Plaquette 5 – Équations diophantiennes et problèmes

Arithmétique dans Z — Prépa MPSI / MP2I (1re année)

Corrections détaillées

Boîte à outils

Équations diophantiennes.

— **Équation linéaire** $ax + by = c$: solvable si et seulement si $d = a \wedge b$ divise c ; si (x_0, y_0) est une solution, les solutions sont

$$x = x_0 + \frac{b}{d}k, \qquad y = y_0 - \frac{a}{d}k, \qquad k \in \mathbb{Z}$$

— **Factorisation** : $xy + \alpha x + \beta y = \gamma \Leftrightarrow (x+\beta)(y+\alpha) = \gamma + \alpha\beta$; on énumère les diviseurs.

— **Obstructions modulaires** : carrés modulo 4 : $\{0, 1\}$; modulo 8 : $\{0, 1, 4\}$; cubes modulo 9 : $\{0, 1, 8\}$.

— **Triplets pythagoriciens primitifs** : $(m^2 - n^2,\ 2mn,\ m^2 + n^2)$ avec $m > n \geq 1$, $m \wedge n = 1$, m et n de parités différentes.

— **Descente infinie** : une solution non nulle en fournirait une strictement plus petite ; comme $\mathbb{N}$ n'a pas de suite strictement décroissante infinie, il n'y en a pas.

— **Lemme** : si q premier, $q \equiv 3 \pmod 4$, alors -1 n'est pas un carré modulo q.

Correction de l'exercice 1 – Équation linéaire à deux inconnues

a) $\gcd(12, 18) = 6$ divise $12x + 18y$ pour tous entiers x, y. Or $6 \nmid 31$: **aucune solution**.

b) $6 \mid 30$: on divise par 6, $2x + 3y = 5$ avec $2 \wedge 3 = 1$. Solution particulière évidente : $(1, 1)$. On soustrait :

$$2(x-1) = -3(y-1)$$

— $2 \mid 3(y-1)$ et $2 \wedge 3 = 1$: par **Gauss**, $y - 1 = -2k$, puis $x - 1 = 3k$.

— Solutions : $(x, y) = (1 + 3k,\ 1 - 2k)$, $k \in \mathbb{Z}$. Contrôle $k = 1$: $12 \times 4 + 18 \times (-1) = 30$ ✓.

c) On se ramène à $2x + 3y = 50$. Alors $3y = 50 - 2x$ est pair, donc y est pair : $y = 2j$ et $x = 25 - 3j$.

— $x \geq 0$ et $y \geq 0$ imposent $0 \leq j \leq 8$: **neuf solutions**, de $(25, 0)$ à $(1, 16)$: $(25, 0), (22, 2), (19, 4), \ldots, (1, 16)$.

Piège : l'ensemble des solutions de b) est infini, mais la contrainte de signe de c) en retient un nombre fini ; il faut toujours finir par l'encadrement du paramètre.

Réponse. a) Aucune. b) $(1 + 3k, 1 - 2k)$. c) Neuf solutions $(25 - 3j, 2j)$, $0 \leq j \leq 8$.

Correction de l'exercice 2 – Le problème des cent volailles

a) Nombre de volailles et prix (les poussins coûtent $\frac{1}{3}$ pièce) :

$$c + p + q = 100, \qquad 5c + 3p + \frac{q}{3} = 100$$

— avec $c, p, q \in \mathbb{N}$. On multiplie la seconde par 3 : $15c + 9p + q = 300$.

b) En soustrayant la première équation : $14c + 8p = 200$, soit $7c + 4p = 100$.

— $4 \mid 7c$ (car $4 \mid 100 - 4p$) et $4 \wedge 7 = 1$: $c = 4k$ par **Gauss**, puis $p = 25 - 7k$.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

— $p \geq 0$ impose $k \leq 3$; $c \geq 0$ impose $k \geq 0$.

c) $q = 100 - c - p = 75 + 3k$ (bien un multiple de 3, ce qui rend le prix des poussins entier). Solutions pour $k = 0, 1, 2, 3$:

— $(c, p, q) = (0, 25, 75)$, $(4, 18, 78)$, $(8, 11, 81)$, $(12, 4, 84)$.

