Plaquette 1 – PGCD, Bézout, congruences et théorème chinois

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

Corrections détaillées

Boîte à outils

Théorèmes du cours.

— **Division euclidienne** : pour $a \in \mathbb{Z}$ et $b \in \mathbb{N}^*$, il existe un unique couple (q, r) avec $a = bq + r$ et $0 \leq r < b$.

— **Algorithme d'Euclide** : $\text{pgcd}(a, b) = \text{pgcd}(b, r)$ — on itère jusqu'à un reste nul.

— **Théorème de Bézout** : a et b sont **premiers entre eux** si et seulement s'il existe $u, v \in \mathbb{Z}$ tels que

$$au + bv = 1$$

— **Identité de Bézout générale** : il existe toujours u, v tels que $au + bv = \text{pgcd}(a, b)$.

— **Théorème de Gauss** : si $a \mid bc$ et $\text{pgcd}(a, b) = 1$, alors $a \mid c$.

— **Lemme d'Euclide** : si p est premier et $p \mid ab$, alors $p \mid a$ ou $p \mid b$.

— **Congruences** : $a \equiv b \pmod{n}$ signifie $n \mid (a - b)$. Les congruences sont compatibles avec l'addition, la multiplication et les puissances — **mais pas avec la division**.

— **Petit théorème de Fermat** : si p est premier et $p \nmid a$, alors

$$a^{p-1} \equiv 1 \pmod{p}$$

— **Théorème chinois** : si m et n sont premiers entre eux, le système $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ admet une unique solution modulo mn.

— **Décomposition en facteurs premiers** : unique à l'ordre près ; le PGCD prend le **min** des exposants, le PPCM le **max**, avec $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|$.

Correction de l'exercice 1 – Algorithme d'Euclide

On enchaîne les divisions euclidiennes.

— $1071 = 2 \times 462 + 147$

— $462 = 3 \times 147 + 21$

— $147 = 7 \times 21 + 0$

— Le dernier reste non nul est 21 : $\text{pgcd}(1071, 462) = 21$.

— **Contrôle par décomposition** : $1071 = 3 \times 7 \times 51 = 3^2 \times 7 \times 17$ et $462 = 2 \times 3 \times 7 \times 11$. Facteurs communs : $3 \times 7 = 21$. Cohérent.

— **Efficacité** : trois divisions seulement, alors que la décomposition en facteurs premiers est coûteuse pour de grands nombres — c'est tout l'intérêt d'Euclide.

Réponse. 21.

Correction de l'exercice 2 – Relation de Bézout

Euclide : $17 = 3 \times 5 + 2$, puis $5 = 2 \times 2 + 1$, puis $2 = 2 \times 1$.

— Le PGCD vaut 1 : les nombres sont premiers entre eux, Bézout s'applique.

— **Remontée** : $1 = 5 - 2 \times 2$, et $2 = 17 - 3 \times 5$, donc

$$1 = 5 - 2(17 - 3 \times 5) = 5 - 2 \times 17 + 6 \times 5 = 7 \times 5 - 2 \times 17$$

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).

— **Solution** : $u = -2$ et $v = 7$.
— **Vérification** : $17 \times (-2) + 5 \times 7 = -34 + 35 = 1$. Cohérent.
— **Non-unicité** : $(u, v) = (-2 + 5k,\ 7 - 17k)$ convient pour tout $k \in \mathbb{Z}$; par exemple $(3, -10)$.

Réponse. $u = -2$, $v = 7$ (à $(5k, -17k)$ près).

Correction de l'exercice 3 – Équation diophantienne

Solution particulière : $\text{pgcd}(7, 11) = 1$, donc il y a des solutions.
— Par tâtonnement ou Euclide : $7 \times (-3) + 11 \times 2 = -21 + 22 = 1$. Donc $(x_0, y_0) = (-3, 2)$.
— **Solution générale** : on soustrait les deux égalités $7x + 11y = 1$ et $7x_0 + 11y_0 = 1$:

$$7(x - x_0) = -11(y - y_0)$$

— 7 divise $11(y_0 - y)$ et $\text{pgcd}(7, 11) = 1$, donc par **Gauss** $7 \mid (y_0 - y)$: on écrit $y = y_0 - 7k$, d'où $x = x_0 + 11k$.
— **Ensemble des solutions** : $(x, y) = (-3 + 11k,\ 2 - 7k)$, $k \in \mathbb{Z}$.
— **Contrôle** avec $k = 1$: $(8, -5)$ et $7 \times 8 + 11 \times (-5) = 56 - 55 = 1$. Cohérent.

Réponse. $(x, y) = (-3 + 11k,\ 2 - 7k)$, $k \in \mathbb{Z}$.

Correction de l'exercice 4 – Congruences et critère de divisibilité

On travaille **modulo 5**.

