Extrait du livre *The sensual (quadratic) form* de John H. Conway (assisté par Francis Y. C. Fung)
Post-scriptum : un avant-goût de la théorie des nombres
Trois théorèmes célèbres

Dans ce post-scriptum, nous allons prouver trois théorèmes célèbres. Ce sont la loi notoire de réciprocité quadratique, le fait que la signature d'une forme quadratique unimodulaire paire soit un multiple de 8, et le théorème célèbre de Legendre des trois carrés. On en déduira quelques conséquences du théorème de Legendre, incluant l'universalité de certaines formes à 4 variables, et on finira par expliquer pourquoi aucune forme ternaire définie positive rationnelle n'est universelle.

La définition de Zolotarev du symbole de Jacobi

Pour un nombre impair n dont la factorisation en nombres premiers est $pqr...$, Jacobi a défini son symbole comme étant

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\left(\frac{a}{r}\right)\ldots,$$

un produit de symboles de Legendre. Même s'il était clair à partir de ses nombreuses propriétés que le symbole de Jacobi était un objet très naturel, il fallut un certain temps avant que Zolotarev n'en trouve une définition ayant davantage de sens : $\left(\frac{a}{n}\right)$ est le signe de la permutation obtenue en multipliant par a modulo n. Dans ce chapitre, on adoptera la définition de Zolotarev.

On rappelle que toute permutation π d'un ensemble fini a un *signe*, qui est juste égal à -1 si un nombre impair de cycles dans π sont de longueur paire. Maintenant on écrira "$\times a \bmod n$" pour la permutation de $\{0, ..., n-1\}$ correspondant à la multiplication par a. Ainsi

$$\times 3 \bmod 11 = (0)(1,3,9,5,4)(2,6,7,10,8).$$

Puisque celle-ci n'a pas de cycle de longueur paire, $\left(\frac{3}{11}\right) = +1$.

Cette définition amène à une preuve extrêmement simple du théorème de réciprocité quadratique. Il est remarquable que cette preuve n'utilise ni la notion de

Traduction : Denise Vella-Chemla, janvier 2024.

nombre premier, ni même celle de nombre carré. On utilisera pourtant le fait que l'opération *signe* d'une permutation est multiplicative.

On dira qu'un nombre est *positif modulo* m s'il est congruent modulo m à un nombre strictement compris entre 0 et $\frac{1}{2}m$ et *négatif modulo* m si à la place il est congruent à un nombre appartenant strictement au domaine $\left(-\frac{1}{2}m, 0\right)$. Le nombre $\frac{1}{2}m$ est *ambigu modulo* m.

Cinq lemmes

On évalue d'abord $\left(\frac{-1}{n}\right)$.

Lemme 1. $\left(\frac{-1}{n}\right)$ *est le signe de* n *modulo 4.*

En d'autres termes, $\left(\frac{-1}{n}\right)$ est égal à 1 si n est de la forme $4k+1$ et est égal à -1 si n est de la forme $4k-1$.

Preuve. Ceci est immédiat à partir de la définition. Par exemple, $\left(\frac{-1}{11}\right)$ et $\left(\frac{-1}{13}\right)$ sont les signes des permutations

