Équations diophantiennes

Samuel Rochetin

Mercredi 21 février 2018

Résumé

Seules les équations diophantiennes linéaires de la forme $ax + by = c$ sont présentées dans le cours de Terminale S, spécialité mathématiques. Sortis de ce cadre, les lycéens sont démunis. Le but de ce document est de présenter quelques méthodes de résolution d'équations diophantiennes élémentaires et classiques. Les solutions proposées se concentrent sur les techniques arithmétiques propres à chaque exercice donc certains détails de calcul sont laissés au lecteur.

1 Méthodes élémentaires

1.1 Encadrement

Exercice 1. *Résoudre* $3x^2 + 2y^2 = 30$*, où* $(x, y) \in \mathbb{N}^2$.

Solution. Le membre de gauche croît rapidement avec x et y donc il ne peut pas y avoir beaucoup de solutions. Nous encadrons une des variables pour limiter le nombre de possibilités et procéder par élimination. $2y^2 = 3\left(10 - x^2\right) \geq 0 \implies 0 \leq x \leq 3$. L'unique solution est donc $(2; 3)$. □

1.2 Divisibilité

Exercice 2. *Résoudre* $5x^2 - 7xy = 17$*, où* $(x, y) \in \mathbb{N}^2$.

Solution. $x(5x - 7y) = 17$ donc $x \mid 17$ donc $x = 1$ ou $x = 17$. L'unique solution est donc $(17; 12)$. □

Exercice 3. *Résoudre* $9x^2 - y^2 = 36$*, où* $(x, y) \in \mathbb{N}^2$.

Solution. $9x^2 - y^2 = (3x - y)(3x + y)$. Nous cherchons donc les paires de diviseurs associés de 36. Nous avons $36 = 1 \times 36 = 2 \times 18 = 3 \times 12 = 4 \times 9 = 6 \times 6$. Puisque $3x + y \geq 3x - y$, nous obtenons cinq systèmes de deux équations à deux inconnues, parmi lesquels un seul est résoluble dans $\mathbb{N}^2$. L'unique solution est donc $(2; 0)$. □

Exercice 4. *Résoudre* $x + y = xy$*, où* $(x, y) \in \mathbb{N}^2$.

Solution. Si $x = 0$, alors $y = 0$. Si $x = 1$, alors l'équation n'admet aucune solution. Si $x > 1$, alors $x + y = xy \iff x = y(x-1)$. Méthode n°1 : $x - 1$ divise x et $x - 1$ divise $x - 1$ donc $x - 1$ divise $x - (x - 1) = 1$. Or, $x - 1 > 0$, donc $x - 1 = 1 \iff x = 2 \implies y = 2$. Méthode n°2 : $x > 1 \implies y \mid x$. Nous avons $x > 1 \implies y > 1$ donc par symétrie du problème en x et y, nous avons $x \mid y$. Or, $(x, y) \in \mathbb{N}^2$ donc $x = y$, ce qui donne la solution $(2; 2)$. Les deux solutions sont donc $(0; 0)$ et $(2; 2)$. □

Exercice 5. *Résoudre* $\dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} = 1$, *où* $(x, y, z) \in (\mathbb{N}^*)^3$.

