Autour de quelques équations diophantiennes

Daniel PERRIN

L'objectif initial de ce texte était d'étudier l'équation diophantienne : $3x^2 - 35y^2 = c$ avec $c \in \mathbf{N}^*$, voire $c \in \mathbf{Z}$, c'est-à-dire de chercher si cette équation admet des solutions x, y entières. C'est un exercice qui figure, sous une forme très édulcorée [1] dans [ME] et que nous [2] donnons aussi parfois en dossier de CAPES. Il s'est un peu élargi dans la mesure où la résolution de cette question oblige à considérer d'autres équations et notamment celles de même discriminant $105 = 3 \times 5 \times 7$ comme $x^2 - 105y^2 = c$.

1 Formes quadratiques de discriminant 105

1.1 Équivalence des formes quadratiques entières

On s'intéresse aux formes quadratiques sur $\mathbf{Z}^2$, de la forme $q(x, y) = ax^2 - by^2$ avec $a, b \in \mathbf{N}^*$ et on suppose a et b premiers entre eux et sans facteur carré. Le discriminant d'une telle forme est [3] ab. Deux formes quadratiques q, q' à coefficients entiers sont dites **équivalentes** sur $\mathbf{Z}$ (et on note $q \sim q'$) si l'on passe de l'une à l'autre par un changement de base à coefficients entiers. Si A, A' sont les matrices de ces formes, cela signifie qu'il existe $P \in GL(2, \mathbf{Z})$ telle que $A' = {}^tPAP$. Le résultat suivant nous sera utile :

1.1 Proposition. *Soit $a' \in \mathbf{N}^*$ un diviseur de ab. On pose $ab = a'b'$. Si la forme q représente [4] a', elle est équivalente à $a'x^2 - b'y^2$.*

Démonstration. On écrit $a' = a''b''$ avec a'' et b'' respectivement diviseurs de a et b. Il existe $\alpha, \beta \in \mathbf{Z}$ tels que $q(\alpha, \beta) = a\alpha^2 - b\beta^2 = a'$ et α, β sont premiers entre eux (sinon ab admet un facteur carré). On pose $\epsilon_1 = (\alpha, \beta)$ et on cherche un vecteur $\epsilon_2 = (\gamma, \delta)$ de $\mathbf{Z}^2$ tel que ϵ_1, ϵ_2 soit une $\mathbf{Z}$-base de $\mathbf{Z}^2$, autrement dit qu'on ait $\alpha\delta - \beta\gamma = 1$, et que les vecteurs ϵ_1 et ϵ_2 soient orthogonaux pour q, donc qu'on ait $a\alpha\gamma = b\beta\delta$. On a $a = a''a_1$ et $b = b''b_1$

1. On y étudie seulement le cas $1 \leq c \leq 20$.
2. Je l'ai donné, ainsi que Laure Blasco, que je remercie de ses commentaires.
3. Les arithméticiens disent plutôt $4ab$.
4. C'est-à-dire s'il existe $x, y \in \mathbf{Z}$ tels que $q(x, y) = a'$.

et, en vertu du théorème de Gauss, $\alpha = b''\alpha'$ et $\beta = a''\beta'$. On vérifie alors que $\gamma = b_1\beta'$ et $\delta = a_1\alpha'$ conviennent.

1.2 Les formes de discriminant 105

Commmençons par un inventaire des formes de discriminant 105 :

1.2 Proposition. *Il y a* 8 *formes quadratiques entières de discriminant* 105*, deux à deux équivalentes, dont voici la liste :*

$$q_1(x,y) = x^2 - 105y^2 \sim 21x^2 - 5y^2,$$
$$q_3(x,y) = 3x^2 - 35y^2 \sim 7x^2 - 15y^2,$$
$$q_{-1}(x,y) = -q_1(y,x) = 105x^2 - y^2 \sim 5x^2 - 21y^2,$$
$$q_{-3}(x,y) = -q_3(y,x) = 35x^2 - 3y^2 \sim 15x^2 - 7y^2.$$

Démonstration. Il suffit de faire le tour des 8 diviseurs de 105. L'équivalence résulte de 1.1 en notant qu'on a $-5 = 10^2 - 105$ et $7 = 3 \times 7^2 - 35 \times 2^2$. Inversement, comme deux formes équivalentes représentent les mêmes entiers, on voit facilement, par les arguments de congruences de 4.2, que les quatre formes ne sont pas équivalentes.

1.3 Définition. *Pour $k = 1, 3, -1, -3$, on note S_k l'ensemble des $c \in \mathbf{Z}$ tels que l'équation $q_k(x,y) = c$ (notée $E_k(c)$, voire E_k) admette une solution entière.*

Le lemme suivant va permettre de se débarrasser des cas où c admet l'un des facteurs $3, 5, 7$:

1.4 Lemme. *Dans ce qui suit k désigne l'un des entiers* $1, 3, -1, -3$.

1) On a $S_{-k} = -S_k$.

2) On a les équivalences : $c \in S_1 \iff 3c \in S_3 \iff 5c \in S_{-1} \iff 7c \in S_3$, $c \in S_3 \iff 3c \in S_1 \iff 5c \in S_{-3} \iff 7c \in S_1$, et les résultats analogues obtenus en changeant tous les signes des coefficients k.

3) On a les équivalences $c \in S_k \iff 9c \in S_k \iff 25c \in S_k \iff 49c \in S_k$.

Démonstration. Le point 1) est évident. Pour 2) montrons par exemple la première équivalence. Si c est dans S_1 on a $c = x^2 - 105y^2$, donc $3c = 3x^2 - 35(3y)^2$ est dans S_3. Si $3c$ est dans S_3, on a $3c = 3x^2 - 35y^2$. On voit que y est multiple de 3, $y = 3y'$, et on a $c = x^2 - 105y'^2$.

