Traductions / transcriptions de divers extraits concernant la fonction $r(n)$ qui compte le nombre de manière d'écrire n comme somme de deux carrés, Denise Vella-Chemla, juin 2026.

Extrait du livre de G. H. Hardy et E. M. Wright, *Introduction à la théorie des nombres*[1], Chapitre XVI : Les fonctions arithmétiques $\phi(n), \mu(n), d(n), \sigma(n), r(n)$, pages 307-310.

16.9 La fonction $r(n)$

Nous définissons la fonction $r(n)$ comme le nombre de représentations de n sous la forme

$$n = A^2 + B^2$$

avec A et B entiers rationnels. Nous comptons toutes les représentations, même celles qui ne diffèrent que "trivialement", i. e. par le signe ou l'ordre de A et B. Ainsi

$$0 = 0^2 + 0^2, \qquad r(0) = 1$$

$$1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2, \qquad r(1) = 4$$

$$5 = (\pm 2)^2 + (\pm 1)^2 = (\pm 1)^2 + (\pm 2)^2 \quad r(5) = 8$$

Nous savons déjà (§ 15.1) que $r(n) = 8$ lorsque n est un nombre premier de la forme $4m + 1$; la représentation est unique à l'exception des huit variantes triviales. D'un autre côté, $r(n) = 0$ lorsque m est de la forme $4m + 3$.

Nous définissons $\chi(n)$ pour $n > 0$, par

$$\chi(n) = 0 \quad (2 \mid n), \qquad \chi(n) = (-1)^{(n-1)/2} \quad (2 \nmid n).$$

Ainsi $\chi(n)$ prend les valeurs $1, 0, -1, 0, 1, \ldots$ pour $n = 1, 2, 3, \ldots$. Puisque

$$\frac{1}{2}(nn' - 1) - \frac{1}{2}(n - 1) - \frac{1}{2}(n' - 1) = \frac{1}{2}(n - 1)(n' - 1) \equiv 0 \pmod 2$$

lorsque n et n' sont impairs, $\chi(n)$ vérifie

$$\chi(nn') = \chi(n)\chi(n'),$$

pour tout n et n'. En particulier $\chi(n)$ est multiplicative au sens du § 5.5.

Il est clair qu'en posant

$$\delta(n) = \sum_{d \mid n} \chi(d), \tag{16.9.1}$$

1. Traduction de François Sauvageot, Préface de Catherine Goldstein, éds. Vuibert-Springer.

nous avons

$$\delta(n) = d_1(n) - d_3(n), \tag{16.9.2}$$

où $d_1(n)$ et $d_3(n)$ sont respectivement les nombres de diviseurs de n de la forme $4m+1$ et $4m+3$.

Supposons maintenant que

$$n = 2^\alpha N = 2^\alpha \mu\nu = 2^\alpha \prod p^r \prod q^s, \tag{16.9.3}$$

où p et q sont des nombres premiers de la forme $4m+1$ et $4m+3$ respectivement.

S'il n'y a pas de facteur q, de sorte que $\prod q^s$ est "vide", nous posons $\nu = 1$. Il est manifeste que

$$\delta(n) = \delta(N).$$

Les diviseurs de N sont les termes du produit

$$\prod(1 + p + \ldots + p^r) \prod(1 + q + \ldots + q^s). \tag{16.9.4}$$

Un diviseur est de la forme $4m+1$ s'il contient un nombre pair de facteurs q, et $4m+3$ dans le cas contraire. Par conséquent, $\delta(N)$ est obtenu en remplaçant p par 1 et q par -1 dans (16.9.4) ; et donc

$$\delta(N) = \prod(r+1) \prod \left(\frac{1 + (-1)^s}{2} \right) \tag{16.9.5}$$

Si un des s est impair, i. e. si ν n'est pas un carré, alors

$$\delta(n) = \delta(N) = 0$$

tandis que

$$\delta(n) = \delta(N) = \prod(r+1) = d(\mu)$$

si ν est un carré.

Nous allons démontrer le

Théorème 278 Si $n \geq 1$ alors

$$r(n) = 4\delta(n)$$

Il nous faut donc démontrer que $r(n)$ vaut $4\,d(\mu)$ lorsque ν est un carré et 0 sinon.

16.10 Démonstration de la formule pour $r(n)$

Nous pouvons écrire (16.9.3) sous la forme

$$n = ((1+i)(1-i))^\alpha \prod((a+bi)(a-bi))^r \prod q^s.$$

avec a et b strictement positifs et distincts, et

$$p = a^2 + b^2$$

L'expression de p est unique (d'après le § 15.1), à l'exception de l'ordre de a et b. Les facteurs

$$1 \pm i, \quad a \pm bi, \quad q$$

sont premiers dans $\mathbf{Q}[i]$.

Si

$$n = A^2 + B^2 = (A + Bi)(A - Bi),$$

alors

$$A + Bi \;\; = i^t(1+i)^{\alpha_1}(1-i)^{\alpha_2} \prod((a+bi)^{r_1}(a-bi)^{r_2}) \prod q^{s_1},$$

$$A - Bi \;\; = i^{-t}(1-i)^{\alpha_1}(1+i)^{\alpha_2} \prod((a-bi)^{r_1}(a+bi)^{r_2}) \prod q^{s_2},$$

avec

$$t = 0, 1, 2 \text{ ou } 3, \alpha_1 + \alpha_2 = \alpha, \quad r_1 + r_2 = r, \quad s_1 + s_2 = s$$

Il est clair que $s_1 = s_2$ de sorte que tous les s sont pairs, et ν est un carré. Si tel n'est pas le cas, n n'admet pas de représentation en somme de deux carrés.

Nous supposons donc que

$$\nu = \prod q^s = \prod q^{2s_1}$$

est un carré. Il n'y a pas de choix à faire pour la répartition des facteurs q entre $A + Bi$ et $A - Bi$. Il y a

$$4(\alpha + 1) \prod (r + 1)$$

choix pour la répartition des autres facteurs. Mais

$$\frac{1-i}{1+i} = -i$$

est une unité, de sorte qu'un changement sur α_1 et α_2 ne donne pas d'autres changements sur A et B que ceux produits par les changements de t. Il nous reste donc au plus

$$4 \prod (r + 1) = 4\delta(n)$$

choix effectifs, i. e. des choix qui produisent des changements sur A et B.

Les variantes triviales d'une représentation $n = A^2 + B^2$ correspondent (i) à la multiplication de $A + Bi$ par une unité, (ii) à l'échange de $A + Bi$ avec son conjugué. Ainsi, ces variantes sont données par

$$1(A + Bi) \;\; = A + Bi \qquad i(A + Bi) \;\; = -B + Ai$$

$$i^2(A + Bi) \;\; = -A - Bi \quad i^3(A + Bi) \;\; = B - Ai$$

et par $A-Bi, -B-Ai, -A+Bi$ et $B+Ai$ qui sont les conjugués de ces quatre nombres précédents. Tout changement de la valeur de t modifie la représentation. Tout changement de r_1 et r_2 la modifie aussi, et ce d'une façon qui n'est pas obtenue par un changement de t ; en effet

$$i^t(1+i)^{\alpha_1}(1-i)^{\alpha_2}\prod((a+bi)^{r_1}(a-bi)^{r_2}) = i^{t'}(1+i)^{\alpha'_1}(1-i)^{\alpha'_2}\prod((a+bi)^{r'_1}(a-bi)^{r'_2})$$

est impossible, d'après le théorème 215, sauf si $r_1 = r'_1$ et $r_2 = r'_2$ [2]. Par conséquent, il existe 4 * d(mu) ensembles de valeurs pour A et $4d(\mu)$ représentations de n et ceci démontre le théorème 278. [3].

Notes § 16.9. Le théorème 278 a été démontré en premier lieu par Jacobi au moyen de la théorie des fonctions elliptiques. Il est néanmoins équivalent à un théorème énoncé par Gauss [[4], § 182] ; et il y a eu de nombreux énoncés ou démonstrations incomplets avant cela. Voir [Dickson [5] ch. vi] et [Bachmann [6] volume 2, chapitre vii].

2. Un changement de r_1 en r_2 et de r_2 en r_1 (avec des changements similaires pour t, α_1, α_2) modifie $A+Bi$ en son conjugué ;

3. NdT. En fait l'écriture

$$A+Bi = i^t(1+i)^{\alpha_1}(1-i)^{\alpha_2}\prod((a+bi)^{r_1}(a-bi)^{r_2})\prod q^{s_1}$$

peut se reformuler en

$$A+Bi = i^{t-\alpha_2}(1+i)^{\alpha}\prod((a+bi)^{r_1}(a-bi)^{r-r_1})\prod q^{s/2}$$

ou encore en

$$A+Bi = i^{u}(1+i)^{\alpha}\prod((a+bi)^{r_1}(a-bi)^{r-r_1})\prod q^{s/2},$$

avec $u = 0, 1, 2,$ ou $3,\ 0 \le r_1 \le r$. Cette écriture est unique car les nombres premiers qui apparaissent ne sont pas associés deux à deux. Il y a donc exactement $4\prod(r+1)$ nombres $A+Bi$ différents.

4. C. F. Gauss, *Disquisitiones arithmeticae, Fleischer, Leipzig, 1801, réimprimé dans . Dsiponible à l'adresse https://gallica.bnf.fr/ark:/12148/bpt6k994003*

5. L. E. Dickson, *Diophantine analysis*, volume II de *History of the theory of numbers*, Carnegie Institution 1920. Réimprimé par Chelsea, New York, 1966.