Vérification pour $(8, 11, 81)$: $8 + 11 + 81 = 100$ volailles ; $40 + 33 + 27 = 100$ pièces ✓.

Remarque : si l'on exige au moins un animal de chaque sorte, il reste trois solutions.

Réponse. $7c + 4p = 100$; $(0, 25, 75)$, $(4, 18, 78)$, $(8, 11, 81)$, $(12, 4, 84)$.

Correction de l'exercice 3 – Billets de 5 et 7 euros

a) On résout $5x + 7y = 100$ dans $\mathbb{N}^2$. $5 \mid 7y$ et $5 \wedge 7 = 1$, donc $y = 5j$, puis $x = 20 - 7j$:

$$(x, y) = (20 - 7j,\ 5j), \qquad 0 \leq j \leq 2$$

— Trois façons : $(20, 0)$, $(13, 5)$, $(6, 10)$.

b) $23 = 7y + 5x$ avec $y \in \{0, 1, 2, 3\}$ donne $23, 16, 9, 2$ à payer en billets de 5 : aucun n'est multiple de 5. Impossible.

— $24 = 7 \times 2 + 5 \times 2$, $25 = 5 \times 5$, $26 = 7 \times 3 + 5$, $27 = 7 + 5 \times 4$, $28 = 7 \times 4$.

— Tout $n \geq 24$ s'écrit $n = m + 5k$ avec $m \in \{24, \ldots, 28\}$ (m est le représentant de n modulo 5 dans cette plage) : on ajoute k billets de 5 €.

c) En testant 1 à 22 : impossibles $1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23$, soit 12 montants.

— $\frac{4 \times 6}{2} = 12$ ✓ et $35 - 12 = 23$ ✓.

Remarque : pour $a \wedge b = 1$, le plus grand montant impossible est $ab - a - b$ (nombre de **Frobenius**) ; il n'existe pas de formule analogue avec trois valeurs de billets.

Réponse. a) 3 façons. b) 23 impossible, tout $n \geq 24$ possible. c) 12 montants impossibles, le plus grand 23.

Correction de l'exercice 4 – Transvasements

a) Chaque opération (remplir, vider, transvaser) ajoute ou retire au contenu total des multiples de 9 ou de 4, ou le conserve : toute quantité obtenue s'écrit $9u + 4v$ avec u, v entiers. Par **Bézout**, ces nombres sont exactement les multiples de

$$9 \wedge 4 = 1$$

— donc toute quantité entière est envisageable. $9 \times 1 - 4 \times 2 = 1$, d'où $9 \times 6 - 4 \times 12 = 6$; la solution générale est $(6 + 4k,\ -12 - 9k)$ et $k = -1$ donne $(u, v) = (2, -3)$: $18 - 12 = 6$.

b) $u = 2$: on remplit **deux fois** le grand bidon ; $v = -3$: on remplit trois fois le petit à partir du grand (deux fois vidé dans l'évier, la troisième fois il reste plein). Suite d'états (g, p) :

— $(9, 0) \to (5, 4) \to (5, 0) \to (1, 4) \to (1, 0) \to (0, 1)$;

— $(9, 1)$ (second remplissage) $\to (6, 4)$: le petit reçoit 3 L.

Bilan : 18 L puisés, 8 L jetés, 4 L dans le petit, 6 L dans le grand ✓.

c) Toute quantité est de la forme $6u + 4v$, donc un multiple de $6 \wedge 4 = 2$. 3 est impair : **impossible**, quelle que soit l'astuce.

Réponse. $9 \times 2 - 4 \times 3 = 6$: deux remplissages du grand, trois du petit ; avec 6 L et 4 L, seules les quantités paires sont possibles.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Correction de l'exercice 5 – Rectangles dont l'aire égale le périmètre

a) $xy = 2(x+y)$, soit $xy - 2x - 2y = 0$. On complète le produit en ajoutant 4 des deux côtés :

$$(x-2)(y-2) = 4$$

b) $x-2$ et $y-2$ sont deux entiers de produit 4 avec $x-2 \leq y-2$.