Enfin, le point 3) résulte de 2). Traitons seulement l'un des cas, les autres sont analogues. Si c est, disons, dans S_1, il est clair que $9c$ y est aussi. Inversement, si $9c$ est dans S_1, $3c$ est dans S_3 par 2), donc c dans S_1.

2 Minkowski et ses applications

Comme beaucoup de problèmes d'arithmétique, celui-ci peut être résolu grâce au théorème de Minkowski sur les réseaux que nous rappelons maintenant (pour une démonstration, voir [Samuel] ou [Stewart-Tall]).

2.1 Le théorème de Minkowski

2.1 Théorème. *Soit L un sous-réseau de $\mathbf{Z}^2$ de rang 2 et d'aire d. Soit B une partie convexe de $\mathbf{R}^2$ contenant $O = (0,0)$, symétrique par rapport à O et d'aire $\geq 4d$. Alors, B contient un point de L distinct de O.*

2.2 *Remarque.* Ce résultat s'applique notamment en prenant pour B un rectangle [5] $|x| \leq p$, $|y| \leq q$ avec $pq \geq d$.

2.2 Application aux formes quadratiques

2.3 Proposition. *Soient a, b des entiers positifs et soit c un entier, premier avec a ou b. On suppose que ab est un carré modulo c. Alors, il existe des entiers x, y et un entier n, avec $|n| \leq \sqrt{ab}$, vérifiant $ax^2 - by^2 = nc$.*

Démonstration. Quitte à échanger les rôles de a et b et à changer c en $-c$, on peut supposer c premier avec a. Soit k une racine carrée de ab modulo c. On considère l'ensemble :

$$L = \{(x,y) \in \mathbf{Z}^2 \ \mid \ ax \equiv ky \pmod{c}\}.$$

2.4 Lemme. *L'ensemble L est un réseau de $\mathbf{R}^2$, d'aire $|c|$.*

Démonstration. Il est clair que L est un sous-groupe de $\mathbf{Z}^2$, donc discret, donc un sous-réseau. Il est de rang 2 car il contient $(c,0)$ et $(\alpha k, 1)$ (où α désigne un représentant d'un inverse de a modulo c). De plus, ces vecteurs constituent une $\mathbf{Z}$-base de L. En effet, si (x,y) est dans L, on a $ax = ky + \lambda c$, avec $\lambda \in \mathbf{Z}$, donc $a\alpha x = \alpha k y + \alpha\lambda c$ et on a $a\alpha = 1 + \mu c$, avec $\mu \in \mathbf{Z}$, d'où $x = \alpha k y + (\alpha\lambda - x\mu)c$ et $(x,y) = (\alpha\lambda - \mu x)(c,0) + y(\alpha k, 1)$. Comme la matrice de cette base sur la base canonique est $\begin{pmatrix} c & \alpha k \\ 0 & 1 \end{pmatrix}$, l'assertion sur l'aire du réseau s'ensuit.

Si (x,y) est un point de L, on note que $ax^2 - by^2$ est multiple de c. En effet, on a $ax \equiv ky \pmod{c}$, donc $a^2x^2 \equiv k^2y^2 \equiv aby^2 \pmod{c}$ et la conclusion vient du fait que a est premier à c.

5. Attention, l'aire d'un tel rectangle est $4pq$.

On applique alors le théorème de Minkowski au réseau L, avec comme convexe le rectangle $|x| \leq u\sqrt{|c|}$, $|y| \leq u^{-1}\sqrt{|c|}$, où u est un nombre > 0 quelconque. Comme ce rectangle est d'aire $4|c|$, il existe $(x, y) \in L$, différent de $(0, 0)$ dedans. On a ainsi des entiers x, y, vérifiant $|x| \leq u\sqrt{|c|}$, $|y| \leq u^{-1}\sqrt{|c|}$ et $ax^2 - by^2 = nc$ avec $n \in \mathbf{Z}$.

Si on prend $u^2 = \sqrt{b/a}$, on voit qu'on a $|n| \leq \sqrt{ab}$. En effet, on a, si $nc > 0$, $nc = |n|\,|c| = ax^2 - by^2 \leq ax^2 \leq a\sqrt{\dfrac{b}{a}}|c| = \sqrt{ab}\,|c|$, donc $|n| \leq \sqrt{ab}$, et si $nc < 0$, $-nc = |n|\,|c| = by^2 - ax^2 \leq by^2 \leq b\sqrt{\dfrac{a}{b}}\,|c| = \sqrt{ab}\,|c|$ donc $|n| \leq \sqrt{ab}$.

2.5 *Remarque.* On peut appliquer ce résultat aux équations $ax^2 - by^2 = c$ de discriminant 105, pourvu que 105 soit un carré modulo c. Il existe alors un entier n avec $|n| \leq 10$ et des entiers x, y tels que $nc = ax^2 - by^2$.

3 Les carrés de $\mathbf{Z}/c\mathbf{Z}$

On a le résultat suivant :

3.1 Proposition. *Soit c un entier positif écrit sous la forme $c = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les p_i premiers distincts. Soit $d \in \mathbf{Z}$.*

1) L'entier d est un carré modulo c si et seulement si c'est un carré modulo $p_i^{\alpha_i}$ pour tout i.

2) Si p est un nombre premier impair, α un entier positif et si d s'écrit $d = d'p^m$, avec $m < \alpha$, et d' premier à p, d est un carré modulo p^α si et seulement si m est pair et d' est un carré modulo p.