$$(0)(1,-1)...(5,-5) \quad \text{and} \quad (0)(1,-1)...(6,-6),$$

notamment -1 et 1, puisqu'ils ont, respectivement, 5 et 6 transpositions. □

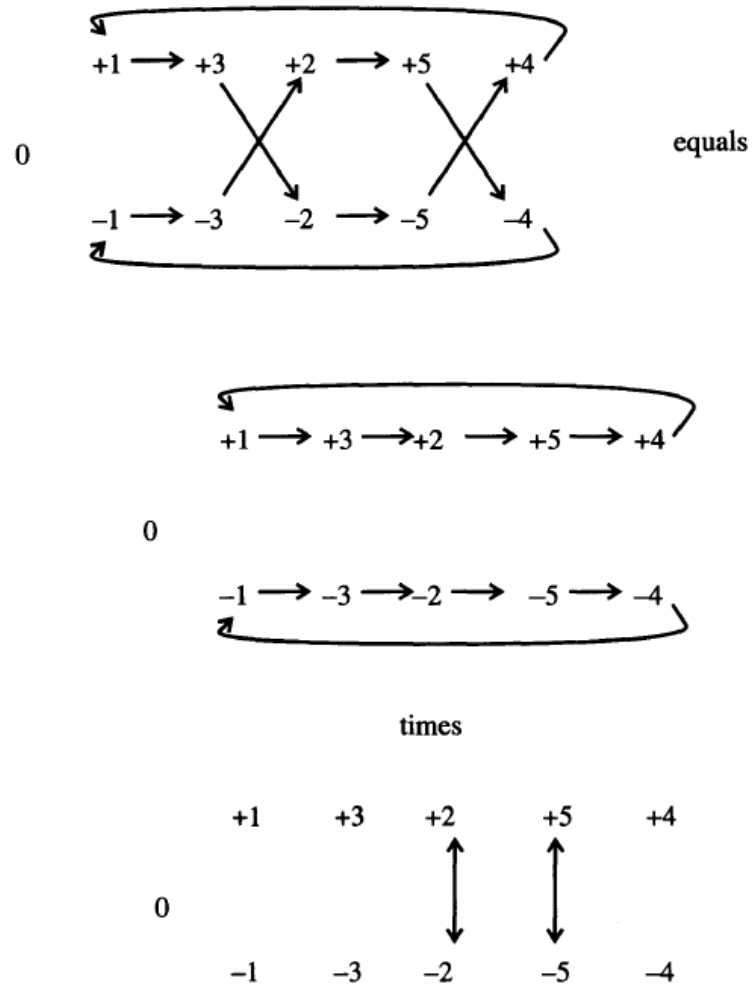
Lemme 2. On a $\left(\frac{a}{n}\right) = (-1)^s$, *où* s *est le "nombre de changements de signe" pour* $\times a \bmod n$*, notamment le nombre de nombres positifs* $k \bmod n$ *pour lesquels* ak *est négatif* $\bmod n$.

Preuve. On va considérer le cas $\left(\frac{3}{11}\right)$. Pour cela, écrivons les nombres échangés par la permutation $\times 3 \bmod 11$, avec leur propre signe :

$$(0)(+1,+3,-2,+5,+4)(-1,-3,+2,-5,-4)$$

On analyse cela dans la figure ci-dessous qui montre que le nombre de points de croisements qui compte le nombre de changements de signes est $s = 2$. La figure montre que cette permutation se factorise comme le produit de deux permutations

$$(0)(1,3,2,5,4)(-1,-3,-2,-5,-4) \text{ et } (2,-2)(5,-5)$$



La première de ces permutations est une permutation qu'on pourrait appeler "multiplication absolue par 3," obtenue en multipliant par 3 excepté qu'on préserve le signe alors que la seconde consiste en les corrections de signes nécessaires.

Dans le cas général, la multiplication absolue par a mod n est une permutation paire, puisque c'est le produit de deux permutations exactement de la même forme, alors que la permutation de changement de signe consiste en s transpositions, et

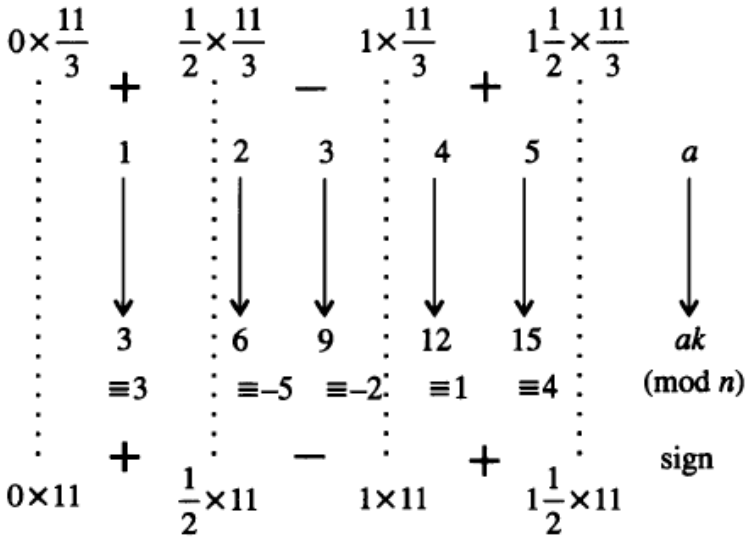
a donc pour signe $(-1)^s$ □

Pour n'importe quel nombre fixé a, le symbole $\left(\frac{a}{n}\right)$ peut être évalué pour tout n en utilisant ce lemme ; par exemple, $\left(\frac{2}{n}\right) = 1$ ou -1 selon que $n \equiv \pm 1$ ou ± 3 modulo 8.

Lemme 3. *Si $a > 0$, alors s est le nombre d'entiers strictement compris entre 0 et $n/2$ qui appartiennent à des intervalles de la forme*

$$\left[\left(l - \frac{1}{2}\right)\frac{n}{a}, \quad l\frac{n}{a}\right]$$

Preuve.



