

Plaquette 5 – Équations diophantiennes et problèmes

Arithmétique dans $\mathbb{Z}$ — Licence 1 (L1)

Corrections détaillées

Boîte à outils

Équation $ax + by = c$ (a, b non nuls, $d = a \wedge b$) :

- **Existence** : il y a des solutions entières si et seulement si $d \mid c$.
- **Méthode** : on divise par d ; on trouve une solution particulière (x_0, y_0) (Bézout multiplié par $\frac{c}{d}$) ; par **Gauss**, toutes les solutions sont

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

Factorisation. $x^2 - y^2 = (x - y)(x + y)$; $xy - ax - by = (x - b)(y - a) - ab$. On liste alors les couples de diviseurs, **sans oublier les négatifs**.

- **Triplets pythagoriciens primitifs** : $(m^2 - n^2, 2mn, m^2 + n^2)$ avec $m > n \geq 1$, $m \wedge n = 1$, $m - n$ impair.
- **Pell-Fermat** $x^2 - 2y^2 = 1$: si (x, y) est solution, $(3x + 4y, 2x + 3y)$ aussi.
- **Frobenius** : si $a \wedge b = 1$, le plus grand entier **non** de la forme $au + bv$ ($u, v \geq 0$) est $ab - a - b$.
- **Obstruction** : réduire modulo 3, 4, 8 ou 9 ; **descente infinie** : une solution non nulle en fournirait une strictement plus petite.

Correction de l'exercice 1 - Solution générale d'une équation linéaire

a) $15 \wedge 21 = 3$ ne divise pas 40 : aucune solution (le membre de gauche est toujours multiple de 3).

b) $3 \mid 39$: on divise par 3, $5x + 7y = 13$, avec $5 \wedge 7 = 1$.

- **Bézout** : $5 \times 3 - 7 \times 2 = 1$, donc $5 \times 39 - 7 \times 26 = 13$; plus simplement, on remarque $5 \times 4 + 7 \times (-1) = 13$: $(x_0, y_0) = (4, -1)$.
- **Gauss** : si $5x + 7y = 13 = 5 \times 4 + 7 \times (-1)$, alors $5(x - 4) = 7(-1 - y)$. 7 divise $5(x - 4)$ et $7 \wedge 5 = 1$, donc $7 \mid x - 4$: $x = 4 + 7k$, puis $y = -1 - 5k$.

$$(x, y) = (4 + 7k, -1 - 5k), \quad k \in \mathbb{Z}$$

- **Réciproque** : $5(4 + 7k) + 7(-1 - 5k) = 20 + 35k - 7 - 35k = 13$ ✓

c) $x > 0 \Leftrightarrow k \geq 0$ (car $4 + 7k > 0 \Leftrightarrow k > -\frac{4}{7}$) ; $y > 0 \Leftrightarrow -1 - 5k > 0 \Leftrightarrow k \leq -1$. Incompatible : **aucune** solution strictement positive.

- Avec $x, y \geq 0$: $k \geq 0$ et $k \leq -\frac{1}{5}$, toujours incompatible. Aucune.
- **Contrôle direct** : avec $x, y \geq 0$, il faut $15x \leq 39$, donc $x \in \{0, 1, 2\}$; alors $21y = 39, 24, 9$, jamais multiple de 21 ✓

d) $|4 + 7k| + |1 + 5k|$ vaut 5 pour $k = 0$, $3 + 4 = 7$ pour $k = -1$, et grandit ensuite : le minimum est $(4, -1)$.

Réponse. a) non ($3 \nmid 40$) ; b) $(4 + 7k, -1 - 5k)$; c) aucune solution positive ; d) $(4, -1)$.

Correction de l'exercice 2 - Les cent volailles

a) Nombre de volailles et prix :

$$x + y + z = 100, \quad 5x + 3y + \frac{z}{3} = 100$$

— avec $x, y, z \in \mathbb{N}$ et z multiple de 3 (on achète les poussins par trois).

b) On multiplie la seconde par 3 : $15x + 9y + z = 300$, et on soustrait la première : $14x + 8y = 200$, soit $7x + 4y = 100$.

c) $4y = 100 - 7x$ impose $4 \mid 7x$, donc (Gauss, $4 \wedge 7 = 1$) $4 \mid x$: $x = 4k$ et $y = 25 - 7k$.

