6

ETUDES

Sur la représentation d'un naturel par la somme de deux carrés

par E. EHRHART (Strasbourg)

La théorie des nombres est riche en propositions intéressantes, mais elles sont en général difficiles à établir. Parfois, cependant, on peut atteindre des théorèmes importants et curieux par des raisonnements élémentaires instructifs, quitte à admettre au départ certains résultats. On se propose d'en montrer un exemple.

Soit u_n le nombre de points de coordonnées entières portés par le cercle

$$X^2 + Y^2 = n \qquad (n \text{ naturel})$$

On démontre que $u_n = 4(d - d')$, où d et d' désignent respectivement les nombres de diviseurs de n de la forme $4K + 1$ et $4K - 1$.

La formule $u_n = 4(d-d')$ a été établie par Dirichlet à partir des formes quadratiques, mais seulement pour n impair (Journal für Math., 21, 1840, page 3). Elle a été retrouvée depuis par plusieurs auteurs.

Désignons par p et q respectivement les nombres premiers des congruences $4K + 1$ et $4K - 1$. La décomposition de n en facteurs premiers s'écrit alors

$$n = 2^\gamma \left(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}\right)\left(q_1^{\beta_1} q_2^{\beta_2} \dots q_s^{\beta_s}\right) = 2^\gamma PQ$$

Il est clair que :

$$(4K'+1)(4K''+1) = 4K+1$$
$$(4K'-1)(4K''-1) = 4K+1$$
$$(4K'+1)(4K''-1) = 4K-1$$

Tout diviseur impair de n est le produit d'un diviseur A de P par un diviseur B de Q. Notons que A est toujours de la forme 4K+1, tandis que B est de la forme 4K+1 ou 4K−1 suivant que le nombre de ses facteurs est pair ou impair.

Il existe $a = \prod_{i=1}^{r} (1+\alpha_i)$ diviseurs de A et $b = \prod_{i=1}^{s} (1+\beta_i)$ diviseurs de B. Nous allons montrer d'abord que si b est impair, $\frac{b-1}{2}$ des B sont des 4K−1 et $\frac{b+1}{2}$ des B sont des 4K+1, de sorte que

$$d-d' = a\frac{b+1}{2} - a\frac{b-1}{2} = a$$

et donc $u_n = 4a$; puis que si b est pair, $\frac{b}{2}$ des B sont des 4K+1 et les $\frac{b}{2}$ autres B sont des 4K−1, de sorte que

$$d = d' = a\frac{b}{2} \text{ et donc } u_n = 0 .$$

1) *b est impair*, c'est-à-dire tous les β sont pairs. Si $Q = q_1^{2m}$, ses diviseurs $B = q_1^{0}, q_1^{1}, q_1^{2}, \ldots q_1^{2m}$ forment une suite dont les termes appartiennent alternativement aux congruences $\mathcal{T}$ des 4K+1 et $\mathcal{Q}$ des 4K−1. Comme les termes extrêmes de la suite font partie de $\mathcal{T}$, il y a bien un B de plus dans $\mathcal{T}$ que dans $\mathcal{Q}$.

Raisonnons alors par récurrence sur

$$Q = \left(q_1^{2m_1}\ q_2^{2m_2} \ldots q_{s-1}^{2m_{s-1}}\right) q^{2m_s}$$

Supposons que les diviseurs du produit entre parenthèses peuvent se ranger dans une suite S de termes appartenant alternativement à $\mathcal{T}$ et à $\mathcal{Q}$, les termes extrêmes faisant partie de $\mathcal{T}$. Les diviseurs $q_s^{2m_s}$ forment une suite S' de même nature. Or les diviseurs de Q s'obtiennent en multipliant tous les termes de S par le premier terme de S', puis tous les termes de S par le second terme de S', etc. Les diviseurs B de Q seront ainsi rangés dans une suite S'' de même nature que S et S' : il y a donc encore un B de plus dans $\mathcal{T}$ que dans $\mathcal{Q}$.