La figure rend cela immédiat. Les lignes en pointillés montrent les changements de signes de + à − quand ak passe à travers un nombre de la forme $\left(l - \frac{1}{2}\right)n$ et les changements de signes inverses de − à + quand ak passe à travers un nombre de la forme ln. □

Lemme 4. (Périodicité du symbole de Jacobi en n)
Si $m \equiv \pm n \pmod{4a}$, alors $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$

Preuve. Si on ajoute ou soustrait un multiple de $4a$ à n, toutes les extrémités des intervalles dans le lemme 3 changent par des nombres pairs, donc s change par un nombre pair. Aussi le symbole $\left(\frac{a}{-n}\right)$ est égal à $\left(\frac{a}{n}\right)$, puisque la multiplication par a modulo $-n$ est la même que la multiplication par a modulo n. □

Lemme 5. *Si m et n sont deux nombres impairs premiers entre eux dont la somme est un multiple positif de 4, alors $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$.*

Preuve. Écrivons $m + n = 4a$. Alors

$$\left(\frac{m}{n}\right) = \left(\frac{4a}{n}\right) = \left(\frac{a}{n}\right) = \left(\frac{a}{m}\right) = \left(\frac{4a}{m}\right) = \left(\frac{n}{m}\right).$$

Ceci est dû au fait que multiplier par m modulo n est la même chose que multiplier par $4a$ modulo n, ce que l'on peut faire en multipliant deux fois par 2 (ce qui n'affecte pas le signe) et en multipliant alors par a.

Réciprocité pour le symbole de Jacobi

La formulation habituelle de la loi de réciprocité pour le symbole de Jacobi est le

Théorème. *Si m et n sont deux nombres impairs positifs premiers entre eux, alors $\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)$ à moins que m et n ne soient tous les deux négatifs modulo 4, auquel cas $\left(\frac{m}{n}\right)$ et $\left(\frac{n}{m}\right)$ sont distincts.*

Preuve. Il est facile de voir que le lemme 5 contient cette assertion. On discute trois cas en utilisant le fait que $\left(\frac{m}{-n}\right) = \left(\frac{m}{n}\right)$ (puisque la multiplication modulo $-n$ est la même que la multiplication modulo n) :

1) *Signes opposés modulo 4.* Dans ce cas, le lemme 5 donne le théorème directement. Par exemple, $\left(\frac{11}{13}\right) = \left(\frac{13}{11}\right)$ parce que $11 + 13$ est divisible par 4.
2) *Les deux positifs modulo 4.* On considère 5 et 13. Ici, le lemme 5 montre que

$$\left(\frac{13}{5}\right) = \left(\frac{13}{-5}\right) = \left(\frac{-5}{13}\right) = +\left(\frac{5}{13}\right).$$

parce que $13-5$ est un multiple positif de 4, et $\left(\frac{-1}{13}\right) = +1$ par le lemme 1.

3) *Tous les deux négatifs modulo 4.* On considère 7 et 11, et on applique le lemme 5 pour trouver

$$\left(\frac{11}{7}\right) = \left(\frac{11}{-7}\right) = \left(\frac{-7}{11}\right) = -\left(\frac{7}{11}\right)$$

puisque $11-7$ est un multiple positif de 4, et $\left(\frac{-1}{11}\right) = -1$ par le lemme 1.

Cette preuve a supprimé beaucoup du mystère de la loi de réciprocité quadratique en utilisant le symbole de Jacobi de Zolotarev plutôt que le symbole de Legendre. Sinon, on suit l'exemple d'une preuve de Scholz de 1939 [Scho].

Symboles de Legendre et symboles linéaires de Jacobi

Pour montrer que la loi de réciprocité implique la loi habituelle de réciprocité quadratique, on doit montrer que le symbole de Jacobi $\left(\frac{a}{p}\right)$ comme défini par Zolotarev coïncide avec le symbole de Legendre traditionnel quand p est un nombre premier impair.

Pour faire cela, on cite le théorème d'Euler qui énonce que le groupe multiplicatif des entiers modulo p est un groupe cyclique d'ordre $p-1$. Mais si g est un générateur de ce groupe, alors la permutation "$\times g \bmod p$" est un $(p-1)$-cycle, et donc $\left(\frac{g^k}{p}\right) = (-1)^k$ ce qui établit le résultat souhaité.

Une façon traditionnelle d'exprimer la loi de réciprocité est

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

en supposant que m et n sont premiers entre eux.