6. P. Bachmann, *Niedere Zahlentheorie*, Teubner, Leipzig, 1902-1910. I - *Niedere Zahlentheorie* ; II - *Additive Zahlentheorie*. Réédité en 1968 par Chelsea Publishing Company, Bronx.

Extrait du livre de Kenneth Ireland et Michael Rosen, [7], chapitre 17, *Équations diophantiennes*, § 6, *Sommes de deux carrés*, page 278-280.

Si p est premier, $p \equiv 1\ (4)$ alors, d'après la proposition 8.3.1, l'équation diophantienne $x^2 + y^2 = p$ admet une solution entière essentiellement unique. Il existe de nombreuses démonstrations de ce résultat. On se souviendra que la démonstration du chapitre 8 utilisait l'anneau des entiers de Gauss. En exploitant davantage l'arithmétique de cet anneau, nous déterminerons le nombre de représentations d'un entier positif arbitraire comme somme de deux carrés. Le résultat est énoncé de manière commode et, en fait, démontré à l'aide du caractère de Dirichlet non trivial modulo 4 introduit dans la paragraphe 2 du chapitre 16. Rappelons que ce caractère χ est défini sur $\mathbb{Z}$ par $\chi(d) = 1$ si $d \equiv 1\ (4)$, $\chi(d) = -1$ si $d \equiv 3\ (4)$ et $\chi(2k) = 0$.

Proposition 17.6.1. *Le nombre de solutions entières $(x, y), x > 0, y \geq 0$ de l'équation $x^2 + y^2 = n$ est $\sum_{d|n} \chi(d)$.*

En d'autres termes, le nombre de représentations de n comme somme de deux carrés non négatifs dont le premier est positif est l'excès du nombre de diviseurs de la forme $4n+1$ sur le nombre de diviseurs de la forme $4n+3$. On voit alors facilement que le nombre total de solutions $(x, y), x, y \in \mathbb{Z}$, est égal à $4\sum_{d|n} \chi(d)$. Avant de procéder à la démonstration, nous en déduisons deux corollaires.

Corollaire 1. *L'équation $x^2+y^2 = n, n > 0$ admet une solution entière si et seulement si $\mathrm{ord}_p\ n$ est pair pour tout nombre premier $p \equiv 3\ (4)$. Dans ce cas, le nombre de solutions est $\prod_{p \equiv 1\ (4)} (1+\mathrm{ord}_p\ n)$.*

Preuve. Puisque $\chi(n)$ est multiplicatif, il découle de l'exercice 10 du chapitre 2 que $\sum_{d|n} \chi(d)$ est multiplicative. Si $p \equiv 1\ (4)$, alors $\sum_{d|p^n} \chi(d) = n + 1$, tandis que si $p \equiv 3\ (4)$, alors $\sum_{d|p^n} \chi(d)$ vaut 0 ou 1 selon que n est impair ou pair. Le résultat s'ensuit. □

Corollaire 2. *Soit m un entier impair positif. Le nombre de solutions entières $(x, y), x > 0, y > 0$, de $x^2 + y^2 = 2m$ est $\sum_{d|m} \chi(d)$.*

Preuve. Puisque $2m \equiv 2\ (4)$, y est positif. D'autre part, $\chi(2d) = 0$ pour tout diviseur $2d$ de $2m$. □

Nous passons maintenant à la démonstration de la proposition. Considérons l'anneau $\mathbb{Z}[i]$ des entiers de Gauss. D'après l'exercice 33 du chapitre 1, les unités sont $\pm 1, \pm i$. Ainsi, chaque $\alpha \in \mathbb{Z}[i]$ non nul a un unique associé $x + iy, x > 0, y \geq 0$. Si $N(x + iy) = x^2 + y^2$ est l'application norme, alors clairement le nombre de solutions de $x^2 + y^2 = n, x > 0, y \geq 0$ est le nombre d'idéaux (α) avec $N(\alpha) = n$. Notons ce nombre par a_n. Rappelons de plus que tout idéal $(\alpha) \neq 0$ peut s'écrire de manière unique (à l'ordre près) sous la forme $(\pi_1)^{t_1} \ldots (\pi_s)^{t_s}$ où π_i est irréductible. Enfin, selon la section 7 du chapitre 9, les irréductibles sont donnés, à une unité près, par $1 + i, \pi$ avec $\pi\overline{\pi} = p \equiv 1\ (4)$, et q, un nombre premier rationnel, $q \equiv 3\ (4)$. De plus, π et $\overline{\pi}$ ne sont pas associés.

7. A classical introduction to modern number theory, second edition, Springer, 1990, éditions précédentes en 1972 et 1982.

Nous introduisons maintenant la série de Dirichlet formelle $\sum_{n=1}^{\infty} a_n/n^s$. Cette série est connue sous le nom de fonction zêta de l'anneau $\mathbb{Z}[i]$. Nous considérons cette expression formellement et n'aurons besoin d'aucune propriété analytique de la fonction associée d'une variable complexe. En utilisant la factorisation unique des idéaux dans $\mathbb{Z}[i]$ prouvée dans la section 4 du chapitre 1, on voit, en utilisant le même argument que dans l'exercice 25 du chapitre 2, que

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{(\pi)} \left(\frac{1}{1 - 1/N(\pi)^s} \right), \tag{34}$$

le produit étant sur l'ensemble des irréductibles (non associés) dans $\mathbb{Z}[i]$. Le membre à droite du signe égal dans (34) devient, par la classification ci-dessus des irréductibles

$$\left(\frac{1}{1 - 1/2^s} \right) \prod_{p \equiv 1 \ (4)} \left(\frac{1}{1 - 1/p^s} \right)^2 \prod_{q \equiv 3 \ (4)} \left(\frac{1}{1 - 1/q^{2s}} \right). \tag{35}$$

Rappelons ensuite que

$$\zeta(s) = \prod_{p} \frac{1}{1 - 1/p^s} = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

En remarquant que $1/(1 - q^{-2s}) = (1/(1 - q^{-s}))(1/(1 + q^{-s}))$, nous voyons par réarrangement des termes que (35) devient

$$\zeta(s) \prod_{p \equiv 1 \ (4)} \frac{1}{1 - 1/p^s} \prod_{q \equiv 3 \ (4)} \frac{1}{1 + 1/q^s}. \tag{36}$$

Ceci peut s'écrire comme

$$\zeta(s) \prod_{p} \frac{1}{1 - \chi(p)/p^s} \tag{37}$$

Enfin, en utilisant le fait que χ est multiplicatif, nous voyons que (37) peut s'écrire comme

$$\zeta(s) \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{38}$$

Rappelons que le deuxième facteur de (38) est la L-série de Dirichlet introduite au chapitre 16, section 2, afin de calculer la densité des nombres premiers $p \equiv 1 \ (4)$. Nous avons montré que

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \left(\sum_{n=1}^{\infty} \frac{1}{n^s} \right) \left(\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \right). \tag{39}$$

La proposition 17.6.1 découle immédiatement de (39) car le coefficient du membre de droite de (39) est, par définition même de la multiplication de Dirichlet, égal à $\sum_{d|n} \chi(d)$.

Ceci achève la démonstration. □

Il convient de noter que l'étape de réarrangement dans la démonstration ci-dessus est purement formelle et ne nécessite aucune propriété analytique des produits infinis.

Article de Jacobi : traduction depuis le latin de l'article du Journal de Crelle d. M. Bd. XII. Hft. 2

12.

Sur la composition des nombres à partir de quatre carrés.

(par le Dr C. G. J. Jacobi, Prof. de Mathématiques.)

Dans ce journal, tome III, page 191, j'ai proposé le théorème suivant sans démonstration :

"Soit n un nombre impair positif donné, et soient w, x, y, z des nombres impairs positifs, le nombre de solutions de l'équation

$$4n = ww + xx + yy + zz,$$

est égal à la somme des facteurs de n."

Ce théorème apparaît clairement à première vue, en comparant les formules que j'ai démontrées dans *Fund. Novis Theor. F. E.*, page 106 (35) et page 184 (7). Cependant, pour les arithméticiens qui ne défendent pas les développements analytiques proposés dans l'ouvrage cité, je le démontrerai ici, en partant uniquement des théorèmes relatifs à la composition des nombres en sommes de deux carrés. Cette démonstration se déduit aisément de l'analyse utilisée en 1. c. page 109. Je la dissimule d'autant moins qu'elle pourrait servir de point de départ à d'autres pour approfondir la méthode que j'emploie par la suite.

Dans ce qui suit, j'utilise le théorème auxiliaire bien connu, ou un théorème qui se déduit facilement des théorèmes connus, comme suit :

"Si tous les nombres premiers qui mesurent un nombre impair donné n sont de la forme $4m+1$, le nombre de solutions de l'équation

$$2n = yy + zz,$$

est égal au nombre de facteurs de n."

Le nombre de solutions de l'équation

$$2nQQ = yy + zz$$

sera le même si les nombres premiers qui mesurent le nombre impair Q ont tous la forme $4m+3$. Car il n'y a pas d'autres solutions à cette équation que celles qui résultent des solutions de l'équation précédente, multipliées par les deux nombres y, z.

Étant donné un nombre impair p quelconque, cherchons le nombre de ses facteurs de la forme $4m+1$ et le nombre de ses facteurs de la forme $4m+3$. À cette fin, comme dans la suite, les éléments, en grec, sans préfixe, dénotent des nombres de la forme $4m+1$; avec préfixe, ils dénotent ceux de la forme $4m+3$. Les lettres latines minuscules dénotent les nombres impairs, sous les deux formes ; les lettres latines majuscules dénotent des nombres pairs et impairs. De plus, on considère tous les nombres comme positifs. Tenons compte de ces remarques dans la suite.