Solution. En multipliant par xyz, l'équation est équivalente à $xy + yz + zx = xyz$. Par symétrie du problème en x, y et z, nous pouvons supposer $x \leq y \leq z$. Si $x = 1$, alors $y + z = 0$. Impossible car $y > 0$ et $z > 0$. Si $x = 2$, alors $2y = (y - 2)z$. Donc $y - 2 \mid 2y$. Or, $y - 2 \mid y - 2$ donc $y - 2 \mid 2y - 2 \times (y - 2) = 4$. Or, $2 = x \leq y$ donc $y - 2 \geq 0$ donc $y - 2 \in \{1; 2; 4\} \iff y \in \{3; 4; 6\}$. Nous avons $y > 2$ et $z \geq y$ donc $\dfrac{2y}{y-2} \geq y \iff y \leq 4$. Donc $y = 3$ ou $y = 4$. Si $y = 3$, alors $(2; 3; 6)$ est l'unique solution. Si $y = 4$, alors $(2; 4; 4)$ est l'unique solution. Si $x = 3$, alors $3(y + z) = 2yz$. Donc $3 \mid 2yz$. Or, 3 est premier à 2 donc d'après le théorème de Gauss, $3 \mid yz$. Or, 3 est premier donc d'après le lemme d'Euclide, $3 \mid y$ ou $3 \mid z$. Si $3 \mid y$, alors il existe un entier $k \geq 1, y = 3k$ donc $3k = (2k - 1)z$. Or, $3 = x \leq z$ donc $3(2k - 1) \leq 3k \iff k \leq 1$ donc $k = 1$ donc $(3; 3; 3)$ est l'unique solution. Si $3 \mid z$, nous obtenons la même solution. Si $x \geq 4$, nous avons $4 \leq x \leq y \leq z$ donc $\dfrac{1}{x} + \dfrac{1}{y} + \dfrac{1}{z} \leq \dfrac{3}{4} < 1$ donc l'équation n'admet aucune solution. Les solutions (x, y, z) vérifiant $x \leq y \leq z$ sont donc $(2; 3; 6), (2; 4; 4)$ et $(3; 3; 3)$. □

1.3 PGCD

Exercice 6. *Résoudre* $x^2 = y^3$, *où* $(x, y) \in \mathbb{N}^2$.

Solution. $(0; 0)$ est solution évidente. Remarquons que $x = 0 \iff y = 0$. Soit (x, y) une solution telle que $xy \neq 0$. Posons $d := \mathrm{PGCD}(x, y)$. Il existe $(x', y') \in \mathbb{N}^2$ tels que $x = dx', y = dy'$ et x', y' premiers entre eux. Il vient $x'^2 = \left(dy'^2\right) \times y'$ donc $y' \mid x'^2 = x' \times x'$. Or, y' est premier à x', donc d'après le théorème de Gauss, $y' \mid x'$. Or, $y' \mid y'$. Donc $y' \mid \mathrm{PGCD}(x', y') = 1$. Donc $y' = 1$. Donc $y = d$ et $x'^2 = d$. Donc $(x, y) = \left(x'^3, x'^2\right)$. Autrement dit, x et y sont respectivement le cube et le carré d'un même entier. La réciproque est évidente car pour tout $x' \in \mathbb{N}$, $\left(x'^3\right)^2 = \left(x'^2\right)^3$. Les solutions sont donc $\left(n^3, n^2\right)_{n \in \mathbb{N}}$. Remarquons qu'on peut aussi obtenir le résultat en examinant simplement les puissances des facteurs premiers de x et y. □

Exercice 7. *Résoudre* $x^2y^2 = 25^3$ *puis* $x^2y^2 = 2018^3$, *où* $(x, y) \in \mathbb{N}^2$.

Solution. Posons $X := xy, Y := 25$. Nous avons $X^2 = Y^3$ donc d'après l'exercice précédent, X et Y sont respectivement le cube et le carré d'un même entier. Or, $Y = 5^2$. Donc $xy = 5^3$, ce qui se résout aisément. En revanche, 2018 n'est pas un carré, donc l'équation $x^2y^2 = 2018^3$ n'admet aucune solution. □

Exercice 8. *Résoudre* $2x^2 + 3y^2 = 5z^2$*, où* $(x, y, z) \in \mathbb{Z}^3$.

Solution. Si $z = 0$, alors $2x^2 + 3y^2 = 0$. Ceci n'est vrai que si $x = y = 0$. Donc $(0; 0; 0)$ est solution et par contraposée, si $(x, y, z) \neq (0; 0; 0)$, alors $z \neq 0$. Soit $(x, y, z) \neq (0; 0; 0)$ une solution. Posons $x' := \frac{x}{z}, y' := \frac{y}{z}$. Alors $(x', y') \in \mathbb{Q}^2$ est solution de $2x'^2 + 3y'^2 = 5$. Cherchons les solutions rationnelles de $\square$

1.4 Congruences

Exercice 9. *Résoudre* $17x^2 - 13y^2 = 5$*, où* $(x, y) \in \mathbb{N}^2$.