— Facteurs positifs : $(1,4)$ donne $(x,y) = (3,6)$; $(2,2)$ donne $(4,4)$.

— Facteurs négatifs : $(-4,-1)$ et $(-2,-2)$ donneraient $x \leq 0$: exclus.

Deux rectangles : 3×6 (aire 18, périmètre 18) et le carré 4×4 (aire et périmètre 16) ✓.

c) $xy = 6(x+y)$ donne $(x-6)(y-6) = 36$. Les couples de diviseurs positifs de 36 avec $d \leq \frac{36}{d}$: $(1,36), (2,18), (3,12), (4,9), (6,6)$, d'où

— $(x,y) \in \{(7,42), (8,24), (9,18), (10,15), (12,12)\}$.

— Facteurs négatifs : $x - 6 = -d$ avec $d \geq 1$ et $y - 6 = -\frac{36}{d}$; $x, y > 0$ impose $d < 6$ et $\frac{36}{d} < 6$, incompatibles.

Contrôle $(10,15)$: aire 150, périmètre 50 ✓.

Réponse. $(x-2)(y-2) = 4$: 3×6 et 4×4 ; aire triple : 7×42, 8×24, 9×18, 10×15, 12×12.

Correction de l'exercice 6 – Somme de deux fractions unitaires

a) On multiplie par nxy : $ny + nx = xy$, soit $xy - nx - ny = 0$, puis en ajoutant n^2 :

$$(x-n)(y-n) = n^2$$

— De plus $\frac{1}{x} < \frac{1}{n}$ (car $\frac{1}{y} > 0$), donc $x > n$; de même $y > n$.

b) Les solutions correspondent aux couples $(d, \frac{n^2}{d})$ avec d diviseur **positif** de n^2 (les facteurs sont positifs d'après a)), via $x = n + d$, $y = n + \frac{n^2}{d}$. Il y en a $\tau(n^2)$.

c) $n^2 = 36 = 2^2 \times 3^2$, $\tau(36) = 3 \times 3 = 9$ couples ordonnés. Avec $x \leq y$ ($d \leq 6$) :

— $d = 1, 2, 3, 4, 6$: $(7,42)$, $(8,24)$, $(9,18)$, $(10,15)$, $(12,12)$.

Contrôle : $\frac{1}{10} + \frac{1}{15} = \frac{3+2}{30} = \frac{1}{6}$ ✓.

d) Le nombre de solutions avec $x \leq y$ est $\frac{\tau(n^2)+1}{2}$ ($\tau(n^2)$ est impair car n^2 est un carré). Il vaut 1 si et seulement si $\tau(n^2) = 1$, soit $n = 1$: $\frac{1}{2} + \frac{1}{2} = 1$. Pour $n = p$ premier, $\tau(p^2) = 3$ donne deux solutions, $(p+1, p^2+p)$ et $(2p, 2p)$.

Réponse. $(x-n)(y-n) = n^2$; $\tau(n^2)$ solutions ; pour $n = 6$:
$(7,42), (8,24), (9,18), (10,15), (12,12)$.

Correction de l'exercice 7 – Différence de deux carrés

a) On factorise :

$$x^2 - y^2 = (x-y)(x+y) = 45$$

— avec $0 \leq x - y \leq x + y$, deux diviseurs de 45 de produit 45 et de **même parité** (leur somme $2x$ est paire). 45 étant impair, tous ses diviseurs le sont.

— $(1,45)$: $x = 23$, $y = 22$; $(3,15)$: $x = 9$, $y = 6$; $(5,9)$: $x = 7$, $y = 2$.