Soit le nombre p décomposé en facteurs premiers

$$p = \alpha^A \beta^B \gamma^C \ldots \times \alpha'^{A'} \beta'^{B'} \gamma'^{C'} \ldots ;$$

on sait que tous les facteurs de p s'obtiennent en développant le produit

$$\begin{array}{l} 1 + \alpha + \alpha^2 + \ldots + \alpha^A \\ 1 + \beta + \beta^2 + \ldots + \beta^B \\ 1 + \gamma + \gamma^2 + \ldots + \gamma^C \\ \ldots \\ 1 + \alpha' + \alpha'^2 + \ldots + \alpha'^{A'} \\ 1 + \beta' + \beta'^2 + \ldots + \beta'^{B'} \\ 1 + \gamma' + \gamma'^2 + \ldots + \gamma'^{C'} \end{array}$$

Établissons dans ce produit

$$\begin{array}{l} \alpha = \beta = \gamma = \ldots = 1, \\ \alpha' = \beta' = \gamma' = \ldots = -1; \end{array}$$

Lors du développement du produit, les termes individuels deviennent soit $+1$ s'ils sont de la forme $4m + 1$, soit -1 s'ils sont de la forme $4m + 3$. La valeur du produit est alors égale à l'excédent du nombre de facteurs de p de la forme $4m + 1$ sur le nombre de facteurs de p de la forme $4m + 3$. On trouve ainsi la valeur du produit :

$$(1 + A)(1 + B)(1 + C) \ldots \left(\frac{1 + (-1)^{A'}}{2}\right) \left(\frac{1 + (-1)^{B'}}{2}\right) \left(\frac{1 + (-1)^{C'}}{2}\right) \ldots,$$

qui s'annule dans tous les cas où les nombres A', B' et C' ne sont pas tous égaux simultanément. Mais dans ce cas, cela devient

$$(1 + A)(1 + B)(1 + C)...,$$

soit le même nombre que le nombre de facteurs

$$\alpha^A \beta^B \gamma^C \ldots .$$

L'excédent est donc égal à 0, sauf si p est de la forme

$$p = nQQ,$$

où n est un nombre impair, non divisible par d'autres nombres, sauf ceux de la forme $4m + 1$, et Q un nombre impair, non divisible par d'autres nombres premiers, sauf ceux de la forme $4m + 3$; mais dans ce cas, cet excédent sera égal au nombre de facteurs de n. Par conséquent, puisqu'il est également clair que le nombre $2p$ n'est divisible par aucun autre carré impair, sauf sous la forme p a une affectation, mais pour cette forme, à partir du théorème auxiliaire, le nombre de solutions de l'équation

$$2p = yy + zz$$

Si n est égal au nombre de facteurs de n, le théorème peut être énoncé de la manière suivante :

"*Pour tout nombre impair p, le nombre de solutions de l'équation*

$$2p = yy + zz$$

est identique à l'excès du nombre de facteurs de p de la forme $4m+1$ *par rapport au nombre de facteurs de p de la forme* $4m+3$."

Ce théorème est évident si l'on compare les formules des Fondements à la page 103 (5.) et 184 (7.). Nous avons brièvement exposé les raisonnements précédents au chapitre 1, page 107.

Dans ce qui suit, pour désigner le nombre de solutions de l'équation proposée, nous encadrerons l'équation elle-même entre crochets et la préfixerons de la lettre N. Ainsi, nous désignerons, par exemple, le nombre de solutions de l'équation

$$2p = yy + zz$$

par le signe

$$N[2p = yy + zz].$$

Par conséquent, le nombre de facteurs de p, qui ont la forme $4m+1$, sera, par la méthode de signification que nous avons proposée ci-dessus,

$$N[p = a\alpha];$$

Le nombre de facteurs de p qui ont la forme $4m+3$ sera

$$N[p = a\alpha'].$$

Par conséquent, le théorème proposé peut être présenté par la formule suivante :

1. $$[2p = xx + yy] = N[p = a\alpha] - N[p = a\alpha'].$$

Passons maintenant à la division du nombre $4p$ en quatre carrés impairs.

2.

Décomposons le nombre donné $2p$ de toutes les manières possibles en deux nombres impairs p' et p'', de sorte qu'il soit égal à

2. $$2p = p' + p''.$$

Ensuite, nous résolvons chacun des $2p'$ et $2p''$ de toutes les manières possibles, en deux carrés, qui seront impairs, de sorte que :

3. $$2p' = ww + xx, \quad 2p'' = yy + zz$$

et donc

4. $$4p = ww + xx + yy + zz.$$

Pour les mêmes nombres p' et p'' en lesquels $2p$ se décompose, le nombre de solutions de cette équation (**4.**) est égal au produit du nombre de solutions des deux équations (**3.**) ; par conséquent, le nombre total de solutions de l'équation (**4.**) est équivalent à la somme

$$\sum(N[2p' = ww + xx]N[2p'' = yy + zz]),$$

étendue à toutes les valeurs impaires des nombres p', p'' qui satisfont l'équation (**2.**). Or, d'après (**1.**), nous avons :

$$N[2p' = ww + xx] = N[p' = a\alpha] - N[p' = a\alpha']$$

$$N[2p'' = yy + zz] = N[p'' = b\beta] - N[p'' = b\beta'].$$

En les prenant en eux-mêmes, nous obtenons le produit, composé de quatre termes,

$$\begin{array}{rcrcrcr} N[p' = a\alpha] & . & N[p'' = b\beta] & + & N[p' = a\alpha'] & . & N[p'' = b\beta'] \\ -N[p' = a\alpha] & . & N[p'' = b\beta'] & - & N[p'' = b\beta] & . & N[p' = a\alpha']. \end{array}$$

Mais si nous étendons la somme à toutes les valeurs de p', p'' qui satisfont l'équation (**3.**), nous avons :

$$\begin{array}{l} \sum(N[p' = a\alpha]N[p'' = b\beta]) = N[2p = a\alpha + b\beta] \\ \sum(N[p' = a\alpha']N[p'' = b\beta']) = N[2p = a\alpha' + b\beta'] \\ \sum(N[p' = a\alpha]N[p'' = b\beta']) = N[2p = a\alpha + b\beta'] \\ \sum(N[p'' = b\beta]N[p' = a\alpha']) = N[2p = b\beta + a\alpha']. \end{array}$$

Il s'ensuit donc que

5. $N[4p = ww + xx + yy + zz] = N[2p = a\alpha + b\beta] + N[2p = a\alpha' + b\beta'] - N[2p = a\alpha + b\beta'] - N[2p = b\beta + a\alpha']$.

Dans la suite, par souci de concision, au lieu

$$N[2p = u]$$

nous écrirons simplement

$$N[u] = N[2p = u].$$

De plus, nous fixerons le nombre de solutions de l'équation proposée (**4.**) à

$$N[4p = ww + xx + yy + zz] = N.$$

Avec ces dispositions, l'équation (**5.**) peut être présentée comme suit :

6. $$N = N[a\alpha + b\beta] + [a\alpha' + b\beta'] - N[a\alpha + b\beta'] - N[b\beta + a\alpha'].$$

Je remarque que dans cette expression, les deux termes négatifs sont égaux, puisque l'un provient de l'autre, les éléments a, b et α, β étant intervertis. D'où, plus simplement :

7. $$N = N[a\alpha + b\beta] + N[a\alpha' + b\beta'] - 2N[a\alpha + b\beta'].$$

Considérons séparément les cas dans lesquels

$$\alpha = \beta\ ; \qquad \alpha' = \beta'\ ;$$

pour le reste, il est permis d'établir $\beta > \alpha, \beta' > \alpha'$, si leur nombre est doublé. Par conséquent, si nous posons

$$\beta = \alpha + 4A, \qquad \beta' = \alpha' + 4A,$$

nous pouvons représenter l'équation (**7.**) comme suit :

8. $$N = N[\alpha(a+b)] + N[\alpha'(a+b)] - 2N[a\alpha + b\beta'] + 2N[(a+b)\alpha + 4bA] + 2N[(a+b)\alpha' + 4bA].$$

Or, puisque les cas où le nombre est de la forme $4m+1$ et ceux où il est de la forme $4m+3$ englobent tous les cas où le nombre est impair, il est possible de réduire les deux termes de l'expression précédente à un seul, de sorte que nous avons :

8. $$N = N[(a+b)c] + 2N[(a+b)c + 4bA] - 2N[a\alpha + b\beta'].$$

Posons dans le second terme

$$c = d + 4AB,$$

où $d < 4A$ et $B = 0$ ou un nombre positif quelconque ; alors

9. $$N = N[(a+b)c] + 2N[(a+b)d + 4A(b + B(a+b))] - 2N[a\alpha + b\beta'].$$

Or, les nombres

$$a+b \quad \text{et} \quad b + B(a+b)$$

peuvent désigner ensemble, l'un un nombre pair et l'autre un nombre impair quelconque, et ce d'une seule manière, ou, étant donnés, a, b et B seront également déterminés ; d'où il est possible d'établir

$$a + b = 2C, \qquad b + B(a+b) = e.$$

En substituant dans le deuxième terme, on obtient

10. $$N = N[(a+b)c] + 2N[2Cd + 4Ae] - 2N[a\alpha + b\beta'],$$

où $d < 4A$.