Solution. Réduisons l'équation modulo 13 pour éliminer le terme en y^2. Il vient $(2x)^2 \equiv 5 \pmod{13}$. Or, un tableau de congruence montre que les carrés modulo 13 sont $0, 1, 3, 4, 9, 10$ et 12. En particulier, 5 n'est pas un carré modulo 13. Donc l'équation n'admet aucune solution. $\square$

Exercice 10. *Résoudre* $x^2 - 3y^2 = 10$*, où* $(x, y) \in \mathbb{Z}^2$.

Solution. La méthode précédente ne fonctionne pas. Réduisons l'équation modulo 10. Un tableau de congruences montre que l'équation $x^2 - 3y^2 \equiv 0 \pmod{10}$ n'est vraie que si $x \equiv 0 \pmod{10}$ et $y \equiv 0 \pmod{10}$ ou $x \equiv 5 \pmod{10}$ et $y \equiv 5 \pmod{10}$. Dans les deux cas, x et y sont multiples de 5 donc $25 \mid x^2 - 3y^2$. Impossible car $25 \nmid 10$. Donc l'équation n'admet aucune solution. $\square$

Exercice 11. *Résoudre* $3^x - y^2 = 8$*, où* $(x, y) \in \mathbb{N}^2$.

Solution. 3^x est impair donc y^2 est impair donc y est impair donc $y^2 \equiv 1 \pmod 8$. Or, si x est pair, $3^x \equiv 1 \pmod 8$ et si x est impair, $3^x \equiv 3 \pmod 8$. Puisque $3^x - y^2 \equiv 0 \pmod 8$, nous avons x pair. Posons $x := 2x'$. Nous reconnaissons une identité remarquable : $3^x - y^2 = \left(3^{x'}\right)^2 - y^2 = \left(3^{x'} - y\right)\left(3^{x'} + y\right)$. Donc $3^{x'} + y \mid 8 \implies 3^{x'} + y \leq 8 \implies 3^{x'} \leq 8 - y \leq 8$ car $y \geq 0$. Donc $x' = 0$ ou $x' = 1$. L'unique solution est donc $(2; 1)$. $\square$

1.5 Descente infinie

Exercice 12. *Résoudre* $x^3 + 2y^3 = 4z^3$*, où* $(x, y, z) \in \mathbb{Z}^3$.

Solution. $(0; 0; 0)$ est solution évidente. Soit $(x, y, z) \neq (0; 0; 0)$ une solution. $x^3 = 2\left(2z^3 - y^3\right)$ donc x^3 est pair donc x est pair. Posons $x := 2x'$. Alors $y^3 = 2\left(z^3 - 2x'^3\right)$ donc y^3 est pair donc y est pair. Posons $y := 2y'$. Alors $z^3 = 2\left(x' + 2y'\right)$ donc z^3 est pair donc z est pair. Posons $z := 2z'$. Alors $x'^3 + 2y'^3 = 4z'^3$. Ainsi, si $(x, y, z) \neq (0; 0; 0)$ est solution, alors $\left(\frac{x}{2}, \frac{y}{2}, \frac{z}{2}\right) \neq (0; 0; 0)$ est solution. Nous pouvons répéter ce processus indéfiniment. Or, $(x, y, z) \neq (0; 0; 0) \iff x \neq 0$ ou $y \neq 0$ ou $z \neq 0$. Nous avons donc au moins une suite d'entiers naturels strictement décroissante. Impossible. Donc l'unique solution est $(0; 0; 0)$. $\square$

Exercice 13. *Résoudre* $x^2 + y^2 = 7z^2$*, où* $(x, y, z) \in \mathbb{Z}^3$.