— $x \geq 0$ donne $k \geq 0$; $y \geq 0$ donne $k \leq \frac{25}{7} \approx 3,6$, soit $k \leq 3$.

— Quatre valeurs : $k \in \{0, 1, 2, 3\}$.

d) $z = 100 - x - y = 100 - 4k - 25 + 7k = 75 + 3k$, toujours multiple de 3 ✓

k	coqs x	poules y	poussins z	prix
0	0	25	75	$0 + 75 + 25 = 100$
1	4	18	78	$20 + 54 + 26 = 100$
2	8	11	81	$40 + 33 + 27 = 100$
3	12	4	84	$60 + 12 + 28 = 100$

— Si l'on exige au moins un animal de chaque sorte, il reste **trois** solutions ($k = 1, 2, 3$), celles du texte chinois.

Réponse. $7x + 4y = 100$, $x = 4k$, $y = 25 - 7k$, $z = 75 + 3k$, $k \in \{0, 1, 2, 3\}$.

Correction de l'exercice 3 - Pièces de 5 et de 7

a) $v \in \{0, 1, 2, 3\}$ (car $7v \leq 23$) : $23 - 7v$ vaut 23, 16, 9, 2, aucun n'est multiple de 5. Non payable.

b) $24 = 5 \times 2 + 7 \times 2$; $25 = 5 \times 5$; $26 = 5 \times 1 + 7 \times 3$; $27 = 5 \times 4 + 7$; $28 = 7 \times 4$.

— Pour $n \geq 24$, on écrit $n = m + 5q$ avec $m \in \{24, \dots, 28\}$ (m est le reste convenable) : on ajoute q pièces de 5 à une décomposition de m .

c) On teste $n = 1$ à 22 : non payables 1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23 (**douze** montants).

— **Remarque** : il y en a $\frac{(a-1)(b-1)}{2} = \frac{4 \times 6}{2} = 12$, formule de Sylvester ✓

d) Supposons $ab - a - b = au + bv$ avec $u, v \geq 0$. Alors $ab = a(u+1) + b(v+1)$.

$$a \mid b(v+1) \text{ et } a \wedge b = 1 \implies a \mid v+1$$

— De même $b \mid u+1$. Comme $u+1 \geq 1$ et $v+1 \geq 1$, on a $u+1 \geq b$ et $v+1 \geq a$, d'où $a(u+1) + b(v+1) \geq ab + ab = 2ab > ab$: **contradiction**.

— Ici $5 \times 7 - 5 - 7 = 23$ ✓ : c'est le **nombre de Frobenius** du couple (5, 7).

Réponse. 23 non payable, tout $n \geq 24$ payable ; non payables : 1, 2, 3, 4, 6, 8, 9, 11, 13, 16, 18, 23 ; en général $ab - a - b$.

Correction de l'exercice 4 - Différence de deux carrés

a) $(x-y)(x+y) = 45$ avec $0 \leq x-y \leq x+y$, et $x-y$, $x+y$ de **même parité** (leur somme $2x$ est paire).

$$(x-y, x+y) \in \{(1, 45), (3, 15), (5, 9)\}$$

— On résout chaque système : $(x, y) = (23, 22), (9, 6), (7, 2)$.

— **Vérification** : $529 - 484 = 45$ ✓ ; $81 - 36 = 45$ ✓ ; $49 - 4 = 45$ ✓

b) $x-y$ et $x+y$ ont même parité. S'ils sont impairs, le produit est impair ; s'ils sont pairs,

il est multiple de 4. Un $n \equiv 2 \pmod{4}$ n'est ni l'un ni l'autre.

c) $n = 2m + 1 : (m + 1)^2 - m^2 = 2m + 1 \checkmark ; n = 4m : (m + 1)^2 - (m - 1)^2 = 4m \checkmark$

d) $2\,026 = 2 \times 1\,013 \equiv 2 \pmod{4}$: **aucune** façon.

— $2\,027$ premier : le seul couple de diviseurs est $(1, 2\,027)$, d'où $x = 1\,014, y = 1\,013$: **une** seule façon.

— **Méthode** : factoriser le membre de gauche transforme l'équation en un problème de **diviseurs**, avec une condition de parité.

Réponse. a) $(23, 22), (9, 6), (7, 2)$; b) $n \equiv 2 \pmod{4}$ impossible ; d) $2\,026$: aucune, $2\,027 = 1\,014^2 - 1\,013^2$.