Quant au troisième terme, on a

$$2N[a\alpha + b\beta'] = N[a\alpha + b\beta'] + N[a\beta' + b\alpha].$$

Dans l'expression de droite, on peut à nouveau établir $b > a$, puisque les valeurs sont doublées simultanément ; le cas $a = b$ ne peut pas se produire, car les expressions entre parenthèses seraient alors divisibles par 4, or le nombre $2p$, auquel elles sont égales, est pairement impair. Par conséquent, si nous établissons dans l'expression de droite :

$$b = a + 2C,$$

nous pouvons présenter l'équation précédente de la manière suivante :

11. $$N[a\alpha + b\beta'] = N[a(\alpha + \beta') + 2\beta' C] + N[a(\alpha + \beta') + 2\alpha C]$$

ou, si nous la mettons de la manière suivante :

12. $$\alpha + \beta' = 4A$$

il découle

13. $$N[a\alpha + b\beta'] = N[2\alpha C + 4Aa] + N[2\beta' C + 4Aa],$$

où, d'après (12.), α et β' doivent tous deux être $< 4A$. On peut réduire les deux termes de droite, pour la même raison que précédemment, à un seul.

14. $$N[a\beta + b\beta'] = N[2Cd + 4Aa],$$

où $d < 4A$. En substituant cette équation dans (**10.**), les deuxième et troisième termes s'annulent ; d'où l'on obtient simplement :

15. $$N = N[(a + b)c] = N[2p = (a + b)c].$$

Dans cette formule, c peut être n'importe quel facteur de p, mais il ne peut pas prendre d'autres valeurs ; par conséquent, en supposant $p = cf$ un facteur commun, l'équation

16. $$2p = (a + b)c$$

Toutes les solutions sont obtenues si, pour chaque facteur c de p, l'équation

$$2f = a + b$$

est résolue de toutes les manières possibles. Cela donne le nombre f. Par conséquent, pour chaque valeur de c, il existe un nombre f de solutions de l'équation (**16**), d'où le nombre total de solutions de l'équation (**16**) égal à la somme des facteurs de p. Ainsi, d'après (**15**), le nombre recherché

$$N = N[4p = ww + xx + yy + zz]$$

est égal à la somme des facteurs de p. *Ce qui devait être démontré.*

Je ne publierai qu'un exemple de cette nouvelle et simple méthode singulière ; je n'aborderai pas ici le grand nombre de théorèmes d'objectif similaire qui découlent des développements présentés dans les *Fondements*.

Écrit le 14 février 1834.

Traduction d'un court texte fournissant une autre preuve du théorème de Jacobi de Michael Hirschhorn [8]

Une preuve simple du théorème des deux carrés de Jacobi

1. Dans une note récente, John A. Ewell [1] dérive le théorème des deux carrés de Fermat :

Un nombre premier $p = 4n + 1$ est la somme de deux carrés.

à partir de l'identité du triple produit.

J'ai observé que de l'identité du triple produit, on peut obtenir le résultat plus fort dû à Jacobi, à savoir :

THÉORÈME 1. *Le nombre $r_2(n)$ de représentations de l'entier positif n comme somme de deux carrés est donné par*

$$r_2(n) = 4(d_1(n) - d_3(n)),$$

où

$$d_i(n) = \sum_{d\,|\,n,\ d\equiv i \pmod 4} 1.$$

2. L'identité du triple produit est

$$\prod_{n\geq 1}(1 + ax^{2n-1})(1 + a^{-1}x^{2n-1})(1 - x^{2n}) = \sum_{-\infty}^{\infty} a^n x^{n^2}, \tag{1}$$

et elle est valable pour toute paire de nombres complexes a, x avec $a \neq 0$ et $|x| < 1$.

Posons $-a^2x$ pour a, puis x pour x^2, multiplions par a et nous obtenons l'identité, invariante par $a \to -a^{-1}$,

$$\begin{aligned}
&(a - a^{-1}) \prod_{n\geq 1}(1 - a^2x^n)(1 - a^{-2}x^n)(1 - x^n) \\
&\quad = \sum_{-\infty}^{\infty}(-1)^n a^{2n+1} x^{(n^2+n)/2} \\
&\quad = \sum_{-\infty}^{\infty} a^{4n+1} x^{2n^2+n} - \sum_{-\infty}^{\infty} a^{4n-1} x^{2n^2-n} \\
&\quad = a \prod_{n\geq 1}(1 + a^4x^{4n-1})(1 + a^{-4}x^{4n-3})(1 - x^{4n}) - a^{-1} \prod_{n\geq 1}(1 + a^4x^{4n-3})(1 + a^{-4}x^{4n-1})(1 - x^{4n}).
\end{aligned} \tag{2}$$

En dérivant (2) par rapport à a, en posant $a = 1$, et en divisant par 2, on trouve

8. Trouvée à cette adresse.

(3) $$\prod_{n\geq 1}(1-x^n)^3 = \prod_{n\geq 1}(1+x^{4n-3})(1+x^{4n-1})(1-x^{4n})\times\left\{1-4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right)\right\}$$

[La dérivée du produit infini à gauche de (2) est sans importance, puisqu'elle s'annule lorsqu'on substitue $a=1$, tandis que les dérivées des produits infinis à droite de (2) sont trouvées à partir de

$$\left(\prod_{n\geq 1}u_n\right)' = \left(\prod_{n\geq 1}u_n\right)\sum_{n\geq 1}\frac{u_n'}{u_n}.$$

Diviser (3) par

$$\begin{aligned}\prod_{n\geq 1}(1+x^n)^2(1-x^n) &= \prod_{x\geq 1}(1+x^n)(1-x^{2n})\\ &= \prod_{n\geq 1}(1+x^{2n-1})(1+x^{2n})(1-x^{2n})\\ &= \prod_{n\geq 1}(1+x^{2n-1})(1-x^{4n})\\ &= \prod_{n\geq 1}(1+x^{4n-3})(1+x^{4n-1})(1-x^{4n}),\end{aligned}$$

et nous avons

(4) $$\prod_{n\geq 1}\left(\frac{1-x^n}{1+x^n}\right)^2 = 1-4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right).$$

Maintenant,

$$\begin{aligned}\prod_{n\geq 1}\left(\frac{1-x^n}{1+x^n}\right) &= \prod_{n\geq 1}\frac{(1-x^{2n-1})(1-x^{2n})}{(1+x^n)}\\ &= \prod_{n\geq 1}(1-x^{2n-1})(1-x^n)\\ &= \prod_{n\geq 1}(1-x^{2n-1})(1-x^{2n-1})(1-x^{2n})\\ &= \sum_{-\infty}^{\infty}(-1)^n x^{n^2},\end{aligned}$$

donc (4) se transforme en

(5) $$\left(\sum_{-\infty}^{\infty}(-1)^n x^{n^2}\right)^2 = 1-4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right).$$

Remplaçons x par $-x$, et nous obtenons

(6) $$\left(\sum_{-\infty}^{\infty}x^{n^2}\right)^2 = 1+4\sum_{n\geq 1}\left(\frac{x^{4n-3}}{1+x^{4n-3}}-\frac{x^{4n-1}}{1+x^{4n-1}}\right)$$

d'où le fait que le théorème 1 découle directement de [2].

Références

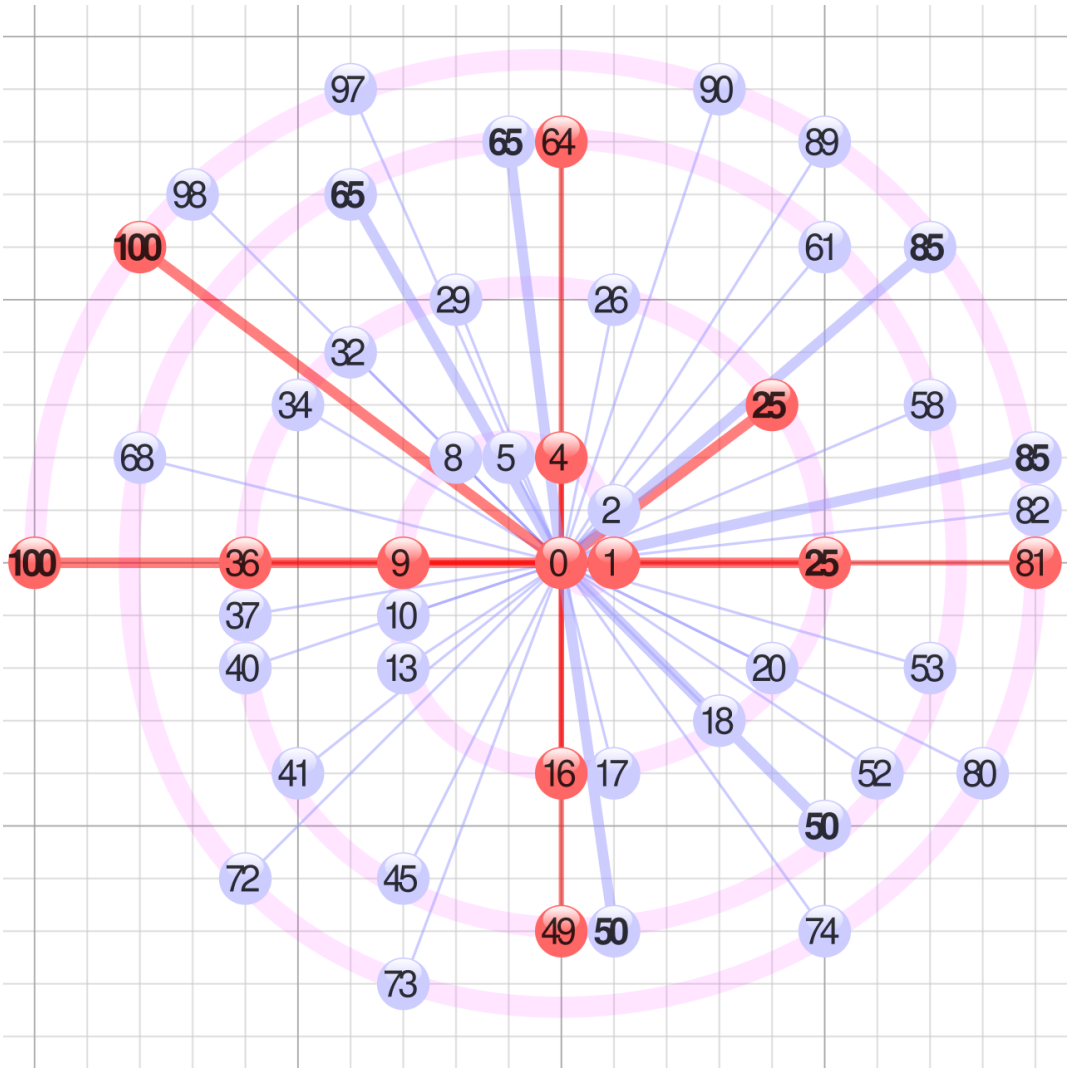
1. John A. Ewell, Une preuve simple du théorème des deux carrés de Fermat, ce MONTHLY, 90 (1983) 635-637.