Démonstration. La première assertion vient du lemme chinois, voir par exemple [Perrin] Ch. 1, §6. Pour le point 2), supposons d'abord que d est un carré modulo p^α : $d \equiv (\delta p^k)^2$ avec δ premier avec p. On a donc $d = d'p^m = \delta^2 p^{2k} + \lambda p^\alpha$. On voit que $2k$ est $\geq m$ et s'il était plus grand, p diviserait d', ce qui est exclu. On a donc $m = 2k$. On en déduit $d' \equiv \delta^2$ modulo $p^{\alpha-m}$, donc aussi modulo p puisque m est $< \alpha$.

Inversement, si d' est un carré modulo p c'est aussi un carré modulo p^α. En effet, on sait (voir [Perrin] Ch. 1, §7) qu'on a un isomorphisme $(\mathbf{Z}/p^\alpha\mathbf{Z})^* \simeq \mathbf{Z}/p^{\alpha-1}\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^*$ et l'image d'un élément $\overline{a}$ dans le second facteur est sa classe modulo p. Comme le groupe cyclique $\mathbf{Z}/p^{\alpha-1}$ est d'ordre impair, ses éléments sont tous des doubles (donc des carrés dans le groupe multiplicatif) et on a la condition voulue.

3.2 *Remarque.* Modulo $c = 2^\alpha$ les choses sont moins claires. Les carrés sont $0, 1$ pour $c = 4$; $0, 1, 4$ pour $c = 8$; $0, 1, 4, 9$ pour $c = 16$; $0, 1, 4, 9, 16, 25$ et $-15 \equiv 49$ pour $c = 32$. On a cependant le lemme suivant :

3.3 Lemme. *Un nombre impair d est un carré modulo 2^α pour tout $\alpha > 0$ si et seulement si il est congru à 1 modulo 8.*

Démonstration. Il est clair que la condition est nécessaire. Dans l'autre sens, on raisonne par récurrence sur α que l'on peut supposer ≥ 3. Si d est un carré modulo 2^α il existe x_0 impair tel que $x_0^2 = d + \lambda 2^\alpha$. Si λ est pair, d est un carré modulo $2^{\alpha+1}$ comme souhaité. Sinon, on pose $x = x_0 + 2^{\alpha-1}$ et on a $x^2 = x_0^2 + 2^\alpha x_0 + 2^{2\alpha-2} = d + (\lambda + x_0)2^\alpha + 2^{2\alpha-2}$ et on conclut car λ et x_0 sont impairs et $\alpha \geq 3$.

3.4 Corollaire. *Soit c un entier positif écrit sous la forme $c = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ avec les p_i premiers impairs distincts. L'entier 105 est un carré modulo c si et seulement si l'on a les deux conditions suivantes :*

1) Pour $p_i = 3, 5$ ou 7 on a $\alpha_i = 1$.

2) L'entier c est un carré modulo chacun des p_i différents de $3, 5, 7$.

4 Le cas c premier à $3, 5, 7$

4.1 Les conditions nécessaires de congruence

4.1 Définition. *Une solution (x, y) de l'équation diophantienne $ax^2 - by^2 = c$ avec $a, b, c \in \mathbf{Z}$ est dite* **primitive** *si x et y sont premiers entre eux.*

4.2 Proposition. *Soit k l'un des nombres $1, 3, -1, -3$ et soit q_k la forme de discriminant 105 correspondante. Soit $c \in \mathbf{Z}$ un entier premier avec $3, 5, 7$. On suppose que c est dans S_k. On a les conditions suivantes :*

1) On a les congruences[6] *:*

• *Pour $k = 1$, $c \equiv 1 \pmod 3$, $c \equiv \pm 1 \pmod 5$ et $c \equiv 1, 2, -3 \pmod 7$.*

• *Pour $k = 3$, $c \equiv 1 \pmod 3$, $c \equiv \pm 2 \pmod 5$ et $c \equiv -1, -2, 3 \pmod 7$.*

Pour $k = -1$ et -3 les conditions se déduisent des précédentes en changeant les signes :

• *$k = -1$, $c \equiv -1 \pmod 3$, $c \equiv \pm 1 \pmod 5$ et $c \equiv -1, -2, 3 \pmod 7$,*

• *$k = -3$, $c \equiv -1 \pmod 3$, $c \equiv \pm 2 \pmod 5$ et $c \equiv 1, 2, -3 \pmod 7$.*

2) Le nombre c n'est pas congru à 2 modulo 4.

3) Ou bien 105 est un carré modulo c (condition 3'), ou bien l'équation admet une solution non primitive (et dans ce cas, c admet un facteur carré).

6. On notera que pour avoir la condition de congruence avec l'un des $p = 3, 5, 7$ il suffit que c soit premier avec celui-là.

On note C_k l'ensemble des $c \in \mathbf{Z}$ premiers à $3, 5, 7$ qui vérifient les conditions 1), 2), 3') relatives à k.

Démonstration. Par examen des congruences, on vérifie que si c est dans S_k on a la condition 1) avec ses variantes et la condition 2) dans tous les cas.

Montrons 3) dans le cas $k = 1$, les autres sont analogues. On suppose qu'on a $c = x^2 - 105y^2$. Il y a deux cas. Si y et c sont premiers entre eux, 105 est un carré modulo c (le carré de xy^{-1}). Sinon, si le nombre premier p divise y et c, il divise x^2, donc x, et la solution n'est pas primitive. On note qu'alors p^2 divise c.