Correction de l'exercice 5 - Triplets pythagoriciens

a) Si a et b sont impairs, $a^2 + b^2 \equiv 1 + 1 = 2 \pmod{4}$, alors qu'un carré vaut 0 ou 1 modulo 4. Impossible. Et ils ne sont pas tous deux pairs (sinon c serait pair : triplet non primitif).

b) a impair et c impair (car $c^2 = a^2 + b^2$ impair) : $c + a$ et $c - a$ sont pairs. Posons $u = \frac{c+a}{2}, v = \frac{c-a}{2}$:

$$uv = \frac{c^2 - a^2}{4} = \left(\frac{b}{2}\right)^2$$

— Un diviseur commun de u et v divise $u + v = c$ et $u - v = a$, donc divise b aussi : il vaut 1 (primitif). $u \wedge v = 1$.

— uv est un carré et $u \wedge v = 1$: par le résultat de la plaquette 2 (exercice « Premier avec un produit »), $u = m^2$ et $v = n^2$ avec $m > n \geq 1$.

c) $c = u + v = m^2 + n^2, a = u - v = m^2 - n^2$, et $\left(\frac{b}{2}\right)^2 = m^2 n^2$ donne $b = 2mn$.

— **Réciproque** : $(m^2 - n^2)^2 + (2mn)^2 = m^4 + 2m^2 n^2 + n^4 = (m^2 + n^2)^2 \checkmark$; le triplet est primitif si $m \wedge n = 1$ et $m - n$ impair.

d) $m^2 + n^2 \leq 30$ avec ces conditions :

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

— **Figure** : $3^2 + 4^2 = 9 + 16 = 25 = 5^2 \checkmark$ — c'est le triangle « 3-4-5 » des arpenteurs égyptiens, qui sert à tracer un angle droit avec une corde à 12 nœuds.

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

Correction de l'exercice 6 - Somme de deux fractions égyptiennes

a) $\frac{1}{x} < \frac{1}{x} + \frac{1}{y} = \frac{1}{6}$, donc $x > 6$; de même $y > 6$.

b) On multiplie par $6xy$: $6y + 6x = xy$, soit $xy - 6x - 6y = 0$. On ajoute 36 pour factoriser :
 $xy - 6x - 6y + 36 = 36 \Leftrightarrow (x - 6)(y - 6) = 36$

c) $x - 6$ et $y - 6$ sont des entiers **strictement positifs** (a) de produit 36. $36 = 2^2 \times 3^2$ a $(2 + 1)(2 + 1) = 9$ diviseurs positifs : 1, 2, 3, 4, 6, 9, 12, 18, 36.

— Solutions $(x, y) : (7, 42), (8, 24), (9, 18), (10, 15), (12, 12), (15, 10), (18, 9), (24, 8), (42, 7)$: **neuf** couples ordonnés.

— **Vérification** : $\frac{1}{10} + \frac{1}{15} = \frac{3+2}{30} = \frac{1}{6} \checkmark$

d) Même calcul : $(x - n)(y - n) = n^2$, avec $x - n, y - n > 0$. Le nombre de couples ordonnés est $d(n^2)$.

— $n = 12 = 2^2 \times 3$: $n^2 = 2^4 \times 3^2$, $d(n^2) = 5 \times 3 = 15$ couples.

— **Piège** : sans a), on oublierait que les facteurs pourraient être négatifs ; ici a) les exclut (dans $\mathbb{Z}$, il y aurait d'autres solutions comme $(x - 6, y - 6) = (-4, -9)$, soit $(2, -3)$: $\frac{1}{2} - \frac{1}{3} = \frac{1}{6}$ ✓).

Réponse. $(x - 6)(y - 6) = 36$: 9 couples, de $(7, 42)$ à $(42, 7)$; en général $d(n^2)$ couples, 15 pour $n = 12$.

Correction de l'exercice 7 - Équation de Pell-Fermat

a) $9 - 8 = 1$ ✓ On développe :

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

b) À partir de $(3, 2)$: $(9 + 8, 6 + 6) = (17, 12)$; puis $(51 + 48, 34 + 36) = (99, 70)$; puis $(297 + 280, 198 + 210) = (577, 408)$.