Contrôle : $81 - 36 = 45$ ✓, $49 - 4 = 45$ ✓.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

b) Modulo 4, un carré vaut 0 ou 1, donc $x^2 - y^2 \in \{0, 1, -1\} \equiv \{0, 1, 3\}$: jamais 2.

c) Impair : $2k + 1 = (k+1)^2 - k^2$. Multiple de 4 : $4k = (k+1)^2 - (k-1)^2$. Exemples : $45 = 23^2 - 22^2$; $12 = 4^2 - 2^2$.

Bilan : n est différence de deux carrés si et seulement si $n \not\equiv 2 \pmod 4$.

Réponse. $(23, 22)$, $(9, 6)$, $(7, 2)$; n est différence de deux carrés $\Leftrightarrow n \not\equiv 2 \pmod 4$.

Correction de l'exercice 8 – Triplets pythagoriciens

a) x et y ne sont pas tous deux pairs ($x \wedge y = 1$). S'ils étaient tous deux impairs, $z^2 = x^2 + y^2 \equiv 1 + 1 = 2 \pmod 4$, impossible pour un carré. Donc l'un est pair, l'autre impair ; z est impair.

b) z et x sont impairs : $z \pm x$ sont pairs, $a = \frac{z+x}{2}$ et $b = \frac{z-x}{2}$ sont entiers. On a

$$ab = \frac{z^2 - x^2}{4} = \left(\frac{y}{2}\right)^2$$

— Un diviseur commun de a et b divise $a + b = z$ et $a - b = x$; or $x \wedge z = 1$ (un premier commun diviserait y^2, donc y). Donc $a \wedge b = 1$.

— Deux entiers premiers entre eux dont le produit est un carré sont des carrés : pour chaque p, $v_p(a) + v_p(b)$ est pair et l'un des deux est nul. Donc $a = m^2$, $b = n^2$.

c) $z = a + b = m^2 + n^2$, $x = a - b = m^2 - n^2$, $y = 2\sqrt{ab} = 2mn$. Avec $m > n \geq 1$, $m \wedge n = 1$, $m - n$ impair :

— $(m, n) = (2, 1)$: $(3, 4, 5)$; $(3, 2)$: $(5, 12, 13)$; $(4, 1)$: $(15, 8, 17)$; $(4, 3)$: $(7, 24, 25)$; $(5, 2)$: $(21, 20, 29)$.

— $(5, 4)$ donnerait $z = 41 > 30$; $(3, 1)$ est exclu (même parité, triplet $(8, 6, 10)$ non primitif).

Cinq triplets primitifs avec $z \leq 30$.

Réponse. $(m^2 - n^2, 2mn, m^2 + n^2)$; $z \leq 30$: $(3, 4, 5)$, $(5, 12, 13)$, $(8, 15, 17)$, $(7, 24, 25)$, $(20, 21, 29)$.

Correction de l'exercice 9 – Points rationnels du cercle unité

a) D_t : $y = t(x + 1)$. En reportant dans l'équation du cercle :

$$x^2 + t^2(x+1)^2 = 1 \Leftrightarrow (x+1)[(1+t^2)x - (1-t^2)] = 0$$

— (on factorise $x^2 - 1 = (x-1)(x+1)$). La racine $x = -1$ correspond à A ; l'autre donne

$$M_t = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right)$$

b) Si $t \in \mathbb{Q}$, les coordonnées sont des quotients de rationnels : $M_t \in \mathbb{Q}^2$. Réciproquement, si $M(x, y) \in C \cap \mathbb{Q}^2$ avec $M \neq A$, la pente de (AM) est $t = \frac{y}{x+1} \in \mathbb{Q}$ et $M = M_t$.

c) Avec $t = \frac{n}{m}$: $M = \left(\frac{m^2 - n^2}{m^2 + n^2}, \frac{2mn}{m^2 + n^2}\right)$. Chasser les dénominateurs dans $x^2 + y^2 = 1$ donne

— $(m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2$: les triplets de l'exercice précédent.