4.2 Les conditions suffisantes

4.3 Théorème. *On désigne encore par k l'un des nombres $1, 3, -1, -3$. Si c est un entier premier avec $3, 5$ et 7 et s'il est dans C_k (c'est-à-dire s'il vérifie les conditions ci-dessus), il est dans S_k (donc l'équation $q_k(x, y) = c$ admet une solution).*

Démonstration. Il suffit évidemment de traiter les cas $k = 1$ et $k = 3$. La démonstration se fait en deux temps.

4.2.1 Le cas c impair

On peut appliquer 2.3. Il existe donc n avec $|n| \leq 10$ et des entiers x, y avec $nc = q_k(x, y)$. On note déjà que n est non nul. Considérons l'un des nombres $p = 3, 5$ ou 7. Si n est premier avec p, comme c est dans C_k et nc dans S_k, ces nombres sont en même temps carrés ou non carrés modulo p et n est donc un carré modulo p. En étudiant successivement les cas $p = 3, 5, 7$, cela permet d'éliminer toutes les valeurs de n sauf 1, 4, 9, -5 et -6. La valeur 1 est celle souhaitée. Examinons maintenant les autres. Pour fixer les idées, nous explicitons le raisonnement dans le cas $k = 1$, mais l'autre cas est analogue.

Si n est égal à 9, on a $9c = x^2 - 105y^2$. On voit que x est multiple de 3, donc y aussi et c est de la forme $x^2 - 105y^2$.

Si n est égal à 4, on a $4c = x^2 - 105y^2$, de sorte que x et y ont même parité. Si x et y sont pairs, on peut simplifier par 4 et c est de la forme voulue. S'ils sont impairs, $x = 2x' + 1$ et $y = 2y' + 1$, on a $c = x'^2 + x' - 105(y'^2 + y') - 104$ et on voit que c est pair, ce qui est contraire à l'hypothèse.

Si n vaut -6 on a $-6c = x^2 - 105y^2$, x est multiple de 3, $x = 3x'$ et on a $2c = 35y^2 - 3x'^2$. Comme c est impair, $2c$ est congru à 2 modulo 4 et on sait que c'est impossible.

Enfin, si n vaut -5, on a $-5c = x^2 - 105y^2$, d'où $x = 5x'$ et $c = 21y^2 - 5x'^2$. Mais, on a vu en 1.4 que les formes $x^2 - 105y^2$ et $21x^2 - 5y^2$ sont équivalentes, donc c est bien dans S_1.

4.2.2 Le cas c pair

On pose $c = 2^\alpha c'$ avec c' impair et $\alpha \geq 2$ (en vertu de la condition 2). Il y a deux cas :

• Si α est pair, c' vérifie les conditions 1), 2), 3') donc est dans C_k. C'est clair pour 1) car 2^α est un carré et pour 2) car c' est impair. Pour 3'), posons $c' = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Il s'agit de montrer que 105 est un carré modulo c', donc modulo les p_i, mais cela vient du fait que 105 est un carré modulo c. En vertu du premier cas, on voit que c' est dans S_k, donc aussi $2^\alpha c'$ puisque α est pair.

• Si $\alpha = 2\beta + 1$ est impair, avec $\beta \geq 1$, on vérifie que $2c'$ satisfait les conditions 1) et 3') (mais pas 2), bien entendu). Le résultat 2.1 s'applique et on montre comme ci-dessus que $8c'$ ou $-12c'$ est dans S_k (car $2c'$ n'est pas dans S_k). Si $8c'$ est dans S_k, il en est de même de $2^\alpha c'$ et on a gagné. Il reste donc seulement le cas $-12c' \in S_k$. Il suffit de montrer le lemme suivant :

4.4 Lemme. *Soit c' un entier impair tel que $-12c' \in S_k$. Alors, $8c'$ est aussi dans S_k.*

Démonstration. Traitons d'abord le cas $k = 1$.

On a $-12c' = x^2 - 105y^2$. Il s'ensuit que $x = 3x'$, d'où $4c' = 35y^2 - 3x'^2$. On voit que y et x' ont même parité. S'ils étaient impairs, $y = 2y' + 1$ et $x' = 2x'' + 1$ on aurait $c' = 35(y'^2 + y') - 3(x''^2 + x'') + 32$ et c' serait pair ce qui est absurde. Ils sont donc pairs et c' est de la même forme $c' = 35y^2 - 3x^2$, donc $-3c' = (3x)^2 - 105y^2$ est dans S_1. Changeant de notations, on écrit $-3c' = x^2 - 105y^2 = z\overline{z} = N(z)$ avec $z = x - y\sqrt{105} \in \mathbf{Z}[\sqrt{105}]$, où N désigne la norme dans cet anneau. On introduit alors $w = 3 + \dfrac{\sqrt{105}}{3}$ qui est de norme $-8/3$. On a donc $N(zw) = 8c'$. On a gagné si on prouve que zw est dans $\mathbf{Z}[\sqrt{105}]$. On a $zw = 3x - 35y + \left(\frac{x}{3} - 3y\right)\sqrt{105}$ et on conclut car x est multiple de 3.

Passons au cas $k = 3$. Le début est analogue et on se ramène à montrer que si $-3c'$ est de la forme $3x^2 - 35y^2$ il en est de même de $8c'$. On note qu'un entier est de la forme $3x^2 - 35y^2$ si et seulement si il s'écrit $\frac{1}{3}N(3x - \sqrt{105}y) := \frac{1}{3}N(z)$ avec $x, y \in \mathbf{Z}$. L'entier $-3c'$ a donc une telle écriture, avec, de plus, y multiple de 3. On en déduit, avec les notations du cas précédent, $8c' = \frac{1}{3}N(zw)$. Mais on a $zw = 9x - 35y + (x - 3y)\sqrt{105}$ et la conclusion vient du fait que y est multiple de 3.

