Réponse de Pierre Renfer (Saint Georges d'Orques).

I - Premières propriétés

On étudie conjointement les ensembles

$A = \{2x^2 + 3y^2 \mid (x, y) \in \mathbb{Z}^2\}$ et $B = \{x^2 + 6y^2 \mid (x, y) \in \mathbb{Z}^2\}$.

Ceci est motivé par les résultats suivants, valable pour tout entier naturel n :

1. n appartient à A si et seulement si $2n$ appartient à B ;
2. n appartient à B si et seulement si $2n$ appartient à A;
3. n appartient à A si et seulement si $3n$ appartient à B ;
4. n appartient à B si et seulement si $3n$ appartient à A.

Le premier point résulte de l'égalité

$$2\left(2x^2+3y^2\right)=\left(2x\right)^2+6y^2,$$

et les points suivants se démontrent de la même façon.

Par ailleurs, pour tout entier n et tout entier d, on vérifie facilement que

1. n appartient à A si et seulement d^2n appartient à A ;
2. n appartient à B si et seulement d^2n appartient à B.

Il suffit donc de chercher dans A et B les entiers impairs, non multiples de 3, sans facteur carré, ce que l'on fait désormais. On note A′ (resp. B′) l'ensemble des éléments de A (resp. de B) de cette forme.

On commence par montrer que les ensembles A′ et B′ sont disjoints. En effet, les carrés modulo 8 sont 0, 1, 4 donc $2x^2 + 3y^2$ vaut 0, 2, 3, 4, 5 ou 6 modulo 8. Si $2x^2 + 3y^2$ est dans A′, il vaut 3 ou 5 modulo 8. Les carrés modulo 3 sont 0 et 1, donc $2x^2 + 3y^2$ vaut 0 ou 2 modulo 3. Si $2x^2 + 3y^2$ est dans A′, il vaut 2 modulo 3. Finalement, si $2x^2 + 3y^2$ est dans A′, il vaut 5 ou 11 modulo 24. On montre de même que si $x^2 + 6y^2$ est dans B′, il vaut 1 ou 7 modulo 24, ce qui montre que A′ et B′ sont effectivement disjoints.

II - Formes quadratiques de discriminant –24

On considère toutes les formes quadratiques définies positives

$$\left(x,y\right)\mapsto ax^2+bxy+cy^2,$$

avec

$$a,c\in\mathbb{N}^*,\quad b\in\mathbb{Z},\quad \Delta=b^2-4ac=-24.$$

À une telle forme est associée la matrice

$$\mathrm{M}=\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$$

de telle sorte que

$$ax^2+bxy+cy^2=\left(x,y\right)\mathrm{M}\begin{pmatrix} x \\ y \end{pmatrix}.$$

Deux formes quadratiques q et q' sont équivalentes si leurs matrices M et M′ vérifient

$$\mathrm{M}'={}^t\mathrm{PMP},$$

où $\mathrm{P}\in \mathrm{GL}(2,\mathbb{Z})$, c'est-à-dire que M est une matrice 2×2, à coefficients entiers, de déterminant ±1. Cela signifie que $q' = q \circ f$ où f est un isomorphisme du $\mathbb{Z}$-module $\mathbb{Z}^2$.

Les images de $\mathbb{Z}^2$ par deux formes quadratiques équivalentes sont les mêmes. Les deux formes définissant A et B ne sont donc pas équivalentes.

On va montrer que toute forme quadratique définie positive, de déterminant −24, est équivalente à l'une de nos deux formes.
Toute forme quadratique est équivalente à une forme q dont le premier coefficient est le minimum de l'ensemble des valeurs strictement positives prises par q. En effet, il suffit de choisir pour f un isomorphisme qui transforme (1, 0) en un couple antécédent de a par q.

