

Plaquette 1 - Division euclidienne, PGCD, Bézout et congruences

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

Corrections détaillées

Boîte à outils

Division euclidienne. Pour $a \in \mathbb{Z}$, $b \in \mathbb{N}^*$, il existe un **unique** couple (q, r) avec

$$a = bq + r, \quad 0 \leq r < b$$

PGCD.

- **Algorithme d'Euclide** : $\text{pgcd}(a, b) = \text{pgcd}(b, r)$, itéré jusqu'à un reste nul.
- **Bézout** : il existe u, v tels que $au + bv = \text{pgcd}(a, b)$.
- a et b sont **premiers entre eux** $\Leftrightarrow \exists u, v, au + bv = 1$.
- **Gauss** : si $a \mid bc$ et $a \wedge b = 1$, alors $a \mid c$.
- $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|$.

Nombres premiers.

- Tout entier ≥ 2 se décompose de **façon unique** en produit de facteurs premiers.
- **PGCD et PPCM** se lisent sur les décompositions : **min** et **max** des exposants.
- n est premier si aucun premier $\leq \sqrt{n}$ ne le divise.
- **Euclide** : il y a une **infinité** de nombres premiers.

Congruences. $a \equiv b \pmod{n}$ signifie $n \mid (a - b)$.

- Compatible avec l'addition, la multiplication et les **puissances** ; **pas** avec la division.
- **Petit théorème de Fermat** : p premier et $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$.
- **Inversibles modulo n** : les classes $\bar{k}$ avec $k \wedge n = 1$; leur nombre est $\varphi(n)$.
- **Théorème chinois** : si $m \wedge n = 1$, le système $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ a une unique solution modulo mn .
- **Équation** $ax \equiv b \pmod{n}$: soluble $\Leftrightarrow (a \wedge n) \mid b$.

Correction de l'exercice 1 - Division euclidienne

- **Contrainte** : il faut $-47 = 6q + r$ avec $0 \leq r < 6$.
- **Piège** : $-47 = 6 \times (-7) - 5$ ne convient **pas** ($r = -5 < 0$).
- On ajuste : $-47 = 6 \times (-8) + 1$, et $0 \leq 1 < 6$ ✓
- **Résultat** : $q = -8$ et $r = 1$.
- **Contrôle** : $6 \times (-8) = -48$, et $-48 + 1 = -47$ ✓
- **Conséquence** : $-47 \equiv 1 \pmod{6}$ — le reste est toujours **positif**, même pour un dividende négatif.
- **Attention aux calculatrices** : beaucoup renvoient -5 pour le reste de -47 par 6 (elles gardent le signe du dividende) ; la définition mathématique impose $r \geq 0$.

Réponse. $q = -8$ et $r = 1$.

Correction de l'exercice 2 - Algorithme d'Euclide

Euclide.

- $1071 = 2 \times 462 + 147$

- $462 = 3 \times 147 + 21$
- $147 = 7 \times 21 + 0$
- **PGCD** : le dernier reste non nul, soit 21.

PPCM. On utilise $\text{pgcd} \times \text{ppcm} = ab$:

$$\text{ppcm} = \frac{462 \times 1071}{21} = \frac{494\,802}{21} = 23\,562$$

- **Contrôle par décomposition** : $462 = 2 \times 3 \times 7 \times 11$ et $1071 = 3^2 \times 7 \times 17$.
- PGCD : $3 \times 7 = 21$ ✓ ; PPCM : $2 \times 3^2 \times 7 \times 11 \times 17 = 23\,562$ ✓
- **Efficacité** : trois divisions pour Euclide, contre une factorisation coûteuse — c'est pourquoi Euclide reste l'algorithme de référence.

Réponse. PGCD = 21 et PPCM = 23 562.

Correction de l'exercice 3 - Relation de Bézout

Euclide.

- $23 = 1 \times 17 + 6$
- $17 = 2 \times 6 + 5$
- $6 = 1 \times 5 + 1$
- $5 = 5 \times 1 + 0$ — le PGCD vaut bien 1.

Remontée.

- $1 = 6 - 5$
- $5 = 17 - 2 \times 6$, donc $1 = 6 - (17 - 2 \times 6) = 3 \times 6 - 17$
- $6 = 23 - 17$, donc $1 = 3(23 - 17) - 17 = 3 \times 23 - 4 \times 17$
- **Solution** : $u = 3$ et $v = -4$.
- **Vérification** : $69 - 68 = 1$ ✓
- **Solutions générales** : $(u, v) = (3 + 17k, -4 - 23k)$ pour $k \in \mathbb{Z}$ — par exemple $(20, -27)$.
- **Application** : $u = 3$ est l'inverse de 23 modulo 17, et $-4 \equiv 19$ l'inverse de 17 modulo 23.

Réponse. $u = 3, v = -4$.