5 Le cas général

5.1 Pour une forme quelconque

5.1 Proposition. *Soit $c \in \mathbf{Z}$ et k l'un des entiers $1, 3, -1, -3$. On écrit $c = 3^\alpha 5^\beta 7^\gamma c'$ avec $\alpha, \beta, \gamma \geq 0$ et c' premier à $3, 5, 7$. On pose $\alpha = 2u + \alpha'$, $\beta = 2v + \beta'$ et $\gamma = 2w + \gamma'$ avec $u, v, w \in \mathbf{N}$ et $\alpha', \beta', \gamma' = 0$ ou 1. Alors c est dans S_k si et seulement si $3^{\alpha'} 5^{\beta'} 7^{\gamma'} c'$ est dans S_k.*

Démonstration. Cela résulte de 1.4.

5.2 Le cas $k = 3$

La proposition 5.1, jointe au lemme 1.4 et au théorème 4.3, permet de répondre à la question : un entier c donné est-il, ou non, dans S_k. La mise en œuvre pratique peut être un peu fastidieuse, aussi le faisons-nous seulement pour le problème initial :

5.2 Corollaire. *Soit $c \in \mathbf{Z}$. On écrit $c = 3^\alpha 5^\beta 7^\gamma c'$ avec $\alpha, \beta, \gamma \geq 0$ et c' premier à $3, 5, 7$. On pose $\alpha = 2u + \alpha'$, $\beta = 2v + \beta'$ et $\gamma = 2w + \gamma'$ avec $u, v, w \in \mathbf{N}$ et $\alpha', \beta', \gamma' = 0$ ou 1. Alors c est dans S_3 si et seulement si l'une des conditions données par le tableau suivant est réalisée :*

α'	0	1	1	0	0	1	1	0
β'	0	1	0	1	0	1	0	1
γ'	0	1	0	0	1	0	1	1
condition	$c' \in C_3$	$c' \in C_{-3}$	$c' \in C_1$	$c' \in C_{-3}$	$c' \in C_1$	$c' \in C_{-1}$	$c' \in C_3$	$c' \in C_{-1}$

Démonstration. Cela résulte de ce qui précède. Supposons, par exemple, que l'on a $\alpha' = \beta' = 1$ et $\gamma' = 0$. La proposition 5.1 montre que c est dans S_k si et seulement si $15c'$ y est. En vertu de 1.4 , cela signifie que $5c'$ est dans S_1, donc que $-c'$ est dans S_1. Comme c' est premier avec $3, 5, 7$, c'est équivalent à $-c' \in C_1$ en vertu de 4.3. C'est bien ce qui est annoncé.

5.3 Compléments sur S_3

Dans ce paragraphe on supposera connus les résultats essentiels sur les carrés modulo p où p est un nombre premier (symbole de Legendre, loi de réciprocité quadratique, etc., voir par exemple [Serre]).

5.3.1 Les petites valeurs de S_3

Les c avec $1 \leq c \leq 100$ donnés par le corollaire précédent sont les suivants :

3	7	12	13	27	28	40	48	52	63	73	75	97

On notera que pour $27, 63$ et 75, les nombres doivent être débarrassés de leurs puissances paires de $3, 5, 7$ avant d'utiliser le tableau des conditions. On vérifie que les treize nombres ci-dessus sont bien dans S_3.

5.3.2 Les nombres premiers de S_3

Si $c = p$ est un nombre premier impair qui est dans C_3, c'est-à-dire congru à 1 modulo 3, à ± 2 modulo 5 et à $-1, -2$ ou 3 modulo 7, la condition sur 105 est automatique. En effet, on a, en vertu de la loi de réciprocité quadratique, la relation suivante sur les symboles de Legendre $\left(\frac{105}{p}\right) = \left(\frac{3}{p}\right) \times \left(\frac{5}{p}\right) \times \left(\frac{7}{p}\right) = \left(\frac{p}{3}\right) \times \left(\frac{p}{5}\right) \times \left(\frac{p}{7}\right)$ (distinguer selon les congruences de p modulo 4) et les trois symboles valent respectivement $1, -1, -1$. Dans ce cas, le résultat est confirmé par l'expérience comme le montre le tableau suivant où l'on a pris pour c les plus petits nombres premiers vérifiant les congruences prescrites. Attention, même pour un nombre premier c, la condition 105 est un carré modulo c ne suffit pas à assurer que c est dans S_3 comme le montre l'exemple de $c = 23$ ($105 \equiv 13 \equiv 36 \pmod{23}$ est un carré) mais 23 étant congru à -1 modulo 3 n'est pas de la forme voulue.

congruences modulo 3, 5, 7	nombre premier c	solutions
$1, 2, -1$	97	$x = 18$, $y = 5$
$1, 2, -2$	397	$x = 12$, $y = 1$
$1, 2, 3$	157	$x = 8$, $y = 1$
$1, -2, -1$	13	$x = 4$, $y = 1$
$1, -2, -2$	103	$x = 9$, $y = 2$
$1, -2, 3$	73	$x = 6$, $y = 1$

5.3.3 Les nombres de S_3 impairs, premiers à $3, 5, 7$ et sans facteurs carrés

On s'intéresse ici aux nombres c de la forme $c = p_1 \cdots p_r$ avec des p_i premiers distincts et différents de $2, 3, 5, 7$. Appelons **propres** ces nombres.