— $7 \equiv 2 \pmod 5$, donc $7^{100} \equiv 2^{100} \pmod 5$.
— On cherche le **cycle** des puissances de 2 : $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 3$, $2^4 \equiv 1 \pmod 5$.
— Le cycle est de longueur 4. Comme $100 = 4 \times 25$, on a $2^{100} = \left(2^4\right)^{25} \equiv 1^{25} = 1 \pmod 5$.
— **Reste** : 1.
— **Contrôle par Fermat** : 5 est premier et $5 \nmid 7$, donc $7^4 \equiv 1 \pmod 5$; comme $4 \mid 100$, on conclut directement. Cohérent.

Réponse. Le reste est 1.

Correction de l'exercice 5 – Petit théorème de Fermat

Fermat : 7 est premier et ne divise pas 3, donc $3^6 \equiv 1 \pmod 7$.
— On réduit l'exposant modulo 6 : $1000 = 6 \times 166 + 4$.
— Donc $3^{1000} = \left(3^6\right)^{166} \times 3^4 \equiv 3^4 \pmod 7$.
— $3^4 = 81 = 7 \times 11 + 4$, donc $3^{1000} \equiv 4 \pmod 7$.
— **Contrôle du cycle** : $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$, $3^5 \equiv 5$, $3^6 \equiv 1$. Le cycle est bien de longueur 6 et la 4^{e} valeur est 4. Cohérent.
— **Réflexe** : réduire l'exposant modulo $p - 1$, jamais modulo p.

Réponse. Le reste est 4.

Correction de l'exercice 6 – Divisibilité par récurrence

Méthode 1 — congruences (la plus rapide).
— $4 \equiv 1 \pmod 3$, donc $4^n \equiv 1^n = 1 \pmod 3$.
— Ainsi $4^n + 5 \equiv 1 + 5 = 6 \equiv 0 \pmod 3$. **Conclusion** : $3 \mid 4^n + 5$.

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).

Méthode 2 — récurrence.

— **Initialisation** : $n = 0$ donne $1 + 5 = 6 = 3 \times 2$. Vrai.
— **Hérédité** : supposons $4^n + 5 = 3k$. Alors

$$4^{n+1} + 5 = 4 \times 4^n + 5 = 4(3k - 5) + 5 = 12k - 15 = 3(4k - 5)$$

— C'est bien un multiple de 3.
— **Contrôle** : $n = 1$ donne 9, $n = 2$ donne 21, $n = 3$ donne 69 — tous multiples de 3.

Réponse. $4 \equiv 1 \pmod 3$ donc $4^n + 5 \equiv 6 \equiv 0 \pmod 3$.

Correction de l'exercice 7 – Théorème chinois

3 et 5 sont premiers entre eux : le **théorème chinois** garantit une unique solution modulo 15.

— De la première congruence : $x = 2 + 3k$.
— On reporte dans la seconde : $2 + 3k \equiv 3 \pmod 5$, donc $3k \equiv 1 \pmod 5$.
— **Inverse de 3 modulo 5** : $3 \times 2 = 6 \equiv 1$, donc l'inverse est 2. D'où $k \equiv 2 \pmod 5$, soit $k = 2 + 5m$.
— Alors $x = 2 + 3(2 + 5m) = 8 + 15m$.
— **Solution** : $x \equiv 8 \pmod{15}$.
— **Vérification** : $8 = 2 \times 3 + 2$ donc $8 \equiv 2 \pmod 3$; $8 = 5 + 3$ donc $8 \equiv 3 \pmod 5$. Cohérent.

Réponse. $x \equiv 8 \pmod{15}$.

Correction de l'exercice 8 – PGCD et PPCM

On pose $a = 12a'$ et $b = 12b'$ avec $\text{pgcd}(a', b') = 1$.

— La condition devient $12(a' + b') = 84$, donc $a' + b' = 7$.
— Les couples avec $a' + b' = 7$: $(1, 6)$, $(2, 5)$, $(3, 4)$ et leurs symétriques. Tous sont formés d'entiers premiers entre eux (leur somme étant 7, premier, tout diviseur commun diviserait 7).
— **Solutions** : $(a, b) \in \{(12, 72), (24, 60), (36, 48)\}$ et les couples symétriques.
— **Vérification** pour $(24, 60)$: somme 84 ; $24 = 2^3 \times 3$, $60 = 2^2 \times 3 \times 5$, PGCD $= 2^2 \times 3 = 12$. Cohérent.
— **Attention au piège** : $(a', b') = (0, 7)$ donnerait pgcd $= 84 \neq 12$ — il faut bien exclure 0.

Réponse. $(12, 72)$, $(24, 60)$, $(36, 48)$ (et symétriques).

Correction de l'exercice 9 – Nombres premiers entre eux

Méthode 1 — Bézout explicite.