2. G. H. Hardy et E. M. Wright, Introduction à la théorie des nombres, 4e éd., Clarendon Press, Oxford, 1960, p. 258.

Article Wikipedia : Théorème de la somme de deux carrés [9]

En théorie des nombres, le théorème de la somme de deux carrés relie la décomposition en nombres premiers de tout entier $n > 1$ à la possibilité de l'écrire comme une somme de deux carrés, tel que $n = a^2 + b^2$ pour certains entiers a et b [1].

Un entier supérieur à un peut être écrit comme une somme de deux carrés si et seulement si sa décomposition en nombres premiers ne contient aucun facteur p^k, où p premier $\equiv 3 \pmod 4$ et k est impair.



Lorsqu'on écrit un nombre comme une somme de deux carrés, il est permis que l'un des carrés soit nul, ou que les deux soient égaux, de sorte que tous les carrés et tous les doubles de carrés sont inclus dans les nombres qui peuvent être représentés de cette manière. Ce théorème complète le théorème de Fermat sur les sommes de deux carrés, qui indique quand un nombre premier peut être

9. Téléchargeable à cette adresse.

écrit comme une somme de deux carrés, en ce qu'il couvre également le cas des nombres composés.

Les entiers satisfaisant le théorème de la somme de deux carrés sont les carrés des distances possibles entre les points entiers du réseau ; les valeurs jusqu'à 100 sont affichées, avec

Les carrés (et donc les distances entières) en rouge, et

Les représentations non uniques (à rotation et réflexion près) en gras

Un nombre peut avoir plusieurs représentations comme somme de deux carrés, comptées par la fonction somme des carrés ; par exemple, tout triplet pythagoricien $a^2 + b^2 = c^2$ donne une deuxième représentation pour c^2 en plus de la représentation triviale $c^2 + 0^2$.

Exemples

La décomposition en nombres premiers du nombre 2450 est donnée par $2450 = 2 \cdot 5^2 \cdot 7^2$. Parmi les nombres premiers présents dans cette décomposition, 2, 5 et 7, seul 7 est congru à 3 modulo 4. Son exposant dans la décomposition, 2, est pair. Par conséquent, le théorème stipule qu'il peut être exprimé comme la somme de deux carrés. En effet, $2450 = 7^2 + 49^2$.

La décomposition en nombres premiers du nombre 3430 est $2 \cdot 5 \cdot 7^3$. Cette fois, l'exposant de 7 dans la décomposition est 3, un nombre impair. Donc, 3430 ne peut pas être écrit comme la somme de deux carrés.

Nombres représentables

Les nombres qui peuvent être représentés comme la somme de deux carrés forment la suite d'entiers [2] :

$$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, \ldots$$

Ils forment l'ensemble de toutes les normes des entiers de Gauss [2] ; leurs racines carrées forment l'ensemble de toutes les longueurs des segments de droite entre paires de points dans le réseau d'entiers bidimensionnel.

Le nombre de nombres représentables dans l'intervalle de 0 à n'importe quel nombre n est proportionnel à $\frac{n}{\sqrt{\log n}}$ avec une constante limite de proportionnalité donnée par la constante de Landau-Ramanujan, approximativement 0.764 [3].

Le produit de deux nombres représentables quelconques est un autre nombre représentable. Sa représentation peut être dérivée des représentations de ses deux facteurs, en utilisant l'identité de Brahmagupta-Fibonacci.

Théorème des deux carrés de Jacobi

Théorème des deux carrés. Notons $d(n)$ le nombre de diviseurs de n, et écrivons $d_a(n)$ le nombre de ces diviseurs avec $d \equiv a \pmod 4$. Soit $n = 2^f p_1^{r_1} p_2^{r_2} \ldots q_1^{s_1} q_2^{s_2} \ldots$ où $p_i \equiv 1 \pmod 4$, $\mathrm{q}_i \equiv 3 \pmod 4$.

Soit $r_2(n)$ le nombre de façons dont n peut être représenté comme la somme de deux carrés.

Alors, $r_2(n) = 0$ si l'un des exposants s_j est impair. Si tous les s_j sont pairs, alors $r_2(n) = 4d(p_1^{r_1} p_2^{r_2} \ldots) = 4(d_1(n) - d_3(n))$.

Démontré par Gauss à l'aide de formes quadratiques et par Jacobi à l'aide de fonctions elliptiques [4]. Une démonstration élémentaire est basée sur la factorisation unique des entiers de Gauss [4]. Hirschhorn donne une courte démonstration dérivée du produit triple de Jacobi [5].

Références

1. Dudley, Underwood (1969). "Sums of Two Squares". Elementary Number Theory. W.H. Freeman and Company. p. 135-139.

2. Sloane, N. J. A. (ed.). "Sequence A001481 (Nombres qui sont sommes de deux carrés)" (https://oeis.org/A001481). The On-Line Encyclopedia of Integer Sequences. OEIS Foundation.

3. Rebák, Örs (2020). "Generalization of a Ramanujan identity". The American Mathematical Monthly. 127 (1) : 80-83. arXiv:1612.08307 (https://arxiv.org/abs/1612.08307). MR 4043992 (https://mathscinet.ams.org/mathscinet-getitem?mr=4043992).

4. Grosswald, Emil (1985). Representations of integers as sums of squares. New York Berlin Heidelberg Tokyo, Springer-Verlag, 1985, pp. 15-19. ISBN 978-3-540-96126-0.

5. Hirschhorn, Michael (1985). "A simple proof of Jacobi's two-square theorem" (https://web.m aths.unsw.edu.au/-mikeh/webpapers/paper21.pdf).

Le théorème de Noël, un extrait de *L'univers des nombres*, de Ian Stewart, Belin Pour la Science, 2000.

Les trois fantômes de Stooge contribuent à discerner quand un nombre premier est égal à la somme de deux carrés.

C'était la veille de Noël : dans un bureau étroit et glacé, une horloge hissait inexorablement ses aiguilles vers la verticale pour y égrener un nombre parfait de coups. Bob Scratchit sécha son registre avec un papier buvard de Möbius, qui n'a qu'un seul côté et ne saurait donc être traversé par l'encre. Il ferma le registre et le replaça sur son rayon. Demain c'étaient ses vacances annuelles. Rien à faire pendant les factorielles quatre heures à venir. Il enfila son manteau et prit une écharpe si râpée que sa dimension fractale était inférieure à deux. En sortant, il passa devant son employeur.

"Joyeux Noël, Monsieur Stooge, dit-il gaiement.

- Bah ! Sottises, grogna le vieil homme ! Toutes les boutiques sont fermées le jour de Noël, Scratchit. Vous voyez ce que cela veut dire ?

- Un jour de repos, Monsieur Stooge !

- Cela veut dire, Scratchit, un jour sans un seul client, sans la moindre recette. Un jour où le tiroir-caisse des *Aux curiosités mathématiques d'autrefois* ne verra pas la couleur d'une pièce de monnaie !"

Cela n'était certes pas le moment rêvé, mais Scratchit avait promis à sa femme de demander.

"Euh... Monsieur ?

- Quoi encore ?

- Vous m'aviez promis une prime de Noël, Monsieur. C'est pour Whiny Jim, voyez-vous. Mon plus jeune, mon mécontent chronique, Monsieur. Juste un petit...

- Une prime ? Une prime ! Un mot de plus et vous êtes à la rue !"

Scratchit partit très déçu. Heureusement la bonne fée des Noëls mathématiques le prit en pitié. Elle inspira ses pensées, balaya son désespoir et lui offrit une vision plus positive de la situation.

"Aucun cadeau, s'écria Whiny Jim ?

- Nous les fabriquerons nous-mêmes, fils, dit Scratchit dont l'optimisme décroissait exponentiellement.

- Je veux un cadeau ! Je veux un nouveau théorème ! Ou au moins un lemme d'occasion ! On en a donné un magnifique à mon ami Charlie Pickens. Même une conjecture serait mieux que rien !

- Je suis désolé, Whiny Jim, mais M. Stooge garde même ses conjectures. Je n'arriverai pas, j'en ai peur, à imaginer un sophisme. Je suis positivement vidé.

- Ton problème, Papa, c'est que tu n'as aucune ambition. Tu devrais postuler pour le job que propose Pythie Appolonius, prêteuse sur gages. Tu sais, celle qui se promène toujours avec un sandwich.