Si c est un tel nombre, on peut lui associer le triplet de ses symboles de Legendre $\left(\left(\frac{c}{3}\right), \left(\frac{c}{5}\right), \left(\frac{c}{7}\right)\right)$, qui indique si c est ou non, un carré modulo $3, 5, 7$, ou simplement le triplet des signes $(\epsilon_3, \epsilon_5, \epsilon_7)$ de ces symboles, qu'on appellera **signe** de c, et qui réside dans $\{\pm\}^3$. Ainsi, le nombre premier 11 est de signe $-, +, +$, tandis que 13 est de signe $+, -, -$. Les nombres premiers qui sont dans S_3 sont exactement ceux de signe $+, -, -$ en vertu de 1.4. et 5.2. Pour les nombres propres, la condition que le signe soit $+, -, -$ est encore nécessaire en vertu de 4.2, mais plus suffisante. Cette condition signifie que le nombre des ϵ_3 (resp. ϵ_5 ou ϵ_7) égaux à -1 parmi les facteurs p_i de c est pair (resp. impair).

Le théorème 4.3 indique que c est dans S_3 si, outre la condition précédente, le nombre 105 est un carré modulo c, donc s'il l'est modulo chaque p_i. Comme on l'a vu ci-dessus, cela signifie que, pour $p = p_i$, le symbole de Legendre $\left(\frac{p}{3}\right) \times \left(\frac{p}{5}\right) \times \left(\frac{p}{7}\right)$ est égal à 1, donc que chaque p_i est de signe $(+, +, +)$ ou $(+, -, -)$ ou $(-, +, -)$ ou $(-, -, +)$.

Cela permet de montrer (par exemple) le résultat suivant :

5.3 Proposition. *Soient p, q des nombres premiers distincts (et toujours différents de $2, 3, 5, 7$). Le produit $c = pq$ est dans S_3 si et seulement si les nombres p, q sont de signes $(+, +, +)$ et $(+, -, -)$ (dans ce cas q est dans S_3 mais pas p) ou $(-, +, -)$ et $(-, -, +)$ (dans ce cas aucun n'est dans S_3), ou les signes obtenus en échangeant p et q.*

5.4 *Exemple.* Un exemple du premier type est $109 \times 13 = 1417 = 3.22^2 - 35$, un exemple du second type $41 \times 53 = 2173 = 3 \times 36^2 - 35 \times 7^2$. Cet exemple montre que S_3 (contrairement à S_1) n'est pas stable par multiplication. En effet, le produit 1417×2173 n'est pas dans S_3 (il est congru à 1 modulo 5).

5.3.4 Les facteurs carrés

Il est clair que si c est dans S_3 et si m est un entier, $m^2 c$ est aussi dans S_3. La réciproque est fausse avec $m = 2$, par exemple $40 = 4 \times 10$ est dans S_3 mais pas 10, ou, si on veut un exemple sans $3, 5, 7$, $c = 4c'$ avec $c' = 2 \times 41$ est dans S_3 : $c = 328 = 3 \times 11^2 - 35$, mais pas c' à cause de la congruence modulo 4. En revanche on a le résultat suivant :

5.5 Proposition. *Soit m un nombre impair. Si $m^2 c$ est dans S_3, c aussi.*

Démonstration. Il suffit de traiter le cas où $m = p$ est premier. Pour $p = 3, 5, 7$ c'est 1.4. Si p est différent de $3, 5, 7$, on se ramène à montrer que $p^2c \in C_k \Longrightarrow c \in C_k$. C'est évident pour les conditions de congruence modulo $4, 3, 5, 7$ et pour le fait que 105 soit un carré cela résulte de 3.1.

5.6 *Remarque.* Toujours à propos des facteurs carrés, si c est dans S_3, on a vu que m^2c y est aussi, mais, *a priori*, avec une solution imprimitive. Lorsque m et c sont des entiers tels que les équations $E_3(c)$ et $E_3(m)$ admettent des solutions primitives on peut espérer que $E_3(m^2c)$ admette aussi des solutions primitives, grâce au procédé suivant.

On note que $3x^2 - 35y^2 = c$ équivaut à $\frac{c}{3} = x^2 - 105(\frac{y}{3})^2 = N(x + \frac{y\sqrt{105}}{3})$. Si on a ainsi $N(z) = \frac{m}{3}$ et $N(w) = \frac{c}{3}$, on en déduit $N(3z^2w) = \frac{m^2c}{3}$. On peut expliciter les formules. On part de $m = 3a^2 - 35b^2$ et de $c = 3a'^2 - 35b'^2$ avec a, b (resp. a', b') premiers entre eux. On en déduit $m^2c = 3X^2 - 35Y^2$ avec $X = (3a^2 + 35b^2)a' + 70abb'$ et $Y = (3a^2 + 35b^2)b' + 6aba'$ et il reste à voir si X, Y sont premiers entre eux. Ce n'est pas toujours vrai (prendre par exemple a multiple de 5), mais ça doit l'être souvent [7] (noter qu'on a $b'X - a'Y = 2ab(35b'^2 - 3a'^2)$ et $3a'X - 35b'Y = (3a^2 + 35b^2)(3a'^2 - 35b'^2)$).

Ainsi, partant des décompositions $13 = 3 \times 4^2 - 35 \times 1^2$ et $73 = 3 \times 6^2 - 35 \times 1^2$ on trouve $73 \times 13^2 = 12337 = 3 \times 778^2 - 35 \times 227^2$.

5.3.5 Le principe de Hasse

Si l'équation $3x^2 - 35y^2 = c$ admet une solution entière, il est clair que, pour tout $n \in \mathbf{N}^*$, l'équation de congruence $3x^2 - 35y^2 \equiv c \pmod{n}$ admet une solution. La question est la réciproque : si l'équation de congruence est satisfaite pour tout n, l'équation initiale admet-elle une solution ? Telle quelle, la réponse est négative. En effet, si on considère le nombre $c = 31 \times 37 = 1147$, il n'est pas dans S_3 (105 n'est pas un carré modulo c), mais les équations de congruences sont toutes vérifiées. Cela vient du lemme suivant :

5.7 Lemme. *1) L'équation $3x^2 - 35y^2 = 1147$ admet une solution modulo p pour tout p premier impair.*

2) Elle admet une solution modulo $2, 4, 8$.