Solution. Le triplet $(0;0;0)$ est solution évidente. Supposons qu'il existe une solution $(x,y,z) \neq (0;0;0)$. Nous avons $x^2+y^2 \equiv 0 \pmod 7$. En examinant x^2+y^2 modulo 7, nous avons nécessairement $x \equiv 0 \pmod 7$ et $y \equiv 0 \pmod 7$. Donc x et y sont des multiples de 7. Posons $x := 7x'$ et $y := 7y'$. Il vient $z^2 = 7\left(x'^2+y'^2\right)$, donc $z^2 \equiv 0 \pmod 7$ donc $z \equiv 0 \pmod 7$. Posons $z := 7z'$. Ainsi, si $(x,y,z) \neq (0;0;0)$ est solution, alors $\left(\frac{x}{7},\frac{y}{7},\frac{z}{7}\right) \neq (0;0;0)$ est solution. Nous pouvons répéter ce processus indéfiniment. Or, $(x,y,z) \neq (0;0;0) \iff x \neq 0$ ou $y \neq 0$ ou $z \neq 0$. Nous avons donc au moins une suite d'entiers naturels strictement décroissante. Impossible. Donc l'unique solution est $(0;0;0)$. $\square$

1.6 Somme de deux carrés

Exercice 14. *Résoudre* $x^2+4y^2 = 8633$, *où* $(x,y) \in \mathbb{N}^2$.

Solution. La méthode d'encadrement peut s'appliquer mais le nombre de cas à étudier est élevé. Nous remarquons que $x^2+4y^2 = x^2+(2y)^2$. Montrons que l'ensemble des sommes de deux carrés est stable par produit. Soient a,b,c,d quatre entiers naturels. Posons $z := \pm a \pm ib$ et $z' := \pm c \pm id$. Nous avons $\left(a^2+b^2\right)\left(c^2+d^2\right) = |z| \times |z'| = |zz'|$. En examinant les seize possibilités de développement de $|(\pm a \pm ib)(\pm c \pm id)| = |zz'|$, nous obtenons d'une part que $\left(a^2+b^2\right)\left(c^2+d^2\right) = (ac+bd)^2+(ad-bc)^2 = (ac-bd)^2+(ad+bc)^2$ et d'autre part que ce sont les deux seules façons de décomposer $\left(a^2+b^2\right)\left(c^2+d^2\right)$ en somme de deux carrés. Or, la décomposition en produit de facteurs premiers donne $8633 = 89 \times 97$. Or, 89 et 97 se décomposent de manière unique en somme de deux carrés $89 = 5^2+8^2$ et $97 = 4^2+9^2$. Donc 8633 est un produit de sommes de deux carrés. D'après ce que nous avons vu, 8633 peut donc se décomposer de deux façons en somme de deux carrés. En posant $a = 5, b = 8, c = 4, d = 9$, nous obtenons $8633 = 13^2+(2\times 46)^2 = 77^2+(2\times 26)^2$. Les deux solutions sont donc $(13;46)$ et $(77;26)$. $\square$

1.7 Famille de solutions

Exercice 15. *Résoudre* $x^2+y^2 = z^2$, *où* $(x,y,z) \in \mathbb{N}^3$.

Solution. Nous cherchons les triplets pythagoriciens. Remarquons que si (x,y,z) est solution non triviale, alors $\frac{1}{\mathrm{PGCD}(x,y,z)}(x,y,z)$ est solution. Et si (x,y,z) est solution, alors $\forall n \in \mathbb{N}, n(x,y,z)$ est solution. Il suffit donc de déterminer les solutions (x,y,z) vérifiant $\mathrm{PGCD}(x,y,z) = 1$. Si x est y sont pairs, alors z^2 est pair donc z est pair, donc $\mathrm{PGCD}(x,y,z) \geq 2$. Impossible. Si x et y sont impairs, alors z^2 est pair donc z est pair donc z^2 est divisible par 4 et $x^2+y^2 \equiv 2 \pmod 4$. Impossible. Donc x et y sont de parité différente. Par symétrie du problème en x et y, nous pouvons supposer x impair et y pair. Alors z^2 est impair donc z est impair. Montrons que x et z sont premiers entre eux. Soit p un diviseur premier commun à x et z. Alors p divise $z \times z - x \times x = y \times y$. Donc d'après le lemme d'Euclide, p divise y. Ainsi, p divise x,y,z donc $p \leq \mathrm{PGCD}(x,y,z) = 1$. Or, p est premier donc $p > 1$. Contradiction. Ainsi,