— $M_{1/2} = \left(\frac{1 - 1/4}{1 + 1/4}, \frac{1}{5/4}\right) = \left(\frac{3}{5}, \frac{4}{5}\right)$, triplet $(3, 4, 5)$.

— $M_{2/3} = \left(\frac{5/9}{13/9}, \frac{4/3}{13/9}\right) = \left(\frac{5}{13}, \frac{12}{13}\right)$, triplet $(5, 12, 13)$.

Idée : c'est la **paramétrisation rationnelle** du cercle, qui ramène un problème d'arithmétique à de la géométrie de droites.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Réponse. $M_t = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$; $M_{1/2} = \left(\frac{3}{5}, \frac{4}{5}\right)$, $M_{2/3} = \left(\frac{5}{13}, \frac{12}{13}\right)$.

Correction de l'exercice 10 – Sommes de deux carrés

a) On développe les deux membres :

$$(ac-bd)^2+(ad+bc)^2 = a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2 = (a^2+b^2)(c^2+d^2)$$

— (interprétation : $|z|^2|w|^2 = |zw|^2$ avec $z = a+\mathrm{i}b$, $w = c+\mathrm{i}d$).

b) $5 = 1^2+2^2$ et $13 = 2^2+3^2$. Avec $(a,b,c,d) = (1,2,2,3)$:
$(2-6)^2+(3+4)^2 = 16+49 = 65$. En échangeant c et d : $(3-4)^2+(2+6)^2 = 1+64 = 65$.

— $65 = 4^2+7^2 = 1^2+8^2$.

c) $2026 = 2\times 1013 = (1^2+1^2)(22^2+23^2)$:

— $(22-23)^2+(23+22)^2 = 1+2025 = 2026$, soit $2026 = 1^2+45^2$.

d) On teste $a^2 \le 21$: $21-0 = 21$, $21-1 = 20$, $21-4 = 17$, $21-9 = 12$, $21-16 = 5$; aucun n'est un carré.

— Explication : $21 = 3\times 7$ contient des premiers $\equiv 3 \pmod 4$ à un exposant **impair**. Le théorème des deux carrés (Fermat-Euler) : n est somme de deux carrés si et seulement si chaque premier $p \equiv 3 \pmod 4$ figure dans n avec un exposant pair. La condition modulo 4 n'est que nécessaire.

Réponse. $65 = 4^2+7^2 = 1^2+8^2$; $2026 = 1^2+45^2$; 21 n'est pas somme de deux carrés.

Correction de l'exercice 11 – Sommes de trois cubes modulo 9

a) Avec $x = 3k+r$, $r \in \{-1,0,1\}$, le binôme donne

$$x^3 = 27k^3+27k^2r+9kr^2+r^3 \equiv r^3 \pmod 9$$

— et $r^3 \in \{-1,0,1\}$. Donc $x^3 \equiv 0, 1$ ou $-1 \equiv 8 \pmod 9$.

b) Somme de trois éléments de $\{-1,0,1\}$: tout entier de -3 à 3, soit modulo 9 : $0,1,2,3,6,7,8$. Jamais 4 ni 5 :

$$x^3+y^3+z^3 \not\equiv \pm 4 \pmod 9$$

c) $2030 = 9\times 225+5$: $2030 \equiv 5 \pmod 9$, **aucune solution**.

— $2026 = 2025+1 \equiv 1 \pmod 9$: la congruence n'interdit rien, on ne peut **pas** conclure ainsi. Par exemple $1 = 1^3+0^3+0^3$ montre que le reste 1 est atteint ; savoir si 2026 lui-même est une somme de trois cubes est une autre question.

Remarque : on conjecture que tout $n \not\equiv \pm 4 \pmod 9$ est somme de trois cubes ; le cas $n = 33$ n'a été résolu qu'en 2019, avec des nombres de 16 chiffres.

Réponse. Cubes modulo 9 : $0, \pm 1$; $x^3+y^3+z^3 \not\equiv \pm 4 \pmod 9$; 2030 impossible, 2026 non tranché par cet argument.