Pour simplifier notre travail avec les p-signatures et les p-excès, il sera pratique d'introduire une version linéaire du symbole de Jacobi, dont la valeur est un entier modulo 8. On définit

$$\left[\frac{m}{n}\right] \quad = \quad 0 \quad \text{ou} \quad 4$$

selon que

$$\left(\frac{m}{n}\right) \quad = \quad -1 \quad \text{ou} \quad 1.$$

La loi de réciprocité devient maintenant

$$\left[\frac{m}{n}\right] + \left[\frac{n}{m}\right] \equiv (m-1)(n-1) \pmod 8.$$

La relation globale

Lors du quatrième exposé, on a défini les invariants σ_p, appelés p-signatures, d'une forme rationnelle quadratique, dont les valeurs sont des entiers ou des entiers modulo 8. On a aussi défini les p-excès e_p par

$$e_p(f) = \sigma_p(f) - \dim(f) \qquad \text{si} \quad p \neq 2,$$

et

$$e_2(f) = \dim(f) - \sigma_2(f).$$

Maintenant puisque chaque e_p peut être calculé juste à partir de la version p-adique de la forme, on s'attendrait naturellement à ce que les e_p soient indépendants. Pourtant, il y a une relation globale remarquable :

La somme de tous les p-excès est un multiple de 8.

La même relation a habituellement été exprimée en disant que le produit de certains invariants est égal à 1, et donc, on connait habituellement ce résultat sous le nom de "la formule du produit". La p-signature pour la forme 1-dimensionnelle $[a] = [p^\alpha A]$ a été définie dans le quatrième exposé comme étant

$$p^\alpha \ \text{ ou } p^\alpha + 4,$$

le 4 étant présent quand a est un anti-carré p-adique, c'est-à-dire quand α est impair et quand A est un non résidu quadratique modulo p. En fonction de notre symbole linéaire de Jacobi, cela devient

$$p^\alpha + \left[\frac{A}{p^\alpha}\right].$$

On peut généraliser cela ! Si π est n'importe quel ensemble de nombres premiers impairs, alors on définira la π-*signature* de $[a]$ comme étant

$$\pi(a) + \left[\frac{\pi'(a)}{\pi(a)}\right],$$

où $\pi(a)$ et $\pi'(a)$ sont les portions de a composées de nombres premiers dans π et dans l'ensemble complémentaire π', respectivement. Le π-*excès* e_π de $[a]$ est défini comme étant égal à 1 de moins, notamment :

$$\pi(a) - 1 + \left[\frac{\pi'(a)}{\pi(a)}\right].$$

La π-signature et le π-excès d'une forme générale $f = [a, b, c, ...]$ sont définis comme étant les sommes

$$\sigma_\pi(f) = \sigma_\pi(a) + \sigma_\pi(b) + \cdots$$

et

$$e_\pi(f) = e_\pi(a) + e_\pi(b) + ...$$

de telle façon que $e_\pi(f) = \sigma_\pi(f) - \dim(f)$.

Théorème. Soient π_1 et π_2 deux ensembles disjoints de nombres premiers impairs, et π leur union. Alors $e_\pi \equiv e_{\pi_1} + e_{\pi_2} \pmod 8$.

Preuve. Soit $a = P_1P_2A$, où P_1 et P_2 sont les parties π_1 et π_2 de a. Alors

$$e_{\pi_1}(a) = (P_1 - 1) + \left[\frac{P_2}{P_1}\right] + \left[\frac{A}{P_1}\right]$$

$$e_{\pi_2}(a) = (P_2 - 1) + \left[\frac{P_1}{P_2}\right] + \left[\frac{A}{P_2}\right]$$

$$e_\pi(a) = (P_1P_2 - 1) + \left[\frac{A}{P_1}\right] + \left[\frac{A}{P_2}\right].$$

Donc le théorème découle immédiatement de la loi de réciprocité

$$(P_1 - 1)(P_2 - 1) \equiv \left[\frac{P_1}{P_2}\right] + \left[\frac{P_2}{P_1}\right] \pmod 8.$$

Qu'en est-il des ensembles de nombres premiers contenant 2 ? On peut faire que le résultat d'additivité continue d'être respecté par ces ensembles, simplement en définissant e_π comme étant $-e_{\pi'}$ pour n'importe lequel de ces ensembles. Cela est consistant avec la définition ci-dessus du 2-excès.