x et z n'admettent aucun diviseur premier commun donc x et z sont premiers entre eux. Or, $y, z-x, z+x$ sont pairs donc nous écrivons $\left(\frac{y}{2}\right)^2 = \frac{z-x}{2} \times \frac{z+x}{2}$. Or, $\frac{z+x}{2}$ et $\frac{z-x}{2}$ sont premiers entre eux. En effet, si $d \geq 1$ est un diviseur commun à ces deux entiers, alors d divise leur différence x et leur somme z. Donc $d \leq \mathrm{PGCD}(x,z) = 1$. Donc $d = 1$. Nous démontrons et appliquons ensuite le lemme suivant : si ab est un carré et si a et b sont premiers entre eux, alors a et b sont des carrés. Soit p un diviseur premier de a. Puisque a et b sont premiers entre eux, $p > 1$ ne divise pas b. Or, p est premier donc p et b sont premiers entre eux. Plus généralement, b est premier à toute puissance de p. Par ailleurs, p divise ab donc par hypothèse, p apparaît à une puissance paire dans la décomposition en produit de facteurs premiers de ab. Il existe donc un entier naturel α tel que $p^{2\alpha} \mid ab$ et $p^{2\alpha+1} \nmid ab$. Or, $p^{2\alpha}$ et b sont premiers entre eux donc d'après le théorème de Gauss, $p^{2\alpha} \mid a$. Et $p^{2\alpha+1} \nmid a$ sinon nous aurions $p^{2\alpha+1} \mid ab$. Ainsi, tout diviseur premier de a apparaît à une puissance paire dans la décomposition canonique de a donc a est un carré. Par symétrie du problème en a et b, il en va de même pour b. Donc a et b sont des carrés. Nous en déduisons que $\frac{z-x}{2}$ et $\frac{z+x}{2}$ sont des carrés. Il vient aisément qu'il existe deux entiers naturels m, n premiers entre eux tels que $(x,y,z) = \left(m^2 - n^2, 2mn, m^2 + n^2\right)$. Réciproquement, pour tous entiers naturels m, n premiers entre eux, nous vérifions que $\left(m^2 - n^2, 2mn, m^2 + n^2\right)$ est solution car $\left(m^2 - n^2\right)^2 + (2mn)^2 = m^4 - 2(mn)^2 + n^4 + 4(mn)^2 = \left(m^2 + n^2\right)^2$. Si nous avions supposé x pair, nous aurions obtenu les solutions $(x,y,z) = \left(2mn, m^2 - n^2, m^2 + n^2\right)$. Le triplet pythagoricien minimal vérifiant $xyz \neq 0$ s'obtient en minimisant m, n premiers entre eux tels que $m > n > 0$. Il suffit de prendre $m = 2, n = 1$ et nous retrouvons bien $(3;4;5)$ ou $(4;3;5)$. $\square$

Exercice 16. *Résoudre* $\left(x^2 + xy - y^2\right)^2 = 1$, *où* $(x,y) \in \mathbb{N}^2$.

