comme p est premier, ce n'est pas un carré parfait et on doit avoir $y > 0$. Comme $(x - z)^2 \geq 0$, on a donc $2x + y + 2z \leq \frac{p}{y} \leq p$ ce qui implique x, y, z dans $\{0, 1, 2, \ldots, p\}$.

Montrons que le nombre fini de telles solutions (avec x, y, z dans $\mathbb{N}$) est impair : Remarquons d'abord que échanger le rôle de x et de z préserve les solutions et transforme une solution (x, y, z) avec $x \neq z$ en une autre solution (z, y, x). Les solutions avec $x \neq z$ viennent donc par paires. Considérons maintenant une solution $(x, y, z) = (z, y, x)$ avec $z = x$ (toujours avec x et y dans $\mathbb{N}$). On a alors

$$p = (2x + y)^2 - (2x)^2 = (2x + y + 2x)(2x + y - 2x) = (4x + y)y \ .$$

Comme p est premier, on ne peut pas avoir $x = 0$ (sinon $p = y^2$ est un carré parfait). On a donc $4x + y > y$ et la primalité de p implique $y = 1$ et $x = (p - 1)/4$ (qui est bien un entier car p est de la forme $1 + 4\mathbb{N}$). Il existe donc une unique solution avec $x = z$ et un nombre inconnu (mais fini) de paires de solutions distinctes $(x, y, z), (z, y, x)$ avec $z \neq x$. Le nombre total de solutions (dans $\mathbb{N}$) de l'équation (1) est donc bien un nombre impair.

L'astuce diabolique de Dolan est de reécrire

$$(x+y+z)^2 - 4xz$$

sous la forme

$$(x+y-z)^2 + 4yz \ .$$

En développant les deux expressions, on obtient bien l'égalité

$$(x+y+z)^2 - 4xz = (x+y-z)^2 + 4yz \ .$$

Comme ces deux expressions coincident, l'équation

$$p = (x+y-z)^2 + 4yz \tag{2}$$

a également un nombre impair de solutions (les mêmes que $p = (x+y+z)^2 - 4xz$) avec x, y, z dans $\mathbb{N}$.

Observons que $x = 0$ implique $p = (y-z)^2 + 4yz = (y+z)^2$ ce qui est impossible car le premier p ne peut pas être un carré parfait.

Considérons d'abord une solution avec $y \neq z$ et fixons l'ensemble $\{a, b\} = \{y, z\}$ formé par ces deux entiers distincts. Comme y et z sont les deux derniers éléments d'une solution $(x, y, z) \in \mathbb{N}^3$ de (2), l'entier

$$p - 4yz = (x+y-z)^2$$

est un carré parfait non-nul car p est premier. Notons $C = |x+y-z|$ sa racine positive. Si $-C \leq y-z \leq C$, alors $x = C - (y-z) = C - y + z$ (le cas $y - z = C$ ou $-C$ est impossible) et on obtient une deuxième solution $(C - z + y, z, y) \in \mathbb{N}^3$ correspondant à l'échange entre z et y.

Si $|y-z| > C$, on peut supposer $y - z < -C$ (le cas $y - z > C$ impliquerait $|x+y-z| > C$ pour $x \geq 0$ ce qui est impossible). On obtient alors deux solutions $(-C-y+z, y, z)$ et $(C-y+z, y, z)$ (correspondant à $x = -C-(y-z)$ et $x = C - (y-z)$).

Ceci montre que les solutions de $p = (x+y-z)^2 + 4yz$ (dans $\mathbb{N}^2$) avec $y \neq z$ viennent par pairs. Comme le nombre total des solutions est impair, il existe donc (au moins) une solution avec $z = y$ exprimant $p = x^2 + (2y)^2$ comme une somme de deux carrés. □

9 La preuve de Grace

Pour p premier congrue à 1 modulo 4 et i entier tel que $i^2 \equiv -1 \pmod{p}$, on considère le sous-réseau

$$\Lambda = \{(x, y) \in \mathbb{Z}^2, x + iy \equiv 0 \pmod{p}\}$$

d'indice p dans $\mathbb{Z}^2$. On a $\Lambda = \mathbb{Z}(i,-1)+\mathbb{Z}(p,0)$. Comme on a $-y+ix \equiv i(x+iy) \pmod{p}$, le réseau Λ est invariant par le quart de tour $(x,y) \longmapsto (-y,x)$. Soit (a,b) un vecteur non-nul de norme minimale non-nulle dans Λ. On a alors $\Lambda = \mathbb{Z}(a,b)+\mathbb{Z}(b,-a)$ et le carré de sommets $(0,0),(a,b),(b,-a),(a+b,b-a)$ est un domaine fondamental d'aire $p = a^2+b^2$ l'indice de Λ dans $\mathbb{Z}^2$. $\square$

La preuve de Grace est algorithmiquement très efficace: on calcule i par exponentiation rapide (prendre $i = g^{(p-1)/4}$ pour g un non-carré modulo p).