Correction de l'exercice 12 – Descente infinie

a) Modulo 3, les carrés valent 0 (si $3 \mid x$) ou 1 (sinon). $x^2+y^2 \equiv 3z^2 \equiv 0$; les sommes possibles sont $0+0$, $0+1$, $1+1 \equiv 2$, et seule $0+0$ convient :

$$x^2 \equiv y^2 \equiv 0 \pmod 3 \implies 3 \mid x,\ 3 \mid y$$

— (car 3 est premier : $3 \mid x^2 \Rightarrow 3 \mid x$).

b) $x = 3x'$, $y = 3y'$: $9(x'^2+y'^2) = 3z^2$, donc $z^2 = 3(x'^2+y'^2)$ et $3 \mid z$; avec $z = 3z'$:

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

$9z'^2 = 3(x'^2 + y'^2)$, soit $x'^2 + y'^2 = 3z'^2$.

c) Descente infinie : si une solution avait $z \neq 0$, on obtiendrait des solutions avec $|z|, \frac{|z|}{3}, \frac{|z|}{9}, \ldots$ entiers strictement décroissants et > 0 — impossible dans $\mathbb{N}$. Donc $z = 0$, puis $x^2 + y^2 = 0$ et $x = y = 0$.

— Si $\left(\frac{a}{c}, \frac{b}{c}\right)$ (dénominateur commun $c \geq 1$) était sur $X^2 + Y^2 = 3$, alors $a^2 + b^2 = 3c^2$ avec $c \neq 0$: impossible.

Contraste : $X^2 + Y^2 = 2$ a le point rationnel $(1, 1)$, et donc une infinité (par la méthode des droites de l'exercice sur le cercle).

Réponse. Seule solution $(0, 0, 0)$; le cercle $X^2 + Y^2 = 3$ n'a aucun point rationnel.

Correction de l'exercice 13 – Puissances de 2 et de 3

a) $y = 0$: $2^x = 2$, donc $x = 1$. Solution $(1, 0)$.

b) $y \geq 1$: $2^x = 3^y + 1 \equiv 1 \pmod 3$. Or $2 \equiv -1 \pmod 3$:

$$2^x \equiv (-1)^x \pmod 3$$

— vaut 1 si et seulement si x est pair. Donc $x = 2k$, avec $k \geq 1$.

c) $3^y = 2^{2k} - 1 = (2^k - 1)(2^k + 1)$. Par unicité de la décomposition, chaque facteur est une puissance de 3 : $2^k - 1 = 3^\alpha$ et $2^k + 1 = 3^\beta$ avec $\alpha < \beta$.

— Leur différence vaut $2 = 3^\beta - 3^\alpha = 3^\alpha(3^{\beta-\alpha} - 1)$. Si $\alpha \geq 1$, $3 \mid 2$: impossible. Donc $\alpha = 0$ et $3^\beta = 3$.

— $2^k - 1 = 1$ donne $k = 1$, $x = 2$, puis $3^y = 3$, $y = 1$.

d) Solutions : $(1, 0)$ car $2 = 1 + 1$; $(2, 1)$ car $4 = 3 + 1$ ✓.

Remarque : c'est un cas du théorème de Mihăilescu (2002) : 8 et 9 sont les seules puissances pures consécutives.

Réponse. $(x, y) \in \{(1, 0), (2, 1)\}$.

Correction de l'exercice 14 – Équation de Pell-Fermat

a) $9 - 2 \times 4 = 1$ ✓. On calcule directement :

$$(3x + 4y)^2 - 2(2x + 3y)^2 = 9x^2 + 24xy + 16y^2 - 8x^2 - 24xy - 18y^2 = x^2 - 2y^2 = 1$$

— (c'est la multiplicativité de la « norme » $N(x + y\sqrt{2}) = x^2 - 2y^2$, avec $N(3 + 2\sqrt{2}) = 1$).

b) Partant de $(1, 0)$ ou $(3, 2)$, l'application $(x, y) \mapsto (3x + 4y, 2x + 3y)$ fournit des solutions de y strictement croissant : une infinité.