Solution. Si $x = y$, nous obtenons $x^4 = 1$ donc $(1;1)$ est l'unique solution vérifiant $x = y$. Si $x \neq y$, nous avons déjà les solutions évidentes $(0;1)$ et $(1;0)$, qui sont les seules solutions correspondant à $xy = 0$. Si de plus $xy \neq 0$, alors $xy \geq 2$. Nous en déduisons que $x^2 - y^2 < 0$, sinon $\left(x^2 + xy - y^2\right)^2 \geq 4$. Ainsi, $x \neq y$, $xy \neq 0$ et l'équation est symétrique en x, y donc nous pouvons choisir $0 < x < y$ sans perte de généralité. Nous remarquons que $(1;2), (2;3), (3;5)$ et $(5;8)$ sont des solutions particulières. Montrons que si (x,y) est solution, alors $(y, x+y)$ est également solution. $\left(y^2 + y(x+y) - (x+y)^2\right)^2 = \left(y^2 + xy + y^2 - x^2 - 2xy - y^2\right)^2 = \left(-\left(x^2 + xy - y^2\right)\right)^2 = 1$. La suite de Fibonacci, définie par $u_0 = 0, u_1 = 1$ et $\forall n \in \mathbb{N}, u_{n+2} = u_{n+1} + u_n$, fournit donc une famille infinie de solutions, les couples $(u_n, u_{n+1}), \forall n \in \mathbb{N}$. Réciproquement, montrons que ce sont les seules solutions différentes de $(1;0)$. Nous pouvons montrer aisément que si (x,y) est solution, avec $x \neq y$ et $xy \neq 0$, alors $(x', y') := (y - x, x)$ est solution. Nous avons $x'y' \neq 0$ sinon $x = y$ ou $x = 0$, ce qui est exclu. Si $x' = y'$, alors $y = 2x$ donc $x^4 = 1$ et comme $x > 0$, nous avons $(x,y) = (1;2)$ et $(x', y') = (1;1)$. Ces deux solutions font bien partie de la famille de solutions donnée par la suite de Fibonacci. Sinon, si $x' \neq y'$, alors $0 < x' < y'$ donc $x' < x = y'$. Nous avons aussi $x = y' < y$. La condition $x' \neq y'$ permet de répéter ce processus indéfiniment si elle est supposée vraie pour chaque nouvelle solution. Nous aurions donc deux suites d'entiers naturels strictement décroissantes, ce qui est impossible. Ce processus s'arrête donc à la solution $(1;1)$, et en remontant les étapes, nous obtenons bien les solutions fournies par la suite de Fibonacci puisque $(x,y) = (y', x'+y')$. Les solutions restantes se déduisent par symétrie en x, y. On remarque qu'en divisant par $y^4 \neq 0$, on reconnaît dans le membre de gauche un trinôme relié au nombre d'or, lui-même relié à la suite de Fibonacci. $\square$

Exercice 17. *Résoudre* $x^2 - 8y^2 = 1$, *où* $(x,y) \in \mathbb{N}^2$.

Solution. Il s'agit d'une équation de Fermat. Remarquons que nous avons nécessairement $x \geq 1$. Si $y = 0$, l'unique solution est $(1;0)$. Si $y = 1$, l'unique solution est $(3;1)$. Soit (x,y) une solution telle que $y \geq 1$. L'idée est de faire apparaître 9 qui est le carré le plus proche de 8. Nous avons $y^2 \geq 1 \iff y^2 + 8y^2 \geq 1 + 8y^2 \iff 9y^2 \geq x^2 \iff 3y \geq x$ donc $3y - x \in \mathbb{N}$. En écrivant $x^2 = (3y)^2 - \big(y^2 - 1\big)$, nous avons l'idée géométrique de considérer que le carré de côté x est obtenu à partir du carré de côté $3y$ auquel nous retranchons la quantité entière $n := 3y - x$. Ainsi, $x^2 = (3y - n)^2$. Les deux expressions de x^2 mènent à $y^2 - 6ny + n^2 - 1 = 0$. Ce n'est pas une équation du second degré en y car n dépend entre autres de y. Cependant, la forme canonique permet d'écrire $(y - 3n)^2 - \big(\sqrt{8n^2+1}\big)^2 = 0$, d'où vient $y = 3n \pm \sqrt{8n^2+1}$. Puisque $y - 3n \in \mathbb{Z}$, nous avons $\sqrt{8n^2+1} \in \mathbb{N}$. Posons $(x', y') := \big(\sqrt{8n^2+1}, n\big)$. Nous vérifions aisément que (x', y') est solution de l'équation de départ. Nous pouvons exprimer (x,y) linéairement en fonction de (x', y'). Nous avons $y = 3n \pm \sqrt{8n^2+1} \iff 3y = 9n \pm 3\sqrt{8n^2+1} \iff 3y - n = 8n \pm 3\sqrt{8n^2+1} \iff x = \pm 3x' + 8y'$. Or, (x', y') est solution donc $x'^2 = 8y'^2 + 1 \implies x'^2 > 8y'^2 \iff x' > \sqrt{8}y' \iff \sqrt{8}x' > 8y' \implies 3x' > 8y' \iff -3x' + 8y' < 0$. Or, $x > 0$, donc $x = 3x' + 8y'$ et $y = 3n + \sqrt{8n^2+1} \iff y = x' + 3y'$. En résumé, si (x,y) est une solution telle que $y \geq 1$, alors il existe une solution (x', y') vérifiant $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$. Réciproquement, s'il existe une solution (x', y'), alors le couple (x,y) défini par $\begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$ est bien solution car $(3x'+8y')^2 - 8(x'+3y')^2 = 9x'^2 + 48x'y' + 64y'^2 - 8x'^2 - 48x'y' - 72y'^2 = x'^2 - 8y'^2 = 1$ et nous avons aussi $y = x' + 3y' \geq x' \geq 1$. En posant $(x_0, y_0) := (1;0)$ et $\forall n \in \mathbb{N}$, $\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} := \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$, nous avons ainsi une famille de solutions données par la suite $(x_n, y_n)_{n \in \mathbb{N}}$. Nous remarquons que $(x_1, y_1) = (3;1)$, solution que nous avions déjà trouvée. Montrons que cette famille de solutions fournit toutes les solutions de l'équation. Soit (x,y) solution telle que $y \geq 1$. Nous avons vu qu'il existe une solution (x', y') telle que $\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 & 8 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$. En inversant la matrice, nous obtenons $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 3 & -8 \\ -1 & 3 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$. Nous avons $0 < 4y^2 + 1 \iff 4y^2 <$