2) *b est pair*, c'est-à-dire l'un au moins des β est impair. Soit d'abord β_s le seul β impair :

$$Q = \left(q_1^{2m_1}\ q_2^{2m_2}\ \dots\ q_{s-1}^{2m_{s-1}}\right)\ q_s^{2m_s+1}$$

Les diviseurs du produit entre parenthèses sont encore rangés dans la suite S. Les diviseurs $q_s^0, q_s^1, q_s^2 \dots q_s^{2m_s+1}$ de q^{2m_s+1} forment une suite T de termes appartenant alternativement à $\mathfrak{T}$ et à $\mathfrak{Q}$, le premier terme étant dans $\mathfrak{T}$ et le dernier dans $\mathfrak{Q}$. Les diviseurs de Q s'obtiennent en multipliant tous les termes de S par le premier terme de T, puis par le second terme de T, etc. Les diviseurs B de Q seront ainsi rangés dans une suite T' de même nature que T. Il y a donc autant de B dans $\mathfrak{T}$ que dans $\mathfrak{Q}$.

Raisonnons alors par récurrence.

Soit $Q = \left(q_1^{2m_1}\ q_2^{2m_2}\ \dots\ q_k^{2m_k}\right)\left(q_{k+1}^{2m_{k+1}+1}\ q_{k+r}^{2m_{k+r}+1}\ q_{s-1}^{2m_{s-1}+1}\right) q_s^{2m_s+1}$

Les diviseurs du premier produit entre parenthèses forment une suite S. Supposons que les diviseurs du second produit entre parenthèses peuvent se ranger en une suite T, de sorte que les diviseurs du produit des deux parenthèses peuvent être rangés en une suite T'.

Or les diviseurs de $q_s^{2m_s+1}$ se rangent en une suite T''. Les diviseurs de Q s'obtiennent en multipliant tous les termes de T' par le premier terme de T'' (ce qui donne autant de B dans $\mathfrak{T}$ que dans $\mathfrak{Q}$), puis tous les termes de T' par le second terme de T'' (ce qui donne encore autant de B dans $\mathfrak{T}$ que dans $\mathfrak{Q}$), etc. On voit donc que pour l'ensemble des B, il y en a autant dans $\mathfrak{T}$ que dans $\mathfrak{Q}$.

Résumons les résultats trouvés.

Théorème 1. Désignons par p *et* q *respectivement les nombres premiers de la forme* $4K+1$ *et* $4K-1$. *Le cercle* $X^2 + Y^2 = n$ *porte des points entiers si et seulement si, dans la décomposition en facteurs premiers de*

$$n = 2^{\gamma} p_1^{\alpha_1}\ p_2^{\alpha_2}\ \dots\ p_r^{\alpha_r}\ q_1^{\beta_1}\ q_2^{\beta_2}\ \dots\ q_s^{\beta_s}$$

tous les β sont pairs. Le nombre de ces points est alors *

$$4 \prod_{i=1}^{r} (1+\alpha_i)$$

Remarque 1. Pour que le théorème (et sa démonstration) s'applique aussi quand il n'y a pas de q dans la décomposition de n, on doit considérer que dans ce cas les β sont nuls ($q^0 = 1$) ; de même quand il n'y a pas de p, on doit considérer que les α sont nuls, de sorte que $\prod(1+\alpha_i) = 1$.

Comme corollaires, on obtient immédiatement les deux résultats classiques suivants :

Théorème 2. Tout nombre premier de la forme $4n+1$ *est égal à la somme de deux carrés.*

Théorème 3. Le produit de sommes de deux carrés est une somme de deux carrés.

Remarquons que le théorème 3 résulte aussi de l'identité :

$$(a^2 + b^2)(a'^2 + b'^2) = (aa' + bb')^2 + (ab' - a'b)^2$$

Notons aussi que si n et n' sont premiers entre eux et si les cercles $X^2 + Y^2 = n$, $X^2 + Y^2 = n'$ portent respectivement N et N' points entiers, le cercle $X^2 + Y^2 = nn'$ en porte $\frac{NN'}{4}$.