- Je sais, Whiny Jim, la Pythie vient en mangeant. Mais je suis un homme fier, jamais je ne tomberai assez bas pour vendre des triangles rectangles râpés aux hypoténuses à l'envers !"

Scratchit s'efforça de se calmer.

"Il doit rester, depuis Pâques, du traditionnel pudding à l'eau et nous nous en contenterons, comme à chaque Noël. Tout au plus, tu seras bien heureux si je réussis à déterrer un de ces vieux paradoxes que votre mère m'a donnés. Une couche toute fraîche de logique moderne et il sera comme neuf !

- De logique intuitionniste, demanda Jim plein d'espoir ? Pas encore de cette vieillerie binaire ? Brillante idée, mon garçon, reconnut Scratchit !"

Whiny Jim, temporairement apaisé, s'en alla, laissant Scratchit à la recherche d'un énoncé dont on ne puisse décider s'il est vrai ou faux. Il pensa appeler M. Stooge pour obtenir une valeur de vérité indéterminée, mais l'opérateur lui apprit que le numéro avait été déconnecté pour cause de sous-emploi.

Dans un appartement poussiéreux, de l'autre côté de la ville, Ebeneezer Stooge se pelotonnait dans son lit, des idées d'argent ou d'impôts dansant dans la tête.

Il s'éveilla comme un vent froid agitait les rideaux et les vitres. Il sauta de son lit pour fermer la fenêtre, mais la trouva bien close. Mais alors, par où le vent...

"Ebeneeeeeezerrr", souffla une voix lugubre.

Stooge bondit dans le lit et se blottit sous les couvertures.

"Qui... Qui êtes-vous ?

- Je suis l'*Esprit des théorèmes anciens*. Je suis venu pour vous emmener, Stooge", dit l'Esprit qui étendit ses mains éthérées, que Stooge empoigna à contrecœur.

Stooge se retrouva tout d'un coup dans une pièce lambrissée. Un homme vêtu d'une robe noire écrivait avec une plume d'oie.

"Où sommes-nous, demanda Stooge ?

- En France. Le jour de Noël, il y a exactement 350 ans.

- Et qui est ce fat en faux cheveux ?

- Le gentleman qui porte perruque, Stooge, est le grand mathématicien Pierre de Fermat, célèbre pour son "dernier théorème", tout récemment démontré, et l'un des fondateurs de la théorie des nombres. Il écrit une lettre à son ami Marin Mersenne. Si nous revenions à notre époque, nous pourrions lire l'original de la lettre, datée du 25 décembre 1640. La lettre annonce à Mersenne une merveilleuse découverte.

- Et en quoi consistait-elle ?

- Elle est connue sous le nom de "théorème de Noël de Fermat". Certains nombres premiers sont les sommes de deux carrés parfaits. Ainsi : $5 = 1 + 4 = 1^2 + 2^2$ ou bien $13 = 4 + 9 = 2^2 + 3^2$. D'autres nombres premiers ne peuvent s'écrire ainsi c'est le cas de 3 ou de 11. Fermat a découvert quels nombres premiers sont somme de deux carrés."

Stooge sortit un calepin de peau et commença à calculer. Il eut vite résolu le problème pour les nombres premiers jusqu'à 100 *(voir la figure 1)*.

"Vois-tu la loi, demanda l'*Esprit des théorèmes anciens* ?"

Stooge secoua la tête.

"Comme c'est Noël, je te donnerai deux indications. La première consiste à ignorer le nombre premier 2, qui est exceptionnel (par exemple, en tant qu'unique nombre premier pair !). La seconde est d'examiner les restes de la division des nombres premiers par 4. Chaque premier impair est multiple de 4 plus 1 ou plus 3, c'est dire qu'il est de la forme $4k + 1$ ou $4k + 3$. Ainsi, par exemple, 5 est égal à $(4 \times 1) + 1$, c'est-à-dire de la forme $4k + 1$.

Stooge ajouta une nouvelle colonne à sa table pour y inscrire une marque indiquant quand chaque nombre premier était de la forme $4k + 1$ ou $4k + 3$ la loi était dès lors manifeste.

"Les premiers nombres premiers pouvant s'exprimer en somme de carrés semblent être tous de la forme $4k + 1$ dit Stooge étonné. À part 2, que vous m'aviez signalé comme faisant exception.

- Excellent. Mais Fermat ne se contenta pas de le subodorer, il le prouva. Pour le moins, il esquissa une méthode de démonstration."

Et, alors que l'*Esprit des théorèmes anciens* commençait à disparaître, Stooge pouvait encore l'entendre murmurer : "Ce n'est que vers 1754 que Leonhard Euler le démontra complètement..."

Et Stooge se retrouva dans sa chambre glacée. Il essaya de dormir, mais ce théorème de Fermat ne cessait de tourner dans sa tête. Nombres premiers, sommes de deux carrés, restes dans les divisions par 4... Rêveries gratuites ! Il s'agita, se tourna, fit une descente au garde-manger, mais ne trouva pas le sommeil.

Pendant ce temps. Bob Scratchit s'agitait et se retournait, se demandant où diable il pourrait trouver à temps une valeur de vérité indéterminée pour la glisser dans les bas de laine de Noël de Whiny Jim. Il n'y avait pas $29 = 4 + 25$ secondes que Stooge dormait enfin, qu'il entendit un hurlement terrible, puis un fracas de tonnerre. Le pot de nuit du pasteur Snows lancé sur le chat de la veuve Kleene ? Non, le bruit venait de l'intérieur de la chambre d'Ebeneezer. Il frissonna de peur : une forme lumineuse se matérialisa devant lui.

La forme gronda :

"Je suis l'*Esprit des intuitions futures*.

Abominable créature, agis à ta guise, je suis trop las pour résister."

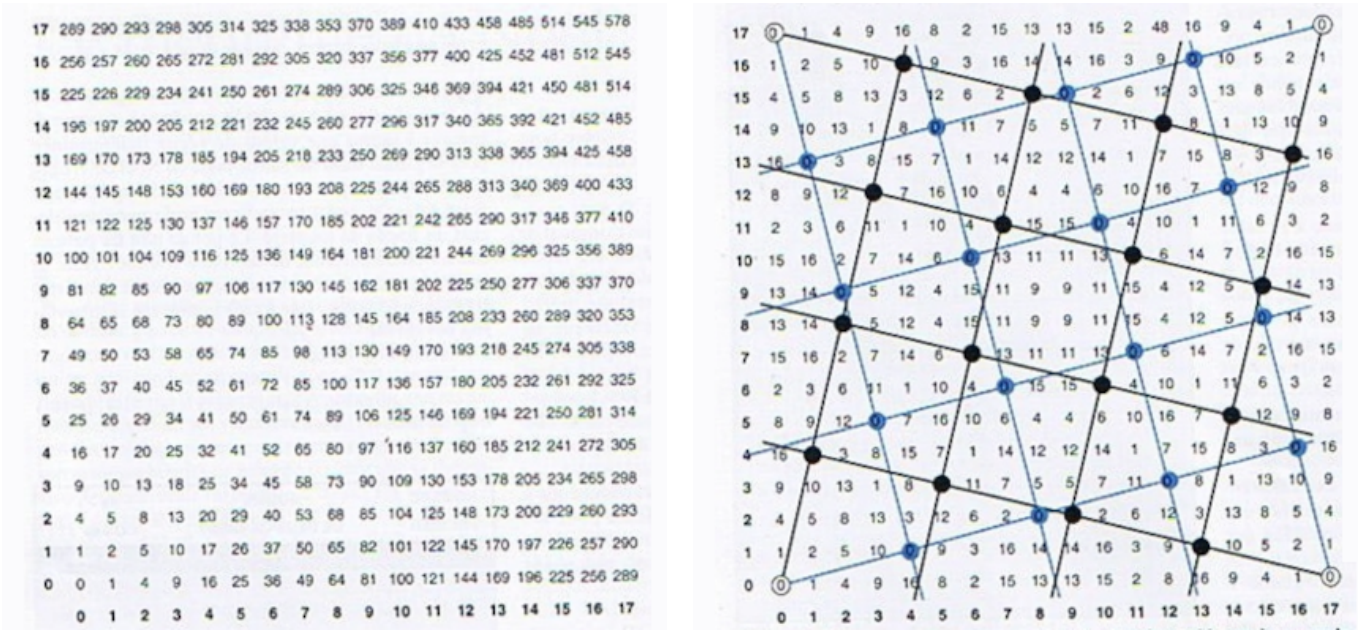
Nombre premier	Somme de deux carrés?	$4k+1$ ou $4k+3$?
2	$1^2 + 1^2$	exception
3	non	$(4 \times 0) + 3$
5	$1^2 + 2^2$	$(4 \times 1) + 1$
7	non	$(4 \times 1) + 3$
11	non	$(4 \times 2) + 3$
13	$2^2 + 3^2$	$(4 \times 3) + 1$
17	$1^2 + 4^2$	$(4 \times 4) + 1$
19	non	$(4 \times 4) + 3$
23	non	$(4 \times 5) + 3$
29	$2^2 + 5^2$	$(4 \times 7) + 1$
31	non	$(4 \times 7) + 3$
37	$1^2 + 6^2$	$(4 \times 9) + 1$
41	$4^2 + 5^2$	$(4 \times 10) + 1$
43	non	$(4 \times 10) + 3$
47	non	$(4 \times 11) + 3$
53	$2^2 + 7^2$	$(4 \times 13) + 1$
59	non	$(4 \times 14) + 3$
61	$5^2 + 6^2$	$(4 \times 15) + 1$
67	non	$(4 \times 16) + 3$
71	non	$(4 \times 17) + 3$
73	$3^2 + 8^2$	$(4 \times 18) + 1$
79	non	$(4 \times 19) + 3$
83	non	$(4 \times 20) + 3$
89	$5^2 + 8^2$	$(4 \times 22) + 1$
97	$4^2 + 9^2$	$(4 \times 24) + 1$

1. Quels sont les nombres premiers qui peuvent s'exprimer comme une somme de deux carrés ?

L'*Esprit des intuitions futures* plaça une boîte sur la table et ordonna à Stooge : "Ouvre-la !"