On a maintenant démontré notre relation globale :

$$e_{-1}(a) + e_2(a) + e_3(a) + e_5(a) + ... \equiv 0 \pmod 8$$

pour les formes 1-dimensionnelles $[a]$, et par additivité on peut la déduire pour toutes les formes f. La somme est vraiment une forme finie parce que tous ses termes sauf un nombre fini d'entre eux sont nuls.

Le principe fort de Hasse-Minkowski

La relation globale peut être utilisée avec l'existence de formes rationnelles d'invariants imposés pour démontrer un principe important parfois appellé le *principe fort de Hasse-Minkowski.*

Théorème. *Une forme rationnelle f représente un nombre rationnel $r \neq 0$ sur le corps rationnel $\mathbb{Q}$ si et seulement si elle représente r sur tout $\mathbb{Q}_p$ ($p = -1, 2, 3...$).*

Preuve. Le nombre r est représenté par f sur un certain corps juste comme f est équivalente à une forme $[r, *, *, ...]$ sur ce corps, ou, en d'autres termes, juste si f est équivalente à $[r] \oplus g$ sur ce corps, pour un certain g. Car les hypothèses nous donnent des formes $g^{(p)}$ pour lesquelles f est p-adiquement équivalente à $[r] \oplus g^{(p)}$ et la conclusion nécessite une forme g pour laquelle f est rationnellement équivalente à $[r] \oplus g$.

Les invariants p-adiques de la forme souhaitée g doivent donc être les mêmes que ceux des formes données $g^{(p)}$. Existe-t-il un tel g ? Oui ! La seule condition est la relation globale, et cela est vérifié pour g car c'est vérifié pour f et pour $[r]$!.

□

Un théorème sur les formes unimodulaires paires

Pour $p \geq 3$, une forme quadratique entière dont le déterminant est premier à p a une diagonalisation entière p-adique

$$f \cong [a_1, a_2, ..., a_n]$$

dans laquelle tous les a_i sont premiers à p. Donc sa p-signature est n et son p-excès est 0. Pour une forme unimodulaire, la relation globale par conséquent se simplifie en l'assertion que $e_{-1}(f) + e_2(f) \equiv 0 \pmod 8$ ou de manière équivalente en

l'assertion que la signature de f est congruente à son imparité modulo 8. On va maintenant démontrer qu'une forme quadratique unimodulaire *paire* a une imparité nulle, et il en est de même de sa signature mod 8 qui est nulle.

Une telle forme représente nécessairement un nombre $2a$ pour lequel a est impair, et on peut utiliser cela inductivement pour la transformer en une somme directe de formes du type suivant :

$$\begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix} \quad a, b \text{ impairs}$$

sur les entiers 2-adiques. La forme obtenue est équivalente sur les rationnels 2-adiques à

$$[2a, 2a'] \quad a' = ad,$$

où d est le déterminant $4ac - b^2$ de la forme, qui est congruent à -1 mod 4. Ainsi l'un des deux nombres a, a' est égal à 1 ou 5 (mod 8), et l'autre est égal à 3 ou 7 (mod 8). Il en découle que l'imparité de cette forme est

$$(1 \text{ ou } 5 + 4) \quad + \quad (3 + 4 \text{ ou } 7),$$

qui dans chaque cas est un multiple de 8.

L'histoire des réseaux pairs unimodulaires

Le fait remarquable que la dimension d'un réseau unimodulaire pair soit un multiple de 8 est le cas défini positif du résultat ci-dessus. On a vu que ceci est une conséquence de la formule du produit. D'un autre côté, on peut montrer que juste comme dans le cas rationnel, la relation globale (qui est une conséquence presque immédiate de la réciprocité quadratique) est la seule relation entre les structures p-adiques pour chaque p, et donc quand elle est satisfaite, il existe une forme quadratique sur les entiers rationnels avec des invariants p-adiques imposés. En effet, le résultat est quantifié par la formule de la masse, qui en un sens convenable, compte le nombre de formes quadratiques entières avec des invariants imposés.

En 1867, H.J.S. Smith [Smi] a appliqué la formule de la masse pour montrer qu'il existe un réseau pair unimodulaire 8-dimensionnel, et ce réseau E_8 a été explicitement construit par Korkine et Zolotareff en 1873. La formule de la masse peut aussi être utilisée pour montrer que ce réseau est unique. Witt en 1941 a trouvé

deux tels réseaux en 16 dimensions que nous avons mentionnés dans notre second exposé. En 1973, Niemeier a montré qu'il y avait juste 24 réseaux unimodulaires pairs en 24 dimensions, incluant le célèbre réseau de Leech.