La forme quadratique de matrice $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ est équivalente à celle de matrice $\begin{pmatrix} a & -b/2 \\ -b/2 & c \end{pmatrix}$, en prenant $\mathrm{P} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, ce qui permet de supposer $b \geq 0$.
Soit $b = 2an + r$ avec $0 \leq r < 2a$, la division euclidienne de b par $2a$. En choisissant $\mathrm{P} = \begin{pmatrix} 1 & -n-1 \\ 0 & 1 \end{pmatrix}$ si $r \leq a$, et $\mathrm{P} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$ si $a < r \leq 2a$, on obtient une matrice $\begin{pmatrix} a & b'/2 \\ b'/2 & c' \end{pmatrix}$ d'une forme équivalente à celle de la matrice $\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$ qui vérifie $|b'| \leq a$. Comme c' est une valeur prise par la forme quadratique, on a l'inégalité $a \leq c'$. Mais alors

$$-24 = b'^2 - 4ac' \leq -3a^2,$$

et donc $0 < a \leq 2$. Les deux seules possibilités sont donc

$$a = 1, b' = 0, c' = 6,$$

ou bien

$$a = 2, b' = 0, c' = 3.$$

III - Résidus quadratiques

Si p est un nombre premier impair et n un entier non multiple de p, le symbole de Legendre $\left(\frac{n}{p}\right)$ vaut 1 si n est un carré modulo p et vaut −1 sinon. Classiquement, si p est un nombre premier distinct de 2 et 3,

$$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right).$$

Or, on sait[1] que

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

(1) Pour plus de précisions sur le symbole de Legendre et la réciprocité quadratique, on pourra consulter le « Cours d'Arithmétique » de Jean-Pierre Serre, publié aux PUF.

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

et la loi de réciprocité quadratique donne

$$\left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}\frac{3-1}{2}}\left(\frac{p}{3}\right)=(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right).$$

Ainsi,

$$\left(\frac{-6}{p}\right)=(-1)^{\frac{p^2-1}{8}}\left(\frac{p}{3}\right).$$

On en déduit que pour un nombre premier congru à 1, 5, 7 ou 11 modulo 24, l'entier −6 est un carré modulo p.
Plus généralement, pour tout entier n, produit de nombres premiers (deux à deux distincts) de ce type, −6 est un carré modulo n. Il existe donc des entiers positifs b et c tels que

$$-6 = b^2 - cn.$$

La forme quadratique $nx^2 - 2bxy + cy^2$ est donc de discriminant −24. Elle prend la valeur n en $(x, y) = (1, 0)$. Suivant la classe d'équivalence de cette forme, le nombre n appartient à l'ensemble A′ ou B′.
Réciproquement, si une forme quadratique $ax^2 + 2bxy + cy^2$ de discriminant −24 prend une valeur n, divisible par un facteur premier p distinct de 2 et 3, mais non divisible par p^2, alors

$$a^2x^2 + 2abxy + acy^2 = (ax + by)^2 + 6y^2 \equiv 0 \mod p.$$

La classe de y est inversible dans $\mathbb{Z}/p\mathbb{Z}$, sinon n serait divisible par p^2. Donc la classe de −6 est un carré dans $\mathbb{Z}/\mathrm{p}\mathbb{Z}$ et p est congru à 1, 5, 7 ou 11 modulo 24.

IV - Conclusion

Soit P l'ensemble des nombres premiers congrus à 5 ou 11 modulo 24 et soit Q l'ensemble des nombres premiers congrus à 1 ou 7 modulo 24
Tout entier strictement positif n s'écrit $n = d^2m$, où m est sans facteur carré.
Alors, n appartient à A ∪ B si et seulement si la décomposition en facteurs premiers de m ne comporte que des facteurs de P ∪ Q ∪ {2, 3}, c'est-à-dire si

$$m = 2^{\alpha}3^{\beta}p_1 \ldots p_jq_1 \ldots q_k,$$

où α, β sont dans {0, 1} et où $p_1, \ldots, p_j$ sont des éléments distincts de P et $q_1, \ldots, q_k$ sont des éléments distincts de Q.
Le produit de deux éléments de B est encore dans B. Le produit de deux éléments de A est dans B. Le produit d'un élément de A et d'un élément de B est dans A.
Finalement, le nombre n appartient à A si $\alpha + \beta + j$ est pair et appartient à B si $\alpha + \beta + j$ est impair.