— **Vérification** : $289 - 288 = 1$ ✓ ; $9\,801 - 9\,800 = 1$ ✓ ; $332\,929 - 332\,928 = 1$ ✓

c) Développement direct : $3x + 2x\sqrt{2} + 3y\sqrt{2} + 4y$ ✓ La « norme » $N(x + y\sqrt{2}) = x^2 - 2y^2$ est **multiplicative** ($N(\alpha\beta) = N(\alpha)N(\beta)$) et $N(3 + 2\sqrt{2}) = 1$: multiplier par $3 + 2\sqrt{2}$ préserve la solution. Les solutions sont les $(3 + 2\sqrt{2})^k$.

d) $x^2 - 2y^2 = 1$ s'écrit $(x - y\sqrt{2})(x + y\sqrt{2}) = 1$, donc $x - y\sqrt{2} = \frac{1}{x + y\sqrt{2}} > 0$. En divisant par y :

$$0 < \frac{x}{y} - \sqrt{2} = \frac{1}{y(x + y\sqrt{2})}$$

— Comme $x > y\sqrt{2}$, on a $x + y\sqrt{2} > 2y\sqrt{2} > 2y$, d'où $\frac{x}{y} - \sqrt{2} < \frac{1}{y \times 2y} = \frac{1}{2y^2}$.

— Approximations de $\sqrt{2} \approx 1,414213\,56$: $\frac{3}{2} = 1,5$; $\frac{17}{12} \approx 1,416\,67$; $\frac{99}{70} \approx 1,414\,29$; $\frac{577}{408} \approx 1,414\,216$: erreur $< 3 \times 10^{-6}$ ✓ (borne $\frac{1}{2 \times 408^2} \approx 3 \times 10^{-6}$).

Réponse. Solutions $(3, 2)$, $(17, 12)$, $(99, 70)$, $(577, 408)$; $0 < \frac{x}{y} - \sqrt{2} < \frac{1}{2y^2}$.

Correction de l'exercice 8 - Factoriser une équation produit

a) On regroupe et on ajoute la constante qui permet de factoriser :

$$xy - 2x - 3y = 0 \Leftrightarrow xy - 2x - 3y + 6 = 6 \Leftrightarrow (x - 3)(y - 2) = 6$$

— Les couples de diviseurs de 6 (**positifs et négatifs**) :

$(1, 6), (2, 3), (3, 2), (6, 1), (-1, -6), (-2, -3), (-3, -2), (-6, -1)$.

— Solutions $(x, y) = (x' + 3, y' + 2)$: $(4, 8), (5, 5), (6, 4), (9, 3), (2, -4), (1, -1), (0, 0), (-3, 1)$.

— **Vérification** : $(5, 5)$: $25 = 10 + 15$ ✓ ; $(-3, 1)$: $-3 = -6 + 3$ ✓

b) Strictement positives : $(4, 8), (5, 5), (6, 4), (9, 3)$.

c) $(x - 5)(y - 5) = 25$. Dans $\mathbb{N}^2$: facteurs $(1, 25), (5, 5), (25, 1)$ donnent $(6, 30), (10, 10), (30, 6)$; facteurs négatifs $(-5, -5)$ donnent $(0, 0)$; $(-1, -25)$ donnerait $y = -20$, exclu.

— Solutions : $(0, 0), (6, 30), (10, 10), (30, 6)$.

d) $xy = 2(x + y) \Leftrightarrow (x - 2)(y - 2) = 4$ avec $x, y \geq 1$: $(x - 2, y - 2) \in \{(1, 4), (2, 2), (4, 1)\}$ (les facteurs négatifs donneraient x ou $y \leq 0$ sauf $(-1, -4)$, qui donne $y = -2$).

— Rectangles 3×6 et 4×4 . **Vérification** : $3 \times 6 = 18 = 2(3 + 6) \checkmark$; $4 \times 4 = 16 = 2 \times 8 \checkmark$

Réponse. $(x - 3)(y - 2) = 6$: 8 solutions ; en c) $(0, 0)$, $(6, 30)$, $(10, 10)$, $(30, 6)$; rectangles 3×6 et 4×4 .

Correction de l'exercice 9 - Théorème chinois sans coprimauté

a) $x \equiv 5 \pmod{8}$: $x = 5 + 8t$. On reporte : $5 + 8t \equiv 3 \pmod{6}$, soit $8t \equiv -2$, soit $2t \equiv 4 \pmod{6}$.