— On remarque que $1 \times (2n + 1) - 2 \times (n + 1) = 2n + 1 - 2n - 2 = -1$.
— Une combinaison linéaire entière valant -1 (donc ± 1) prouve que les deux nombres sont **premiers entre eux**.

Méthode 2 — Euclide.

— $2n + 1 = 1 \times (n + 1) + n$, puis $n + 1 = 1 \times n + 1$, puis $n = n \times 1 + 0$.
— Dernier reste non nul : 1. Même conclusion.
— **Contrôle** : $n = 5$ donne $\text{pgcd}(11, 6) = 1$; $n = 10$ donne $\text{pgcd}(21, 11) = 1$. Cohérent.
— **Réflexe** : pour prouver que deux expressions en n sont premières entre elles, chercher une **combinaison linéaire constante** égale à ± 1.

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. $1 \times (2n+1) - 2 \times (n+1) = -1$: Bézout conclut.

Correction de l'exercice 10 – Infinité des nombres premiers

Raisonnement par l'absurde. Supposons qu'il n'y ait qu'un nombre fini de premiers $p_1, \dots, p_r$.

— On pose $N = p_1 p_2 \cdots p_r + 1$. Comme $N \geq 3$, il admet au moins un **diviseur premier** p (tout entier ≥ 2 en admet un : son plus petit diviseur > 1).
— Ce p figure dans la liste, donc p divise le produit $p_1 \cdots p_r$.
— Or p divise aussi N. Par différence, p divise $N - p_1 \cdots p_r = 1$.
— Un nombre premier vaut au moins 2 : il ne peut pas diviser 1. **Contradiction.**
— **Conclusion** : l'ensemble des nombres premiers est **infini**.
— **Attention** : le raisonnement ne dit pas que N est premier. Par exemple $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$ n'est pas premier, mais ses facteurs sont bien absents de la liste.

Réponse. Absurde : un facteur premier de $p_1 \cdots p_r + 1$ diviserait 1.

Correction de l'exercice 11 – Congruences et dernier chiffre

Le chiffre des unités est le reste **modulo 10**.

— Cycle des puissances de 2 modulo 10 : 2, 4, 8, 6, 2, 4, … — période 4 à partir de l'exposant 1.
— On réduit l'exposant : $2026 = 4 \times 506 + 2$.
— Le reste étant 2, on est au **deuxième** terme du cycle : le chiffre des unités est 4.
— **Contrôle** : $2^2 = 4$, $2^6 = 64$, $2^{10} = 1024$ — tous finissent par 4, et leurs exposants sont bien congrus à 2 modulo 4. Cohérent.
— **Piège** : il n'y a pas de terme d'exposant 0 dans le cycle ($2^0 = 1$ est hors cycle) ; d'où l'importance de bien repérer où commence la périodicité.

Réponse. Le chiffre des unités est 4.

Correction de l'exercice 12 – Euclide étendu en tableau

a) L'algorithme d'Euclide **étendu** tient, pour chaque reste, ses coefficients de Bézout. On part de $r_0 = a$ avec $(1, 0)$ et $r_1 = b$ avec $(0, 1)$, puis on applique à chaque ligne la même relation que pour les restes :

$$r_{k+1} = r_{k-1} - q_k r_k, \qquad (u_{k+1}, v_{k+1}) = (u_{k-1}, v_{k-1}) - q_k (u_k, v_k)$$

— $2024 = 1 \times 1155 + 869$: 869 a pour coefficients $(1, 0) - 1 \times (0, 1) = (1, -1)$;
— $1155 = 1 \times 869 + 286$: $(0, 1) - 1 \times (1, -1) = (-1, 2)$;
— $869 = 3 \times 286 + 11$: $(1, -1) - 3 \times (-1, 2) = (4, -7)$;
— $286 = 26 \times 11 + 0$: on s'arrête.

Le dernier reste non nul est $d = 11$.

b) La ligne du reste 11 donne directement $u = 4$, $v = -7$. Vérification : $2024 \times 4 - 1155 \times 7 = 8096 - 8085 = 11$ ✓.

c) $33 = 3 \times 11$ est un multiple de d : l'équation a des solutions. On divise par 11 : $184x + 105y = 3$, avec $\text{pgcd}(184, 105) = 1$.

— Solution particulière : $3 \times (4, -7) = (12, -21)$.
— Par différence, $184(x - 12) = -105(y + 21)$; 184 divise $105(y + 21)$ et $184 \wedge 105 = 1$, donc par **Gauss** $y + 21 = -184k$, puis $x - 12 = 105k$.

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).

Ensemble des solutions : $(x, y) = (12 + 105k,\ -21 - 184k)$, $k \in \mathbb{Z}$. Contrôle $k = 0$: $2024 \times 12 - 1155 \times 21 = 24288 - 24255 = 33$ ✓.