3) Elle admet une solution modulo p^α pour tout p premier et tout α positif.

4) Elle admet une solution modulo n pour tout n.

Démonstration. 1) Il faut distinguer les cas $p = 3, 5, 7$. Dans ce cas, le résultat vient du fait que 1147 est bien de signe $+, -, -$. Pour les autres cas, c'est un résultat classique : on compte les carrés de $\mathbf{F}_p$, voir par exemple [Perrin] Ch. V, lemme 6.10.

7. Le lecteur se penchera sur cette intéressante question.

2) Il suffit d'examiner les trois cas.

3) C'est le lemme de Hensel, voir [Serre] Ch. II, cor. 2 et 3. L'idée est simple, expliquons juste le passage de p à p^2 dans le cas impair. On dispose d'une solution (x_0, y_0) de l'équation modulo p, avec, disons, $3x_0$ premier à p. On a donc $3x_0^2 - 35y_0^2 = 1147 + \lambda p$ et on cherche une solution modulo p^2 sous la forme $x = x_0 + hp$, $y = y_0$. On a à résoudre en h l'équation $\lambda + 6x_0h \equiv 0 \pmod{p}$ et c'est possible car $6x_0$ est premier à p.

4) C'est le lemme chinois.

En fait, voir la preuve de 5.9, le problème vient du fait que la congruence $3x^2 \equiv 35y^2 \pmod{p}$ ne permet d'affirmer que 105 est un carré modulo p que si x ou y est non nul dans $\mathbf{Z}/p\mathbf{Z}$. C'est ce qui nous conduit à la définition suivante :

5.8 Définition. *Soit $q(x, y)$ une forme quadratique sur un anneau A et soit $c \in A$. On dit que q* **représente** *c s'il existe $x, y \in A$* **non tous deux nuls** [8] *tels que $q(x, y) = c$.*

Mais, attention, il n'est pas vrai que si l'équation $3x^2 - 35y^2 = c$ admet une solution entière la forme $3x^2 - 35y^2$ représente c dans $\mathbf{Z}/n\mathbf{Z}$ pour tout n. Voici un contre-exemple. On prend $c = 3 \times 11^2$, il est clair que l'équation a une solution ($x = 11$, $y = 0$), mais la forme ne représente pas $c \equiv 0$ (au sens fort) modulo 11. En effet, on aurait $3x^2 - 35y^2 \equiv 0 \pmod{11}$ avec x ou y non nul et cela implique que 105 est un carré modulo 11, ce qui n'est pas le cas. Cette fois, c'est le facteur carré de c qui est en cause.

Une dernière remarque : si c est, par exemple, multiple de 3, la condition de congruence $3x^2 - 35y^2 \equiv c \pmod{3}$ n'apporte aucune information (même avec la restriction x, y non tous deux nuls modulo 3 car on peut prendre $x \neq 0$ et $y = 0$).

Toutes ces remarques expliquent la minceur du résultat suivant :

5.9 Théorème. (Principe de Hasse) *Soit $c \in \mathbf{Z}$ un entier premier avec $3, 5, 7$ et sans facteur carré impair. Les conditions suivantes sont équivalentes :*

1) L'équation $3x^2 - 35y^2 = c$ admet une solution entière.

2) L'équation $3x^2 - 35y^2 \equiv c \pmod{4}$ a une solution et, pour tout nombre premier p impair, la forme $3x^2 - 35y^2$ représente c dans $\mathbf{Z}/p\mathbf{Z}$.

5.10 *Remarque.* La condition sur les facteurs carrés impairs est innocente en vertu de 5.5. En revanche l'autre ne l'est pas, mais en utilisant les notations et la méthode de 5.2, on pourrait avoir un théorème analogue pour chaque cas de α', β', γ', en changeant d'équation.

8. Cette condition n'a d'intérêt que si c est nul.

Démonstration. Montrons que 1) implique 2). La condition sur la congruence modulo 4 est évidente. Pour l'autre, on a une solution de $3x^2 - 35y^2 = c$ que l'on réduit modulo p. Le seul cas à considérer est celui où p divise c. Dans ce cas, il faut voir que x et y ne sont pas tous deux multiples de p, mais sinon c admettrait le facteur p^2.

Montrons que 2) implique 1). On applique 5.2 et il suffit de montrer que les conditions 1), 2), 3') de 4.2 sont remplies. C'est évident pour 1) (car c est premier à $3, 5, 7$) et 2). Il reste à montrer que 105 est un carré modulo c, donc modulo les facteurs premiers impairs p de c. Par hypothèse, il existe des entiers x, y non tous deux multiples de p tels que $3x^2 - 35y^2 \equiv 0 \pmod{p}$, ce qui montre que 105 est un carré modulo p.

6 Calcul des solutions

Dans ce paragraphe, nous donnons, sur l'exemple de l'équation $3x^2 - 35y^2 = c$, en supposant qu'elle admet des solutions, des indications sur le nombre de solutions et une méthode pour les calculer. On commence par quelques rappels sur l'anneau $\mathbf{Z}[\sqrt{105}]$.