À l'intérieur, Stooge découvrit quelque chose qui ressemblait à une loupe de joaillier munie d'un cadran. Il prit la chose en main.

"Qu'est-ce ?"



2. La table des sommes des carrés (à gauche) et la même table vue à travers le moduloscope réglé sur le canal 17 (à droites).

“C’est un moduloscope. Il permet de ne pas voir ce que l’on désire ignorer.

- Comme le font les pauvres ? Moi, par exemple.

- Avec un moduloscope, on efface ce que l’on veut, et définitivement. Par exemple, quand on règle le cadran sur un entier et que l’on regarde dans l’appareil, tous les multiples de ce nombre auront disparu. Place-le sur le “canal 4” et observe mes deux mains : combien vois-tu de doigts ?

- Deux. Les huit autres ont disparu.

- Le moduloscope commence par éliminer huit doigts, car 8 est le plus grand multiple de 4 ne dépassant pas 10, puis il exhibe les deux doigts restants. Les mathématiciens décrivent l’opération plus succinctement ainsi : 10 est égal à 2 modulo 4.

Stooge observa dans le moduloscope les 147 pièces d’or qu’il avait déposées sur sa table de nuit. N’en voyant que trois, il poussa des cris aigus, éloigna vivement l’appareil de ses yeux et nota, pour son plus grand soulagement, que toutes les pièces étaient encore là.

“Trêve d’enfantillages, dit sèchement l’Esprit. Sors ton calepin et observe la table des nombres premiers en restant sur le canal 4. Que vois-tu ?

- Je ne vois que des 1 et des 3, sauf pour 2 qui est exceptionnel. Et chaque nombre premier somme de deux carrés est devenu un 1. alors que les autres sont vus comme 3. Mais bien sûr ce n’est là que l’alternative $4k + 1$ ou $4k + 3$, c’est-à-dire l’égalité soit à 1, soit à 3 modulo 4.”

Il fit une pause.

“Mais je ne vois toujours pas pourquoi la valeur des nombres premiers modulo 4 a une importance.

- Au lieu des nombres premiers, observe à présent les carrés.”

Stooge scruta la table au moduloscope. Après un long silence : “Tout ce que je vois, ce sont des équations évidentes comme $1 = 0 + 1$ indéfiniment répétées.

- Oui, et tu devines pourquoi ?

- Parce que, modulo 4, les carrés sont tous égaux à 0 ou 1 ?

- Exactement. Le carré $4k^2$ d'un nombre pair est un multiple de 4, soit 0 dans le moduloscope canal 4, et celui d'un nombre impair, 1, 9, 25, 49..., sont tous des multiples de 4 augmentés de 1. De sorte que les sommes de carrés modulo 4 sont $0+0 = 0$, soit $0+1 = 1$ soit $1+1 = 2$. Que manque-t-il ?

• 3, dit Stooge.

- Exact. Une somme de deux carrés peut être égale à 0, 1 ou 2 modulo 4, mais jamais égale à 3, de sorte que les nombres premiers et les autres de la forme $4k + 3$ ne sauraient être somme de deux carrés. Et maintenant tu vois l'importance du modulo 4, non ?”

C'est alors que l'Esprit commença à disparaître.

“Ne partez pas, supplia Stooge ! Tout ceci est bel et bien. Il est clair que tout premier de la forme $4k + 3$ n'est pas somme de deux carrés, mais nous n'avons pas prouvé que ceux de la forme $4k + 1$ le sont toujours, n'est-ce pas ?”

La réponse lui parvint faiblement :

“C'est exact. Mais la solution est proche. Garde le moduloscope et aaattteeennndddsss...

- Diantre, pensa Stooge, il doit y avoir un autre Esprit. Les ennuis vont toujours par trois.”

Se tournant vers le plafond, il cria : “Allons, un effort, matérialisez-vous, nous n'allons pas y passer la nuit !

- Je suis l'Esp... Atchoum !

- Pardon ?

- L'*Esprit des démonstrations actuelles*. Comme il fait froid ici ! Tu ne fais jamais de feu ?”

L'Esprit se moucha bruyamment dans son linceul.

“Êtes-vous venu me montrer comment prouver que tout nombre premier de la forme $4k + 1$ est

somme de deux carrés ?

- Tout à fait ! Nous, Esprits, avons parfois de singulières activités. Mais assez de temps perdu, Ebeneezer Stooge. Règle sur le canal 17 et tout te sera révélé !"

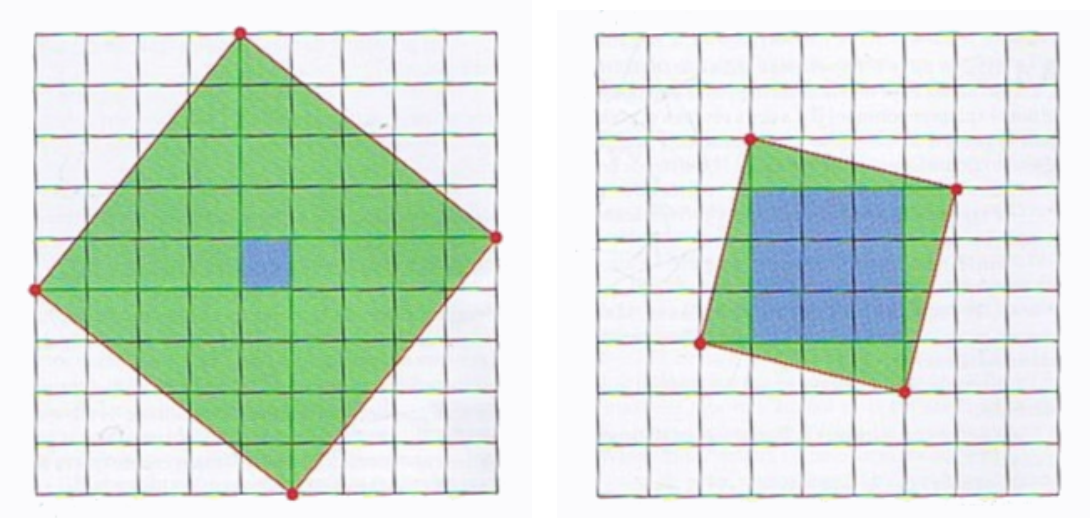
Avec un geste emphatique, l'*Esprit des démonstrations actuelles* exhiba une feuille de plastique, divisée en carrés, et la posa sur la table.

"Je vais te faire la démonstration pour 17, mais la méthode est générale. L'idée, Ebeneezer mon ami, est de partir des sommes de deux carrés et non des nombres premiers. Cette feuille spéciale indique toutes les sommes possibles de deux carrés avec x^2+y^2 noté colonne x et ligne y. Observe-la dans le moduloscope. Que vois-tu ?

- Il y a des nombres partout, tous compris entre 0 et 16.

- Hmmph, bien sûr, suis-je sot ! Prends cette plume d'oie et entoure chacun des 0, d'accord ?"

Stooge fit alors apparaître un curieux ensemble périodique de cercles (*voir la figure 2*), l'observa longuement, puis secoua la tête d'un air dubitatif.



3. Quelle est l'aire du parallélogramme maille d'un réseau formé par les sommes de carrés égales à zéro modulo 17 (à gauche) ou modulo 41 (à droite) ?

"Il y a une structure cachée, dit l'Esprit. Laisse-moi colorier certains cercles en rouge et les autres en bleu... Remarques-tu quelque chose ?

- Saperlotte ! Il y a deux grilles régulières posées l'une sur l'autre.

- Exact ! Le nom technique d'une telle grille est un réseau. Nous avons colorié les points (x, y) sur la colonne x et la ligne y, tels que x^2+y^2 soit un multiple de 17. A présent, examine le réseau rouge et dis-moi lequel de ses points est le plus proche de l'origine (colonne 0, ligne 0).

- Facile, c'est le point $(1; 4)$.

- Et la somme de carrés correspondante est quel multiple de 17 ?

• $1^2 + 4^2 = 17$ lui-même ! Je vois ! Le point du réseau rouge le plus proche de l'origine résout le problème de la représentation de 17 en somme de deux carrés.

- Tout à fait exact. Et il en est de même du réseau bleu, si ce n'est que la solution est dans l'ordre inverse $4^2+1^2 = 17$. Fais un autre essai, sur le canal 41 cette fois. Observes-tu le même phénomène ?

- Oui, voyez, encore deux réseaux superposés, s'écria Stooge. Et le point du réseau rouge le plus proche de l'origine est $(4; 5)$, et $4^2 + 5^2$ est bien égal à 41 !

- Superbe ! Résumons-nous : tu choisis un nombre premier p, tu marques les points (x, y) tels que $x^2 + y^2$ soit multiple de p et, dans tous les cas, tu obtiens une réunion de deux réseaux, encore que tu ne l'aurais probablement pas remarqué si je ne te l'avais fait observer pour p égal à 17.