— On divise **tout** par 2 : $t \equiv 2 \pmod{3}$, $t = 2 + 3s$, et $x = 5 + 16 + 24s = 21 + 24s$.

$$x \equiv 21 \pmod{24}$$

— **Vérification** : $21 = 3 \times 6 + 3 \checkmark$; $21 = 2 \times 8 + 5 \checkmark$ Le module final est $\text{ppcm}(6, 8) = 24$, et non 48.

b) $x \equiv 1 \pmod{6}$ impose x **impair** ; $x \equiv 2 \pmod{8}$ impose x **pair**. Incompatible.

— En termes de c) : $\text{pgcd}(6, 8) = 2$ ne divise pas $1 - 2 = -1$.

c) et **d)** Soit $d = \text{pgcd}(m, n)$. Si x est solution, $d \mid m \mid x - a$ et $d \mid n \mid x - b$, donc d divise la différence $(x - b) - (x - a) = a - b$: c'est la condition nécessaire.

— (Réciproquement, par Bézout $mu + nv = d$; si $a - b = dk$, alors $x = a - muk$ convient : $x \equiv a \pmod{m}$ et $x = a - (d - nv)k = b + nvk \equiv b \pmod{n}$.)

— Deux solutions diffèrent d'un multiple commun de m et n , donc d'un multiple de $\text{ppcm}(m, n)$.

— **Contrôle** en a) : $d = 2 \mid 3 - 5 = -2 \checkmark$

Réponse. a) $x \equiv 21 \pmod{24}$; b) aucune solution (parité) ; condition : $\text{pgcd}(m, n) \mid a - b$.

Correction de l'exercice 10 - Puissances de 2 et de 3

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

b) $y \geq 1$: $2^x = 1 + 3^y \equiv 1 \pmod{3}$. Or $2 \equiv -1$, donc $2^x \equiv (-1)^x$, qui vaut 1 si et seulement si x est **pair**.

c) Avec $x = 2m$ (et $m \geq 1$ car $2^x > 1$) :

$$3^y = 2^{2m} - 1 = (2^m - 1)(2^m + 1)$$

— Par unicité de la décomposition, chaque facteur est une puissance de 3 : $2^m - 1 = 3^\alpha$ et $2^m + 1 = 3^\beta$, avec $\beta > \alpha$ et $3^\beta - 3^\alpha = 2$.

d) Si $\alpha \geq 1$, alors 3 divise $3^\beta - 3^\alpha = 2$: impossible. Donc $\alpha = 0$, $2^m - 1 = 1$, $m = 1$, puis $2^m + 1 = 3 = 3^1$.

— On obtient $x = 2$, $y = 1$: $4 - 3 = 1 \checkmark$

— **Solutions** : $(1, 0)$ et $(2, 1)$.

— **Culture** : c'est un cas particulier de la conjecture de **Catalan** (démontrée par Mihăilescu en 2002) : $8 = 2^3$ et $9 = 3^2$ sont les seules puissances consécutives.

Réponse. Solutions $(x, y) = (1, 0)$ et $(2, 1)$.

Correction de l'exercice 11 - Descente infinie

a) Un carré vaut 0 ou 1 modulo 3. $x^2 + y^2 \equiv 0$ impose $x^2 \equiv y^2 \equiv 0$ (les autres sommes valent 1 ou 2), donc $3 \mid x$ et $3 \mid y$ (3 premier).

b) $3 \mid 3z^2 = x^2 + y^2$: par a), $x = 3x'$ et $y = 3y'$. Alors

$$9x'^2 + 9y'^2 = 3z^2 \Leftrightarrow z^2 = 3(x'^2 + y'^2)$$

— Donc $3 \mid z^2$, puis $3 \mid z$; avec $z = 3z'$: $9z'^2 = 3(x'^2 + y'^2)$, soit $x'^2 + y'^2 = 3z'^2$: (x', y', z') est solution.

c) Supposons une solution non nulle ; on choisit celle pour laquelle $|x| + |y| + |z| > 0$ est **minimal**. Par b), $(\frac{x}{3}, \frac{y}{3}, \frac{z}{3})$ est une solution non nulle de somme **trois fois plus petite** : contradiction avec la minimalité.