6.1 Rappels sur l'anneau $A := \mathbf{Z}[\sqrt{105}]$

Rappelons qu'il s'agit de l'ensemble des nombres réels de la forme $z = a+b\sqrt{105}$ avec $a, b \in \mathbf{Z}$. On dispose dans cet anneau d'un automorphisme qui à z associe $\overline{z} = a - b\sqrt{105}$ et de la norme $N(z) = z\,\overline{z} = a^2 - 105b^2$. Comme $z \mapsto \overline{z}$ est un automorphisme, la norme est multiplicative. Les éléments inversibles de l'anneau sont ceux dont la norme vaut ± 1. Un exemple d'élément inversible est $u = 41 + 4\sqrt{105}$ et on trouve une infinité de tels éléments en prenant les $\pm u^n$ pour $n \in \mathbf{Z}$. On montre d'ailleurs que ce sont les seuls.

6.2 Infinitude

Le premier point porte sur le nombre de solutions de l'équation :

6.1 Proposition. *On suppose que l'équation* $(*)$ *:* $3x^2 - 35y^2 = c$ *admet une solution. Alors, elle en a une infinité.*

Démonstration. Partons de la solution (x, y) de $3x^2 - 35y^2 = c$.Cette relation s'écrit $x^2 - 105\big(\frac{y}{3}\big)^2 = \frac{c}{3}$. Si l'on pose $z = x + \frac{y}{3}\sqrt{105}$, on a, dans A, $\frac{c}{3} = N(z)$. Soit $w = a + b\sqrt{105}$ un élément inversible de A. On a encore $N(wz) = \frac{c}{3}$.

On calcule wz :

$$wz = ax + \frac{105by}{3} + (bx + \frac{ay}{3})\sqrt{105} := X + \frac{Y}{3}\sqrt{105}$$

où $X = ax + 35by$ et $Y = 3bx + ay$ sont dans $\mathbf{Z}$. On a donc $N(wz) = X^2 - \frac{105}{9}Y^2 = X^2 - \frac{35}{3}Y^2 = \frac{c}{3}$ et donc $3X^2 - 35Y^2 = c$. En faisant varier w dans A^*, on obtient une infinité de solutions distinctes de $(*)$. En effet, si (X, Y) et (X', Y') sont les solutions correspondant à $w, w' \in A^*$, on voit qu'elles ne sont égales que si $w = w'$.

Au passage on a prouvé le lemme suivant :

6.2 Lemme. *Si (x, y) est une solution de $(*)$ et (a, b) une solution de $(**)$: $a^2 - 105b^2 = 1$, alors $X = ax + 35by$, $Y = 3bx + ay$ est solution de $(*)$.*

En particulier, avec $a = -41$ et $b = 4$, on voit que $X = -41x + 140y$, $Y = 12x - 41y$ est solution.

6.3 Calcul des solutions

Le théorème suivant donne montre l'existence de "petites" solutions de l'équation $(*)$:

6.3 Théorème. *Soit $c \in \mathbf{N}$. Si l'équation $(*)$: $3x^2 - 35y^2 = c$ admet des solutions, elle admet une solution X, Y vérifiant $X \leq \sqrt{7c}$ et $Y \leq \sqrt{\frac{4c}{7}}$.*

Démonstration. On note d'abord que, si X, Y est solution de $(*)$, on a $3X^2 = 35Y^2 + c$, de sorte que si Y vérifie la condition de taille, X aussi.

On prouve alors le théorème par l'absurde. Supposons que $(*)$ n'admette pas de solution avec $y \leq \sqrt{\frac{4c}{7}}$. Soit (x, y) la solution de $(*)$ avec $y \in \mathbf{N}$ minimum (y est donc plus grand que $\sqrt{\frac{4c}{7}}$) et posons $X = -41x + 140y$ et $Y = 12x - 41y$. On a vu que (X, Y) est encore une solution de $(*)$. Si l'on montre qu'on a $-y < Y < y$ on aura une contradiction avec la minimalité de y. Or, cette inégalité est équivalente à $\frac{10}{3} < \frac{x}{y} < \frac{7}{2}$ ou encore à $\frac{100}{9} < \frac{x^2}{y^2} < \frac{49}{4}$. L'équation $3x^2 - 35y^2 = c$ donne $\frac{x^2}{y^2} = \frac{35}{3} + \frac{c}{3y^2}$. On voit que l'inégalité de gauche est toujours vérifiée et celle de droite équivaut à $y^2 > \frac{4c}{7}$. Mais cette condition est réalisée par hypothèse et on a le résultat.

6.4 *Exemple.* Le nombre $c = 125887$ est premier et vérifie les conditions de congruences (il est congru à 1 modulo 3, 2 modulo 5 et -1 modulo 7). L'équation correspondante admet donc une solution X, Y avec $X \leq 938$ et $Y \leq 268$. Il suffit d'écrire quelques lignes d'un programme rudimentaire pour la trouver. Voici le programme sur *xcas* :

```
D4(a,b,c,M,N):={
local x,y;
pour x de 0 jusque M faire
pour y de 0 jusque N faire
si a*x^2-b*y^2==c alors
Disp x,y;
fsi
fpour
fpour
}:;
```

Avec $a = 3$, $b = 35$, $c = 125887$, $M = 938$ et $N = 268$ on trouve $X = 347$, $Y = 82$.

7 Références

[ME] **PERRIN Daniel**, *Mathématiques d'École*, Cassini, 2005.

[Perrin] **PERRIN Daniel**, *Cours d'algèbre*, Ellipses, 1996.

[Samuel] **SAMUEL Pierre**, *Théorie algébrique des nombres*, Hermann, 1967.

[Serre] **SERRE Jean-Pierre** *Cours d'arithmétique*, PUF, 1970.

[Stewart-Tall] **STEWART Ian & TALL David**, *Algebraic Number Theory*, Chapmann & Hall, 1979.