— $(3, 2) \to (17, 12) \to (99, 70) \to (577, 408)$. Contrôle : $17^2 - 2 \times 12^2 = 289 - 288 = 1$ ✓ ; $99^2 - 2 \times 70^2 = 9801 - 9800 = 1$ ✓.

c) $x^2 - 2y^2 = 1$ s'écrit $(x - y\sqrt{2})(x + y\sqrt{2}) = 1$, donc

$$\frac{x}{y} - \sqrt{2} = \frac{1}{y(x + y\sqrt{2})} \leq \frac{1}{y \times 2y\sqrt{2}} < \frac{1}{2y^2}$$

— car $x > y\sqrt{2}$. Avec $(577, 408)$: $\frac{577}{408} \approx 1{,}414\,215\,69$ et l'erreur est inférieure à $\frac{1}{2 \times 408^2} \approx 3 \times 10^{-6}$ (en réalité $2{,}1 \times 10^{-6}$; $\sqrt{2} \approx 1{,}414\,213\,56$).

Réponse. $(3x + 4y, 2x + 3y)$; $(17, 12)$, $(99, 70)$, $(577, 408)$; $\frac{577}{408}$ approche $\sqrt{2}$ à 3×10^{-6} près.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).

Correction de l'exercice 15 – Synthèse : l'équation $y^2 = x^3 + 7$

a) Supposons $y^2 \equiv -1 \pmod{q}$. Alors $q \nmid y$, et par **Fermat** $y^{q-1} \equiv 1$. Mais $q - 1 = 2m$ avec $m = \frac{q-1}{2}$ **impair** (car $q \equiv 3 \pmod 4$) :

$$y^{q-1} = (y^2)^m \equiv (-1)^m = -1 \pmod{q}$$

— d'où $1 \equiv -1 \pmod{q}$, soit $q \mid 2$: absurde puisque $q \geq 3$.

b) Si x est pair, $x^3 \equiv 0 \pmod 8$ et $y^2 \equiv 7 \pmod 8$; or les carrés modulo 8 sont $0, 1, 4$. Donc x est impair, $x^3 + 7$ est pair, y est pair et $y^2 \equiv 0 \pmod 4$. Alors $x^3 \equiv -7 \equiv 1 \pmod 4$; comme x est impair, $x^3 \equiv x \pmod 4$ (car $x^2 \equiv 1$), donc $x \equiv 1 \pmod 4$.

c) On ajoute 1 : $y^2 + 1 = x^3 + 8 = x^3 + 2^3$, et $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$ donne

$$y^2 + 1 = (x + 2)(x^2 - 2x + 4)$$

— $x^2 - 2x + 4 = (x - 1)^2 + 3$ et $4 \mid x - 1$, donc $x^2 - 2x + 4 \equiv 3 \pmod 4$ (et il est positif).

d) $x^2 - 2x + 4 \equiv 3 \pmod 4$ a un facteur premier $q \equiv 3 \pmod 4$ (produit de facteurs tous $\equiv 1$ serait $\equiv 1$). Ce q divise $y^2 + 1$, donc $y^2 \equiv -1 \pmod{q}$ — contradiction avec a). L'équation n'a pas de solution entière.

— Contrôle numérique : aucune solution avec $-2 \leq x \leq 2000$ (vérifié par programme) ; pour $x = 1$ par exemple, $x^3 + 7 = 8$ n'est pas un carré.

Réponse. -1 n'est pas un carré modulo $q \equiv 3\ (4)$; $x \equiv 1\ (4)$; $x^2 - 2x + 4 \equiv 3\ (4)$ a un facteur $q \equiv 3\ (4)$ divisant $y^2 + 1$: aucune solution.

mathlvl.fr — Tous droits réservés. Toute reproduction, diffusion, revente ou exploitation commerciale, même partielle, est strictement interdite.
Tout contrevenant s'expose à des poursuites en vertu du Code de la propriété intellectuelle (art. L.335-2 et suivants).