Piège : on divise par d **avant** d'écrire la solution générale ; garder 1155 et 2024 comme pas donnerait seulement une solution sur onze.

Réponse. $d = 11 = 4 \times 2024 - 7 \times 1155$; $(x, y) = (12 + 105k,\ -21 - 184k)$, $k \in \mathbb{Z}$.

Correction de l'exercice 13 – Somme et produit premiers entre eux

a) Un entier divise a et $a + b$ si et seulement s'il divise a et b : dans un sens $b = (a + b) - a$, dans l'autre $a + b$ est une somme de multiples. Les deux couples ont donc **les mêmes diviseurs communs**, et le même plus grand :

$$\text{pgcd}(a, a + b) = \text{pgcd}(a, b)$$

b) Par l'absurde, supposons $ab \wedge (a + b) > 1$: il admet un diviseur premier p.

— $p \mid ab$, donc par le **lemme d'Euclide** $p \mid a$ ou $p \mid b$; par symétrie, disons $p \mid a$.
— $p \mid a + b$ et $p \mid a$, donc $p \mid b$.
— p divise alors $a \wedge b = 1$: impossible.

Donc $ab \wedge (a + b) = 1$.

c) Numérateur $a + b$ et dénominateur ab sont premiers entre eux d'après b) : la fraction est irréductible. Exemple : $\frac{1}{3} + \frac{1}{5} = \frac{5+3}{15} = \frac{8}{15}$, et $8 \wedge 15 = 1$ ✓.

Piège : l'hypothèse $a \wedge b = 1$ est indispensable. Pour $a = 2$, $b = 6$: $\frac{8}{12}$ se simplifie par 4.

Réponse. $\text{pgcd}(a, a + b) = \text{pgcd}(a, b)$; si $a \wedge b = 1$, alors $ab \wedge (a + b) = 1$.

Correction de l'exercice 14 – PGCD de deux expressions en n

a) On écrit $n^2 + 1 = (n + 2)(n - 2) + 5$ (développer : $n^2 - 4 + 5$). On applique la propriété qui fonde l'algorithme d'Euclide :

$$\text{pgcd}(a, b) = \text{pgcd}(b,\ a - qb) \quad \text{pour tout } q \in \mathbb{Z}$$

— avec $a = n^2 + 1$, $b = n + 2$, $q = n - 2$: $d_n = \text{pgcd}(n + 2, 5)$.

Ce n'est pas une division euclidienne d'entiers au sens strict (le « reste » 5 peut dépasser $n + 2$ pour $n \leq 2$), mais la propriété ne demande qu'une égalité $a = qb + r$ avec q entier.

b) d_n divise 5, qui est premier : $d_n \in \{1, 5\}$.

c) $d_n = 5 \Leftrightarrow 5 \mid n + 2 \Leftrightarrow n \equiv 3 \pmod 5$.

— $n = 3$: $n^2 + 1 = 10$, $n + 2 = 5$, $d_3 = 5$ ✓ ;
— $n = 8$: 65 et 10, $d_8 = 5$ ✓ ;
— contre-exemple $n = 4$: 17 et 6, $d_4 = 1$ ✓.

Réflexe : pour un PGCD d'expressions en n, éliminer n par combinaisons jusqu'à une **constante** ; seuls ses diviseurs sont possibles.

Réponse. $d_n = \text{pgcd}(n + 2, 5) \in \{1, 5\}$; $d_n = 5 \Leftrightarrow n \equiv 3 \pmod 5$.

Correction de l'exercice 15 – Synthèse : équation modulaire

Étape 1 : 5 est-il inversible modulo 12 ? $\text{pgcd}(5, 12) = 1$, donc oui.

— On cherche l'inverse : $5 \times 5 = 25 = 2 \times 12 + 1$, donc $5^{-1} \equiv 5 \pmod{12}$.
— **Étape 2** : on multiplie les deux membres par 5 :

$$25x \equiv 15 \pmod{12} \implies x \equiv 3 \pmod{12}$$

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).

— **Solution** : $x \equiv 3 \pmod{12}$, c'est-à-dire $x \in \{\ldots, -9, 3, 15, 27, \ldots\}$.
— **Vérification** : $5 \times 3 = 15 = 12 + 3 \equiv 3 \pmod{12}$. Cohérent.
— **Cas à connaître** : si $\text{pgcd}(a, n) = d > 1$, l'équation $ax \equiv b \pmod{n}$ n'a de solution que si $d \mid b$, et elle en a alors exactement d modulo n. Par exemple $6x \equiv 3 \pmod{12}$ n'a **aucune** solution, car $\text{pgcd}(6, 12) = 6$ ne divise pas 3.

Réponse. $x \equiv 3 \pmod{12}$.

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).