Mais, je suis l'*Esprit des démonstrations actuelles* et je ne me contente pas d'exemples ! Je dois expliquer pourquoi il y a deux réseaux et pourquoi le point d'un réseau le plus proche de l'origine résout toujours le problème ! D'abord : l'existence des deux réseaux. Cela résulte des racines carrées de -1.

- J'ignorais que -1 eût des racines carrées, interrompit Stooge.

- Ah ! Aucun nombre réel n'a pour carré -1, aussi a-t-on introduit un nouveau nombre, noté i, tel que $i^2 = -1$ et engendré les nombres complexes. Mais avec un moduloscope, les nombres complexes ne sont pas nécessaires."

L'Esprit écrivit quelque chose sur la feuille de plastique.

"Observe ceci à travers le moduloscope réglé sur le canal 17."

Stooge lut : $x^2 + y^2 = (x + 4y)(x - 4y)$.

"Absurde !"

Mais la plupart des choses sont absurdes vues au moduloscope, jusqu'à ce qu'on les interprète autrement. L'algèbre nous enseigne que $(x + 4y)(x - 4y) = x^2 - 16y^2$. Mais au moduloscope -16 est égal à $17-16$ (les multiples de 17 étant invisibles), c'est-à-dire à 1. Et l'on a bien $x^2-16y^2 = x^2+y^2$.

"Les points que nous avons entourés, fit alors remarquer l'Esprit, sont ceux qui, vus au moduloscope, vérifient l'équation $x^2 + y^2 = 0$ qui, modulo 17, se factorisent en $(x + 4y)(x - 4y) = 0$ soit en $x = -4y$ ou $x = 4y$. Chacune de ces équations correspond à un réseau. Le réseau rouge est donné par $x = -4y$ et le bleu par $x = 4y$. Tout ceci modulo 17 bien entendu ! Examinons les réseaux et vérifions. Par exemple, sur le réseau bleu, on trouve les points $(4; 1), (8; 2), (12; 3), (16; 4) \ldots$ qui sont solutions de l'équation $x = 4y$."

“Voici le premier point important. Regarde au moduloscope réglé sur le canal 17, le nombre -1 a une racine carrée, à savoir 4, car $4^2 + 1 = 17 = 0$. Et ceci conduit directement à l'existence des deux réseaux. Il en est de même pour tout nombre premier de la forme $4k + 1$ c'est-à-dire ceux qui sont précisément les modulo pour lesquels -1 a une racine carrée. Es-tu prêt pour le deuxième point important ?

- On ne saurait être plus prêt, affirma Stooge.

- Tout réseau est constitué de parallélogrammes identiques. Ici les parallélogrammes sont en fait des losanges, mais pour beaucoup de réseaux, il n'en va pas de même, aussi garderons-nous le mot parallélogramme. Quelle est l'aire d'un tel parallélogramme ? Essaye sur quelques exemples.”

Ebeneezer griffonna sur son calepin. “Pour p égal à 17, l'aire d'un parallélogramme est 17 carrés unités, et pour p égal à 41, c'est 41 carrés unités (*voir la figure 3*). Je suppose que pour un nombre premier quelconque p l'aire du parallélogramme maille serait p carrés unités.

- Tout à fait exact, encore que nous n'ayons pas le temps de le prouver. Tu te demandes sans doute pourquoi je m'intéresse à l'aire des parallélogrammes.

- Ca ne m'avait pas traversé l'esprit, je veux dire... Je n'y avais pas pensé.

- C'est à cause d'un théorème prouvé par Hermann Minkowski, un mathématicien russe qui enseigna en Allemagne. Il inventa l'espace de Minkowski, qu'Albert Einstein utilisa dans sa théorie de la relativité. Concernant les réseaux, Minkowski eut une idée remarquable et extrêmement simple : si l'aire des parallélogrammes est petite, alors les sommets du réseau sont proches les uns des autres. Et donc certains doivent être proches de l'origine.

“En précisant tout cela, il démontra un théorème. Si l'on se donne un réseau de parallélogrammes et un cercle centré à l'origine, le théorème de Minkowski énonce que si l'aire du cercle vaut au moins quatre fois celle d'un parallélogramme maille, alors au moins un des sommets du réseau, autre que l'origine, est intérieur au cercle.

Nous pouvons utiliser le théorème de Minkowski pour montrer notre second point : un sommet du réseau le plus proche possible de l'origine résout le problème de la décomposition de p en somme de deux carrés. Raisonnons sur l'exemple $p = 17$. Prenons un cercle de rayon légèrement supérieur à $\sqrt{17}$, de rayon 5 par exemple. Son aire est $5^2\pi = 25\pi$, soit environ 78.54 : elle est supérieure à $4 \times 17 = 68$, de sorte que le théorème de Minkowski s'applique. Me suis-tu jusqu'ici ?

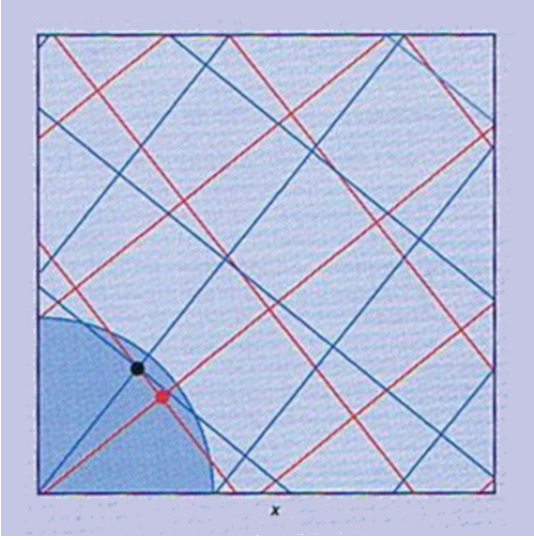
- Je suis suspendu à vos lèvres.

- D'après ce théorème, le réseau a au moins un point autre que l'origine dans le cercle. Soit (x, y) l'un de ces points. On a donc $x^2 + y^2$ qui est inférieur ou égal au carré du rayon du cercle (*voir la figure 4*), c'est-à-dire $x^2 + y^2$ inférieur à 25. Mais pour les points du réseau, $x^2 + y^2$ est un multiple de 17. Le point n'étant pas l'origine, ce multiple ne peut être 0. Quels multiples de 17 vois-tu entre

0 et 25, 0 exclu ?

- 17 lui-même, et c'est tout, dit Stooge.

- Correct ! Ainsi $x^2+y^2 = 17$ et notre problème est résolu ! Et la méthode est générale, dit fièrement l'Esprit. Cette idée de Minkowski donna naissance à une nouvelle branche des mathématiques nommée la géométrie des nombres, d'après son livre de 1896 qui portait ce titre. Elle utilise la géométrie pour étudier la théorie des nombres. Deux sujets qu'on n'imaginait pas être connectés ! Une autre de ses applications est le fameux théorème des quatre carrés, lequel énonce que tout entier positif (premier ou non) est somme de quatre carrés parfaits. Mais nous laisserons ce problème hanter ta pensée jusqu'au prochain Noël, Ebeneezer."



4. La démonstration de Minkowski du théorème des deux carrés.

Whiny Jim s'éveilla de bonne humeur, ce matin de Noël. "Papa, papa : as-tu apporté le vieux paradoxe de grand-maman et sa couche fraîche de logique intuitionniste ? Celui avec une valeur de vérité indéterminée ?

- Eh bien, dit Scratchit, ce n'est pas facile à dire, fils."

Il se torturait les méninges, cherchant désespérément une formulation capable de faire cesser les cris à briser les tympans de Whiny Jim.

"Je ne suis pas sûr si je l'ai ou si je ne l'ai pas !"

C'était un coup de génie (ou peut-être l'*Esprit des intuitions futures* s'était-il assis sur ses épaules et lui avait-il chuchoté à l'oreille), car le visage de Whiny Jim s'éclaira comme un sapin de Noël.

"Oh, papa, merci beaucoup. Quel beau cadeau !".

Regardons les choses en face : on peut difficilement trouver une valeur de vérité plus indéterminée que la réponse de Scratchit.

Le théorème de Landau de 1908 [10]

Théorème. *Soit $S(x)$ le nombre de nombres n qui peuvent être représentés comme des sommes de deux carrés. On a que*

$$S(x) = K\frac{x}{\sqrt{\log x}} + \mathrm{O}\left(\frac{x}{(\log x)^{3/2}}\right),$$

où

$$K = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod 4} \left(1 - \frac{1}{p^2}\right)^{-1/2} \approx 0.764223653\ldots$$

appelé constante de Laudau-Ramanujan.

Preuve : le lecteur peut se reporter à l'exercice 6.2.21 dans la référence de H. L. Montgomery et R. C. Vaughan *Multiplicative Number Theory I : Classical Theory*, Cambridge University Press, 2006.

Un très court extrait du livre d'Underwood Dudley : *Is mathematics inevitable ? A miscellany* [11], page 93

4. Un théorème de Legendre (voir Davenport [6], par exemple) énonce que si D_+ et D_- sont les nombres de diviseurs de n de la forme $4k+1$ et $4k-1$, alors le nombre de représentations de n comme somme de deux carrés est $4(D_+ - D_-)$.

Donc $D_+ \geq D_-$ pour tout nombre ! [12]

Référence : [6] H. Davenport, *The Higher Arithmetic*, Hutchinson's University Library, 1952, p. 128.

10. Trouvé en annexe de l'article https://arxiv.org/pdf/2508.17662.
11. éds Mathematical Association of America, 2008.
12. *Note de la traductrice : Hum !* 2.5.5.7.7.7.7 *est bien sûr tel que* $D_+ < D_-$.