— La seule solution est $(0, 0, 0)$.

d) Si $(\frac{a}{b}, \frac{c}{b})$ (même dénominateur $b \geq 1$) vérifiait $X^2 + Y^2 = 3$, alors $a^2 + c^2 = 3b^2$ avec $b \neq 0$: impossible par c).

— **Remarque** : le cercle $X^2 + Y^2 = 2$ contient, lui, une infinité de points rationnels (par exemple $(1, 1)$ et $(\frac{1}{5}, \frac{7}{5})$) ; la réponse dépend de l'arithmétique du rayon au carré.

Réponse. Seule solution $(0, 0, 0)$ (descente) ; aucun point rationnel sur $X^2 + Y^2 = 3$.

Correction de l'exercice 12 - Compter les décompositions

a) $2a = 100 - 5b$ doit être **pair** et positif : b pair et $5b \leq 100$, soit $b \in \{0, 2, 4, \dots, 20\}$.

— Chaque b donne un unique $a = \frac{100 - 5b}{2}$: 11 façons (de 50 pièces à 20 billets).

b) Pour b fixé, $a = \frac{n - 5b}{2}$ est un entier naturel si et seulement si $5b \leq n$ et $n - 5b$ est pair, c'est-à-dire $b \equiv n \pmod{2}$ (car $5b \equiv b$).

$$N_n = \text{card} \left\{ b \in \left\{ 0, \dots, \left\lfloor \frac{n}{5} \right\rfloor \right\} : b \equiv n \pmod{2} \right\}$$

— où N_n désigne le nombre de solutions.

c) $n = 101$: b impair, $b \leq 20$: $b \in \{1, 3, \dots, 19\}$, soit 10 façons.

— $n = 3$: $b \leq 0$ et b impair : **aucune**.

d) D'après Frobenius ($2 \wedge 5 = 1$), le plus grand montant impossible est $2 \times 5 - 2 - 5 = 3$. Les montants impossibles sont 1 et 3 (il y en a $\frac{(2-1)(5-1)}{2} = 2$).

— **Contrôle** : 2, 4 = 2 + 2, 5, 6, 7 = 2 + 5 sont possibles, puis on ajoute des pièces de 2.

Réponse. 11 façons pour 100 ; 10 pour 101, 0 pour 3 ; montants impossibles : 1 et 3.

Correction de l'exercice 13 - Les marins et les noix de coco

a) Le marin retire 1 noix (le singe), puis un tiers de $T - 1$; il reste les deux tiers de $T - 1$:

$$T = \frac{2}{3}(T - 1)$$

b) $T + 2 = \frac{2T - 2 + 6}{3} = \frac{2(T + 2)}{3}$ ✓ La quantité $T + 2$ est simplement multipliée par $\frac{2}{3}$: c'est le changement de variable qui **linéarise** le problème.

c) Après trois marins, le tas T_3 vérifie $T_3 + 2 = \left(\frac{2}{3}\right)^3 (N + 2) = \frac{8M}{27}$.

— Pour que T_3 soit entier, $27 \mid 8M$, donc $27 \mid M$ (Gauss, $27 \wedge 8 = 1$).

— Le matin, $T_3 \equiv 1 \pmod{3}$, soit $T_3 + 2 \equiv 0 \pmod{3}$: $3 \mid \frac{8M}{27}$, donc $81 \mid 8M$, puis $3^4 = 81 \mid M$.

d) Le plus petit M est 81, d'où $N = 79$.

- **Vérification** : $79 = 3 \times 26 + 1$, il reste 52 ; $52 = 3 \times 17 + 1$, il reste 34 ;
 $34 = 3 \times 11 + 1$, il reste 22 ; au matin $22 = 3 \times 7 + 1$ ✓ Chacun reçoit encore 7 noix.
- Les solutions sont $N = 81k - 2$ (79, 160, ...). **Version à cinq marins** (Williams, 1926) :
 même méthode avec $M = N + 4$ et $5^6 \mid M$, d'où $N = 15\,621$.

Réponse. $T + 2$ est multiplié par $\frac{2}{3}$ à chaque passage ; $81 \mid N + 2$; plus petit $N = 79$.

Correction de l'exercice 14 - Points entiers d'un segment

a) Les points du segment sont $(ta; tb)$ avec $t \in [0; 1]$. Écrivons $a = da'$, $b = db'$ avec $a' \wedge b' = 1$.