Le théorème des trois carrés

Dans la prochaine section, on démontrera le célèbre *théorème des trois carrés* de Legendre de 1798 : un entier positif est la somme de trois nombres carrés entiers si et seulement s'il n'est pas le produit de 4 et d'un nombre congru à -1 modulo 8. Dans cette section, on montre qu'un tel n est la somme de trois carrés rationnels.

Maintenant, une forme représente un nombre sur les rationnels juste si elle le fait sur chaque $\mathbb{Q}_p$. Donc n est la somme de trois carrés rationnels si et seulement s'il peut être représenté comme la somme de trois carrés réels et comme la somme de trois carrés rationnels p-adiques pour tout nombre premier positif $p = 2, ...$ Ceci est très facile à décider puisqu'on a seulement besoin de parler d'un nombre dans chaque classe p-adique de carrés.

On discute des cas :

- $p = -1$: 1 est clairement non représentable, mais $+1 = 1^2 + 0^2 + 0^2$ l'est. Donc la condition pour qu'un nombre n non nul soit la somme de trois carrés réels est juste qu'il soit positif.
- $p = 2$. Les équations

$$\begin{array}{ccc} 1 = 1^2 + 0^2 + 0^2, & 3 = 1^2 + 1^2 + 1^2, & 5 = 2^2 + 1^2 + 0^2 \\ 2 = 1^2 + 1^2 + 0^2, & 6 = 2^2 + 1^2 + 1^2, & 10 = 3^2 + 1^2 + 0^2, \\ & 14 = 3^2 + 2^2 + 1^2 & \end{array}$$

  gèrent toutes les classes de carrés exceptée celle de -1 (ou 7). On montre d'un autre côté que -1 n'est pas la somme de trois carrés de nombres rationnels 2-adiques. Si tel était le cas, alors on pourrait supposer que

$$-d^2 = a^2 + b^2 + c^2$$

  où a^2, b^2 et c^2 couvrent tous les entiers 2-adiques, où au moins l'un d'entre eux, disons a, est impair (puisque sinon on éliminerait un facteur 2). Maintenant, modulo 8, cette congruence se lit

$$-(0 \text{ ou } 1 \text{ ou } 4) \equiv 1 + (0 \text{ ou } 1 \text{ ou } 4) + (0 \text{ ou } 1 \text{ ou } 4),$$

et ceci est impossible.

- $p \geq 3$: comme dans le quatrième exposé, on appelle $u = r + 1$ le plus petit nombre positif qui n'est pas un reste quadratique mod p, et on suppose que $r \equiv x^2 (\text{mod } p)$. Alors les classes de carrés de 1 et u sont représentées par des sommes de deux carrés, notamment :

$$r \equiv x^2 + 0^2, \quad u \equiv x^2 + 1^2.$$

Tout multiple mp de p est alors la somme de trois carrés, puisque $mp - 1$ est dans la même classe de carrés que l'un des r ou u et par conséquent est la somme de deux carrés.

La discussion explique le rôle des deux conditions dans le théorème de Legendre. La condition -1-adique est que n doit être positif ; la condition 2-adique est que ce ne peut être un $4^a(8k-1)$; les autres conditions p-adiques sont toujours satisfaites.

Représentation par trois carrés entiers

On montrera que tout entier n qui est la somme de trois carrés rationnels est également effectivement la somme de trois carrés entiers, en utilisant une méthode ingénieuse de réduction publiée par Aubry en 1912 [Aub].

L'équation

$$n = x_1^2 + x_2^2 + x_3^2$$

nous dit que $n = (\mathbf{x}, \mathbf{x})$ où $\mathbf{x} = (x_1, x_2, x_3)$. Maintenant si les x_i ne sont pas tous entiers, soit m_i le x_i le plus proche d'un entier et soit $x_i = m_i + r_i$. Alors on a $\mathbf{x} = \mathbf{m} + \mathbf{r}$, où $0 < \mathbf{r} \cdot \mathbf{r} < 1$, et les vecteurs $\mathbf{m}$ et $d\mathbf{r}$ ont des coordonnées entières. Cela montre que

$$n = (\mathbf{x}, \mathbf{x}) = (\mathbf{m}, \mathbf{m}) + 2(\mathbf{m}, \mathbf{r}) + (\mathbf{r}, \mathbf{r}),$$

qui implique d'abord que $2(\mathbf{m}, \mathbf{r}m, r) + (\mathbf{r}, \mathbf{r})$ est un entier, N disons, et ensuite que $(\mathbf{r}, \mathbf{r})$ est une fraction propre de dénominateur d, disons d'/d $(0 \leq d' < d)$. Cela montre en retour que le vecteur $\mathbf{r}/(\mathbf{r}, \mathbf{r}) = d\mathbf{r}/d'$ a un dénominateur qui divise d'.