Théorème 4. Les cercles $X^2 + Y^2 = n$ *et* $X^2 + Y^2 = 2n$ *portent le même nombre de points entiers.*

Rappelons enfin deux théorèmes fameux :

Théorème de Bachet, 5. Tout naturel est égal à une somme de quatre carrés, dont certains peuvent être nuls.
(Pour la démonstration, voir par exemple l'article "Théorème de Bachet" de A. Buquet dans le Bulletin n° 198 de mars 1959)

Théorème de Gauss, 6. Un naturel est la somme de trois carrés si et seulement si il n'est pas de la forme $4^n(8k-1)$.
(Voir une démonstration dans le "Cours d'arithmétique" de J.P. Serre aux Presses Universitaires de France, 1970)

* Déjà en 1625 A. Girard savait qu'un entier est décomposable en somme de deux carrés si et seulement si sa décomposition en facteurs premiers ne présente pas de puissance impaire d'un premier de la forme $4K-1$ (L'arithmétique de Simon Stevin annotée par A. Girard, Leide, page 622). Gauss a trouvé le nombre $4\prod(\alpha_i+1)$ de ces décompositions en partant des formes quadratiques binaires (Oeuvres posthumes, pages 269-275).

Remarque 2. Pour appliquer le théorème 1, il n'est en général pas nécessaire de faire la décomposition complète de n en facteurs premiers. On peut en effet l'énoncer autrement :

Théorème 1 bis. Pour que le cercle $X^2 + Y^2 = n$ *porte des points entiers, il faut et il suffit que, débarrassé des facteurs 2 et des facteurs premiers de la forme* $4K+1$, n *devienne un carré parfait. Si alors l'ensemble des facteurs enlevés se présente sous la forme*

$$2^{\gamma} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

le nombre de points entiers du cercle est

$$4 \prod_{i=1}^{r} (1+\alpha_i)$$

Remarque 3. Le nombre u_n, déterminé pour tout $n \geqslant 0$, a une définition simple : c'est le nombre des décompositions de n en somme ordonnée de deux carrés de naturels. Son calcul par le théorème 1 bis est également simple, quoique éventuellement long, puisqu'il exige une décomposition partielle en facteurs premiers. Mais ce calcul s'énonce de manière assez compliquée ; on est loin des banales fonctions rationnelles, où il suffit de traiter n directement par "les quatre opérations". Le graphe cartésien de la fonction $n \longmapsto u(n)$ est une suite infinie et capricieuse de points, dont la plupart sont situés sur l'axe de n. Sans être croissant, $u(n)$ prend "dans l'ensemble" des valeurs de plus en plus grandes quand n croît et, sans être périodique, il reprend une infinité de fois toute valeur qu'il a prise une fois. Insolite arithmétique !

Remarque 4. En écrivant $u_n = 4(d_n - d'_n)$ pour $u_1, u_2, \dots, u_n$, en remarquant que $u_0 = 1$ et en ajoutant toutes ces égalités membre à membre, on retrouve sans difficulté un théorème célèbre, dû à Gauss :

Théorème 7. Le nombre de points entiers situés dans ou sur le cercle $X^2 + Y^2 = n$ *est*

$$V_n = 1 + 4\left(n - \left|\frac{n}{3}\right| + \left|\frac{n}{5}\right| - \left|\frac{n}{7}\right| + \dots\right) \quad \begin{cases} n \text{ naturel} \\ |a| = \text{partie entière de } a \end{cases}$$

Si dans cette expression on supprime les barres de partie entière, on obtient une approximation de V_n :

$$V_n \simeq 1 + 4n\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots\right) = 1 + \pi.n = 1 + S_n$$

De manière évidente, la surface S_n *du cercle est en effet une bonne approximation de* V_n.