On calcule ensuite un vecteur minimale de $\Lambda = \mathbb{Z}(i,-1) + \mathbb{Z}(p,0)$ par réductions de Gauss (qui est essentiellement encore une variation de l'algo d'Euclide).

Complément : **La formule de Pick** Soit P un polygone à sommets entiers, d'intérieur connexe. (On suppose que P est la fermeture de son intérieur.) L'aire de P est alors donnée par $\frac{1}{2}\sharp(\partial P \cap \mathbb{Z}^2) + \sharp(\mathrm{Int}(P) \cap \mathbb{Z}^2) - 1$.

Preuve: La formule est valable par "découpe" le long d'un segment (ou d'une ligne brisé) à sommets entiers. On se ramène donc à des triangles "vides" n'intersectant $\mathbb{Z}^2$ qu'en ses sommets. Recollant un tel triangle Δ avec son opposé, on obtient un domaine fondamental pour $\mathbb{Z}^2$.

10 Le théorème de Lagrange

Théorème Tout entier naturel est somme de quatre carrés (entiers).

Pour la preuve on utilise la multiplication dans les quaternions. Il suffit donc de montrer le théorème pour les nombres premiers congrus à 3 modulo 4 (pour les autres, on peut utiliser Fermat: $n = a^2+b^2$ implique $n = a^2+b^2+0^2+0^2$).

Soit $p \equiv 3 \pmod 4$. Soit a le plus petit carré de $\mathbb{Z}/p\mathbb{Z}$ (identifié à $\{0,\ldots,p-1\}$, comme d'habitude) tel que $a+1$ est un non-carré. Comme -1 est également un non-carré, la classe de $-a-1$ est un carré modulo p. Soit $b^2 \equiv -a-1 \pmod{p}$. On a donc $a^2+1+b^2 \equiv 0 \pmod{p}$. On considère maintenant le sous-réseau

$$\Lambda = \mathbb{Z}(a,b,1,0) + \mathbb{Z}(b,-a,0,1) + \mathbb{Z}(p,0,0,0) + \mathbb{Z}(0,p,0,0)$$

d'indice p^2 (le quotient est $(\mathbb{Z}/p\mathbb{Z})^2$) de $\mathbb{Z}^2$. Tous les produits scalaires parmi deux éléments de Λ sont divisibles par p. Les normes au carré d'éléments dans Λ sont donc dans $p\mathbb{N}$. Soit (d,e,f,g) un vecteur non-nul de norme minimale dans Λ. On a $p|d^2+e^2+f^2+g^2$. On a terminé si $p = d^2+e^2+f^2+g^2$. Sinon on a $d^2+e^2+f^2+g^2 \geq 2p$. Les boules ouvertes de rayon $\sqrt{\frac{p}{2}}$ centrées en les éléments de Λ ne s'intersectent donc pas et sont donc de volume (quadridimensionnel) $\leq p^2$. Or le volume d'une boule de rayon r dans l'espace euclidien de dimension 4 est donné par $\frac{\pi^2}{2}r^4$ ce qui donne un

volume plus grand que p^2 pour $r^2 = \frac{d^2+e^2+f^2+g^2}{4} \geq \frac{p}{2}$. Ceci est impossible car le volume du domaine fondamental d'un sous-réseau d'indice fini de $\mathbb{Z}^d$ est égal à son indice. $\square$

Compléments

Le problèmes des trois carrés est plus difficile.

L'ensemble des entiers qui sont somme de deux carrés rationels est de densité nulle dans $\mathbb{N}$. L'ensemble des entiers qui sont somme de deux cubes rationels est de densité strictement positive dans $\mathbb{N}$. (Les cubes ne sont généralement pas des entiers!)

Les octonions (construction par les entiers d'Eisenstein modulo 7, lien avec le plan de Fano) donnent un produit sur les octuplets de carrés.

Le groupe des quaternions unitaires agit par isométries sur $\mathbb{R}^3$ (par conjugaison des quaternions purement imaginaires) avec noyau ± 1. Cela définit le revêtement spin de SO(3).