Maintenant réfléchissons $\mathbf{x}$ dans le vecteur $\mathbf{r}$! Cela produit un nouveau vecteur $\mathbf{x}'$ avec $(\mathbf{x}', \mathbf{x}') = (\mathbf{x}, \mathbf{x})$ et ainsi une nouvelle représentation de n comme somme de

trois carrés rationnels. Pourtant, on trouve :

$$\begin{aligned}\mathbf{x}' &= \mathbf{x} - 2(\mathbf{x},\mathbf{r})/(\mathbf{r},\mathbf{x}\mathrm{r})\mathbf{r} \\ &= \mathbf{m} + \mathbf{r} - 2(\mathbf{m},\mathbf{r})/(\mathbf{r},\mathbf{r})\mathbf{r} - 2\mathbf{r} \\ &= \mathbf{m} - N\mathbf{r}/(\mathbf{r},\mathbf{r}),\end{aligned}$$

qui est un vecteur dont le dénominateur divise d'.

Cela montre qu'à partir de n'importe quelle représentation de n comme somme de trois carrés de nombres rationnels de dénominateur commun $d > 1$, on peut dériver une autre telle représentation avec comme dénominateur commun $d' < d$. En continuant de cette manière, on trouve finalement une représentation de n avec $d = 1$ qui est une somme de trois carrés *entiers*.

Conséquences du théorème de Legendre

Peut-être que l'entrée la plus célèbre du journal que Gauss a tenu lorsqu'il était jeune est celle du 10 juillet 1796, jour pour lequel il a écrit

$$\text{EYPHKA !} \qquad num = \Delta + \Delta + \Delta$$

Probablement que Gauss avait démontré l'un des énoncés de Fermat : *tout entier positif est la somme de trois nombres triangulaires.*

Cela découle aisément du théorème de Legendre, qui nous dit qu'un nombre de la forme $8n + 3$ est une somme de trois carrés. Mais puisqu'ils doivent tous être impairs, on a l'équation

$$8n + 3 = (2a + 1)^2 + (2b + 1)^2 + (2c + 1)^2,$$

qui entraîne

$$n = a(a + 1)/2 + b(b + 1)/2 + c(c + 1)/2$$

Le théorème nous permet aussi de décider quels sont les nombres qui sont sommes de quatre carrés *positifs*. On observe d'abord que les nombres des formes $8k + 3$ et $8k + 6$, puisqu'ils sont sommes de trois carrés et non de deux, sont nécessairement sommes de trois carrés positifs. En multipliant par 4, la même chose est vraie des nombres des formes $32k + 12$ et $32k + 24$.

Théorème. *Les entiers positifs qui ne sont pas sommes de quatre carrés positifs sont précisément*

$$1, 3, 5, 9, 11, 17, 29, 41, 2 \times 4^m, 6 \times 4^m, 14 \times 4^m.$$

Preuve. On montre d'abord que n'importe quel nombre plus grand que 49 qui n'est pas un multiple de 8 est la somme de quatre carrés positifs, en soustrayant un carré de façon à obtenir un nombre de l'une des formes décrites ci-dessus. Ainsi à partir d'un :

$8k + 2$ soustraire 2^2 pour obtenir un nombre de la forme $8k + 6$

$8k + 3$ soustraire 4^2 pour obtenir un nombre de la forme $8k + 3$

$8k + 4$ soustraire 12 pour obtenir un nombre de la forme $8k + 3$

$8k + 6$ soustraire 4^2 pour obtenir un nombre de la forme $8k + 6$

$8k + 7$ soustraire 2^2 pour obtenir un nombre de la forme $8k + 3$

$8k+1$ soustraire 1^2 ou 3^2 ou 5^2 ou 7^2 pour obtenir un nombre de la forme $32k+24$

$8k+5$ soustraire 1^2 ou 3^2 ou 5^2 ou 7^2 pour obtenir un nombre de la forme $32k+12$.