- Si ta et tb sont entiers, alors t est rationnel ; $x = ta$ et $y = tb$ vérifient $b'x = a'y$ (car $\frac{x}{a} = \frac{y}{b}$ donne $bx = ay$, puis on divise par d).
- Par **Gauss**, $a' \mid b'x$ et $a' \wedge b' = 1$ donnent $a' \mid x$: $x = ka'$, puis $y = kb'$, avec $0 \leq x \leq a$, soit $0 \leq k \leq d$.

$$(x; y) = \left(\frac{ka}{d}; \frac{kb}{d} \right), \quad 0 \leq k \leq d$$

b) Les valeurs $k = 0, 1, \dots, d$ donnent des points distincts : $d + 1$ points.

c) $P(12; 8)$: $d = 4$, donc 5 points : $(0; 0)$, $(3; 2)$, $(6; 4)$, $(9; 6)$, $(12; 8)$ ✓ (figure).

— $P(1\,769; 551)$: $d = 29$ (plaquette 2), donc 30 points, espacés de $(61; 19)$.

d) Formule : $12 + 8 - 4 = 16$ carreaux.

- **Justification** : entre O et P , la diagonale franchit 11 lignes verticales intérieures ($x = 1$ à 11) et 7 horizontales ($y = 1$ à 7), et entre à chaque franchissement dans un nouveau carreau ; aux $d - 1 = 3$ points intérieurs du réseau, elle franchit deux lignes à la fois et n'entre que dans **un** nouveau carreau. Total : $1 + 11 + 7 - 3 = 16$ ✓
- **Petit cas** : un sol 2×1 : $2 + 1 - 1 = 2$ carreaux ✓ ; un sol 2×2 : la diagonale passe par le coin central, $2 + 2 - 2 = 2$ carreaux ✓

Réponse. $d + 1$ points du réseau (5 pour $(12; 8)$, 30 pour $(1\,769; 551)$) ; la diagonale 12×8 traverse 16 carreaux.

Correction de l'exercice 15 - Synthèse : racines carrées de 1 modulo 105

a) 3, 5, 7 sont deux à deux premiers entre eux : $105 \mid x^2 - 1$ si et seulement si 3, 5 et 7 divisent $x^2 - 1$ (corollaire de Gauss).

b) Modulo un premier p , $x^2 \equiv 1 \Leftrightarrow x \equiv \pm 1$ (lemme d'Euclide, plaquette 3) :

— modulo 3 : $x \equiv \pm 1$; modulo 5 : $x \equiv \pm 1$; modulo 7 : $x \equiv \pm 1$.

c) Chaque choix de signes $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ donne, par le théorème chinois, une unique solution modulo 105 : $2^3 = 8$ solutions.

$$x \equiv 70\varepsilon_1 + 21\varepsilon_2 + 15\varepsilon_3 \pmod{105}$$

- $(+, +, +)$: $106 \equiv 1$; $(-, -, -)$: $-1 \equiv 104$;
- $(+, +, -)$: 76 ; $(+, -, +)$: 64 ; $(-, +, +)$: $-34 \equiv 71$;
- $(+, -, -)$: 34 ; $(-, +, -)$: $-64 \equiv 41$; $(-, -, +)$: $-76 \equiv 29$.
- Solutions : 1, 29, 34, 41, 64, 71, 76, 104. **Vérification** : $29^2 = 841 = 8 \times 105 + 1$ ✓ ;
 $34^2 = 1\,156 = 11 \times 105 + 1$ ✓

d) Avec $x = 29$: $x^2 - 1 = (x - 1)(x + 1) = 28 \times 30$ est multiple de 105, mais ni 28 ni 30 ne l'est. Donc $\text{pgcd}(28, 105) = 7$ et $\text{pgcd}(30, 105) = 15$ sont des **diviseurs non triviaux** :
 $105 = 7 \times 15$.

- **Intérêt** : savoir extraire des racines carrées modulo n permettrait de **factoriser** n .
C'est pourquoi la sécurité de certains cryptosystèmes (Rabin, RSA) repose sur la difficulté de ces deux problèmes, qui sont liés.

Réponse. 8 solutions : 1, 29, 34, 41, 64, 71, 76, 104 ; $\text{pgcd}(28, 105) = 7$ factorise $105 = 7 \times 15$.