$4y^2+4y^2+1 \iff 4y^2 < x^2 \iff 2y < x \iff -x+3y < y$ donc $y' < y$. La condition $y' \geq 1$ permet de répéter ce processus indéfiniment si elle est supposée vraie pour chaque nouvelle solution. Nous aurions donc une suite d'entiers naturels strictement décroissante, ce qui est impossible. Ce processus s'arrête donc à la solution $(1;0)$ et nous pouvons remonter les étapes jusqu'à (x,y), qui appartient donc à la famille de solutions données par la suite $(x_n, y_n)_{n\in\mathbb{N}}$.. ☐

2 Quelques équations particulières

2.1 Autour de $7^x - 3 \times 2^y = 1$

Exercice 18. *Résoudre* $7^x - 3 \times 2^y = 1$, *où* $(x,y) \in \mathbb{N}^2$.

Solution n° 1. Les deux seules solutions pour $0 \leq y \leq 4$ sont $(1;1)$ et $(2;4)$. Montrons qu'il n'existe pas d'autre solution. Soit $y \geq 5$. Posons $y := y'+5$, où $y' \geq 0$. Ainsi, $7^x - 3 \times 32 \times 2^{y'} = 1$ donc $7^x \equiv 1 \pmod{32}$. Or, $7^0 \equiv 1 \pmod{32}, 7^1 \equiv 7 \pmod{32}, 7^2 \equiv 17 \pmod{32}, 7^3 \equiv 23 \pmod{32}$ et $7^4 \equiv 1 \pmod{32}$. Nous en déduisons que $4 \mid x$. En effet, la division euclidienne de x par 4 donne l'existence de $(q,r) \in \mathbb{N}^2, x = 4q+r, 0 \leq r \leq 3$. Donc $\left(7^4\right)^q \times 7^r \equiv 1 \pmod{32}$, d'où $7^r \equiv 1 \pmod{32}$. Cela impose $r = 0$ donc $x = 4q$. Le fait que $7 \equiv 2 \pmod 5$ nous incite à réduire l'équation modulo 5. Nous avons $2^4 \equiv 1 \pmod 5$ donc $7^x \equiv 1 \pmod 5$. Or, $-3 \equiv 2 \pmod 5$. Donc nous obtenons $2^{y+1} \equiv 0 \pmod 5$. Or, 5 n'apparaît pas dans la décomposition en produit de facteurs premiers de 2^{y+1}, donc $5 \nmid 2^{y+1}$. Contradiction. Les deux solutions sont donc $(1;1)$ et $(2;4)$. ☐