Le théorème est complété en vérifiant les nombres jusqu'à 49, et en vérifiant qu'un nombre de la forme $8k$ est la somme de quatre carrés positifs seulement si $2k$ l'est. [Si 1 ou 2 ou 3 des carrés sont impairs, le nombre est de l'une des formes $4k + 1$ ou $4k + 2$ ou $4k + 3$; alors que si tous les quatre sont impairs, il est de la forme $8k+4$. Ils doivent donc tous être pairs.] □

Des méthodes similaires montrent que les différentes formes définies positives en quatre variables sont universelles ; c'est-à-dire qu'elles représentent tous les entiers positifs. Cela est vérifié par exemple par les formes

$$x^2 + y^2 + z^2 + mt^2 \quad \text{pour} \quad m = 1, 2, 3, 4, 5, 6, 7$$

Le théorème des trois carrés montre que si une telle forme manque n'importe quel entier positif, alors le plus petit entier qu'elle rate doit être de la forme $8k+7$. Mais

alors en soustrayant mt^2 pour $t = 1, 1, 2, 1, 1, 1, 2$ dans les sept cas, on obtient des nombres des formes respectives $8k+6, 8k+5, 8k+3, 8k+3, 8k+2, 8k+1, 8k+3$ qui *sont* représentés par $x^2 + y^2 + z^2$.

Le quinzième théorème

William Schneeberger et moi avons récemment utilisé ces idées pour démontrer un théorème remarquable. Si une forme définie positive (en un nombre quelconque de variables) avec matrice entière représente chacun des nombres

$$1,\ \ 2,\ \ 3,\ \ 5,\ \ 6,\ \ 7,\ \ 10,\ \ 14,\ \ 15,$$

alors elle représente tout nombre positif. Pour voir que ceci contient le théorème de Lagrange des quatre carrés, on doit juste vérifier que chacun des entiers ci-dessus est la somme d'au plus quatre carrés :

$$\begin{aligned} &1 = 1^2, \quad 2 = 1^2 + 1^2, \quad 3 = 1^2 + 1^2 + 1^2 \quad 5 = 2^2 + 1^2, \\ &6 = 2^2 + 1^2 + 1^2, \quad 7 = 2^2 + 1^2 + 1^2 + 1^2, \quad 10 = 3^2 + 1^2, \\ &14 = 3^2 + 2^2 + 1^2, \quad 15 = 3^2 + 2^2 + 1^2 + 1^2, \end{aligned}$$

et on a terminé !

Le lecteur intéressé peut utiliser le théorème pour vérifier n'importe quelle autre assertion vraie de ce type ; par exemple, que tout entier positif peut s'écrire comme $a^2 + 2b^2 + 5c^2 + 5d^2 + 15e^2$.

Le quinzième théorème est démontré par des arguments du type ci-dessus, en remplaçant la forme contenant les trois carrés par plusieurs autres formes g, trouvées comme suit. Si f représente les 9 nombres ci-dessus, alors son réseau doit contenir des vecteurs de normes 1, 2, 3, 5,.... Il y a seulement un nombre fini de possibilités pour la forme du sous-réseau couvert par ces vecteurs, et dans presque tous les cas, on peut trouver un sous-réseau 3-dimensionnel dont la forme correspondante g est unique en son genre. On sait alors juste quels nombres sont représentés par g, et on peut utiliser cela pour montrer que tout nombre est représenté par f.

Aucune forme ternaire définie n'est universelle

Pourtant, un argument simple montre que toute forme ternaire définie doit échouer à représenter un nombre infini d'entiers, même dans les rationnels. Car si une forme

ternaire f de déterminant d représente n'importe quoi dans la classe des carrés p-adique de $-d$ sur $\mathbb{Q}_p$, alors elle doit être équivalente p-adiquement à $[-d, a, b]$ où la "forme quotient" $[a, b]$ a pour déterminant -1, et donc p-adiquement, f doit être la forme isotropique $[-d, 1, -1]$.

Mais une forme définie positive ne peut représenter -1, et n'est donc pas p-adiquement isotropique pour $p = -1$. Par la relation globale, il doit exister un autre p pour lequel cela n'est pas p-adiquement isotropique, et donc cela échoue à représenter tous les nombres dans la classe des carrés p-adiques de $-d$ pour ce p aussi !

Le théorème des trois carrés illustre cela joliment - la forme $[1, 1, 1]$ échoue à représenter -1 à la fois -1-adiquement et 2-adiquement. Dans mon troisième exposé, on montrera que la forme

$$x^2 + 2y^2 + yz + 4z^2$$

échoue à représenter 31. On voit maintenant que puisque cela échoue à représenter la classe -1-adique de son déterminant $-31/4$ (i.e., les nombres négatifs), cela doit également échouer à représenter l'infinité des nombres entiers positifs dans la classe $-31/4$ des carrés 31-adiques.