Solution n° 2. Nous pouvons nous passer des congruences pour résoudre cette équation, en reconnaissant la somme des termes d'une suite géométrique. Cette solution est due à Tarik Belhaj Soulami. Les deux seules solutions pour $0 \leq x \leq 2$ et $0 \leq y \leq 4$ sont $(1;1)$ et $(2;4)$. Soient $x \geq 3$ et $y \geq 5$. Nous avons $7^x - 3 \times 2^y = 1 \iff \dfrac{7^x-1}{7-1} = 2^{y-1} \iff 7^{x-1}+7^{x-2}\cdots+7+1 = 2^{y-1}$. Le membre de gauche de cette égalité est pair donc le nombre de puissances de 7 différentes de 1, c'est-à-dire x, est pair donc $x \geq 4$. En regroupant par paires, il vient donc $7^{x-1}+7^{x-2}\cdots+7+1 = 7^{x-2}(7+1)+\cdots+7^2(7+1)+7+1 = (7+1)\left(7^{x-2}+7^{x-4}+\cdots+7^2+1\right)$ donc $7^{x-2}+7^{x-4}+\cdots+7^2+1 = 2^{y-4}$. Or, $y-4 \geq 1$ donc le membre de gauche de cette dernière égalité est pair. Donc le nombre de puissances de 7 différentes de 1, c'est-à-dire $\dfrac{x}{2}$, est pair. En regroupant par paires, il vient donc $7^{x-2}+7^{x-4}+\cdots+7^2+1 = 7^{x-4}\left(7^2+1\right)+7^{x-8}\left(7^2+1\right)+\cdots+7^2+1 = \left(7^2+1\right)\left(7^{x-4}+7^{x-8}+\cdots+7^4+1\right) = 2^{y-4}$. Donc 50 divise 2^{y-4}. C'est la contradiction souhaitée. ☐

2.2 Autour de $x^y = y^x$

Exercice 19. *Résoudre* $x^y = y^x$, *où* $(x,y) \in \mathbb{N}^2$ *et* $x \neq y$.

Solution n° 1. Par symétrie du problème en x et y, nous pouvons supposer $x < y$. Il vient aisément $2 \leq x < y$. Donc x et y se décomposent chacun en produit de facteurs premiers. Ainsi, il existe un entier naturel $n \geq 1$ tel que $x = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ et $y = p_1^{\beta_1} \dots p_n^{\beta_n}$ avec éventuellement certaines puissances nulles. Par unicité de la décomposition, l'équation implique que $\forall i \in [\![1, n]\!], \alpha_i y = \beta_i x \iff \dfrac{\beta_i}{\alpha_i} = \dfrac{y}{x}$. Or, $\dfrac{y}{x} > 1$ donc $\forall i \in [\![1, n]\!], \alpha_i < \beta_i$ donc $x \mid y$. Posons $k := \dfrac{y}{x}$. Il vient $\forall i \in [\![1, n]\!], \beta_i = k\alpha_i$ donc $y = x^k$, avec $k \geq 2$. Donc $\dfrac{y}{x} = x^{k-1} \implies k = x^{k-1} \geq 2^{k-1}$. Or, nous pouvons montrer par récurrence que pour tout entier $k \geq 3, 2^{k-1} > k$. Donc $k = 2$. Les deux solutions sont donc $(2; 4)$ et $(4; 2)$. $\square$

Solution n° 2. Nous pouvons résoudre cette équation à l'aide d'une étude de fonction. Comme précédemment, partons de $2 \leq x < y$. Nous avons $x^y = y^x \iff \dfrac{\ln x}{x} = \dfrac{\ln y}{y}$. Étudions la fonction $f : x \mapsto \dfrac{\ln x}{x}$.

x	2		e		$+\infty$
signe de $f'(x)$		$+$	0	$-$	
variations de f	$\dfrac{\ln 2}{2}$	$\nearrow$	$\dfrac{1}{\mathrm{e}}$	$\searrow$	0

Soit $x \in [2; \mathrm{e}[$. Puisque $\dfrac{\ln 2}{2} > 0$, le théorème des valeurs intermédiaires assure l'existence d'un unique $y \in]\mathrm{e}; +\infty[$ tel que $f(x) = f(y)$. Or, $x = 2$ est le seul entier naturel de l'intervalle $[2; \mathrm{e}[$. Il existe donc un unique réel $y \in]\mathrm{e}; +\infty[$ tel que $2^y = y^2$. Or, l'entier $y = 4$ convient. Les deux solutions sont donc $(2; 4)$ et $(4; 2)$. $\square$