Correction de l'exercice 4 - Équation diophantienne

- **Solubilité** : $\text{pgcd}(5, 8) = 1$ divise 3 — il y a des solutions.
- **Bézout** : $5 \times (-3) + 8 \times 2 = 1$, donc en multipliant par 3 : $5 \times (-9) + 8 \times 6 = 3$.
- **Solution particulière** : $(x_0, y_0) = (-9, 6)$.
- **Solutions générales** : en soustrayant, $5(x - x_0) = -8(y - y_0)$. Comme $5 \wedge 8 = 1$, Gauss donne $5 \mid (y_0 - y)$, d'où

$$(x, y) = (-9 + 8k, 6 - 5k), \quad k \in \mathbb{Z}$$

- **Vérifications** : $k = 0$ donne $(-9, 6)$ et $-45 + 48 = 3$ ✓ ; $k = 2$ donne $(7, -4)$ et $35 - 32 = 3$ ✓
- **Solution « minimale » positive** : $k = 2$ donne $x = 7$; il n'y a pas de solution avec x, y tous deux positifs ici (puisque y décroît).

Réponse. $(x, y) = (-9 + 8k, 6 - 5k), k \in \mathbb{Z}$.

Correction de l'exercice 5 - Nombres premiers

Pour 221. Il suffit de tester les premiers $\leq \sqrt{221} \approx 14,9$, soit 2, 3, 5, 7, 11, 13.

- Non divisible par 2 (impair), 3 (somme 5), 5 (ne finit pas par 0 ou 5), 7 ($221 = 7 \times 31 + 4$), 11 ($221 = 11 \times 20 + 1$).
- Mais $221 = 13 \times 17$ ✓ — **il n'est pas premier**.

Pour 211. On teste les premiers $\leq \sqrt{211} \approx 14,5$.

- 211 est impair ; somme des chiffres 4 (pas divisible par 3) ; ne finit pas par 0/5 ; $211 = 7 \times 30 + 1$; $211 = 11 \times 19 + 2$; $211 = 13 \times 16 + 3$.
- Aucun diviseur : 211 est **premier**.
- **Justification du critère $\sqrt{n}$** : si $n = ab$ avec $a \leq b$, alors $a \leq \sqrt{n}$ — un diviseur non trivial en fournit toujours un petit.
- **Économie** : pour 211, six tests au lieu de 209.

Réponse. $221 = 13 \times 17$ (non premier) ; 211 est premier.

Correction de l'exercice 6 - Congruences et reste

- **Cycle des puissances de 2 modulo 7** : $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 1$.
- Le cycle est de **longueur 3**.
- **Réduction de l'exposant** : $100 = 3 \times 33 + 1$, donc

$$2^{100} = \left(2^3\right)^{33} \times 2 \equiv 1^{33} \times 2 = 2 \pmod{7}$$
- **Reste** : 2.
- **Contrôle par Fermat** : 7 est premier et $7 \nmid 2$, donc $2^6 \equiv 1$; comme $100 = 6 \times 16 + 4$, on a $2^{100} \equiv 2^4 = 16 \equiv 2 \pmod{7}$ ✓ — même résultat.
- **Remarque** : l'ordre réel de 2 modulo 7 est 3, qui **divise** $6 = p - 1$ — conforme au théorème de Lagrange.

Réponse. Le reste est 2.

Correction de l'exercice 7 - Critère de divisibilité

Écrivons $N = \sum_{k=0}^p a_k 10^k$ où les a_k sont les chiffres.

- **Observation clé** : $10 \equiv 1 \pmod{9}$, donc $10^k \equiv 1^k = 1$ pour tout k .
- **Conséquence** :

$$N \equiv \sum_k a_k \pmod{9}$$

- Donc $9 \mid N$ **si et seulement si** 9 divise la somme des chiffres ✓
- **Exemple** : $N = 4752$, somme $4 + 7 + 5 + 2 = 18$, divisible par 9 — et $4752 = 9 \times 528$ ✓
- **Même preuve pour 3** : $10 \equiv 1 \pmod{3}$ également.
- **Critère par 11** : $10 \equiv -1 \pmod{11}$, donc N est congru à la **somme alternée** de ses chiffres. Exemple : $4752 \rightarrow -4 + 7 - 5 + 2 = 0$, donc $11 \mid 4752$ ✓ (en effet $4752 = 11 \times 432$).

Réponse. $10^k \equiv 1 \pmod{9}$, donc $N \equiv$ somme des chiffres.

Correction de l'exercice 8 - Théorème chinois

- **Système** : $x \equiv 2 \pmod{5}$ et $x \equiv 3 \pmod{7}$, avec $5 \wedge 7 = 1$ — le **théorème chinois** garantit une unique solution modulo 35.
- De la première : $x = 2 + 5k$.
- **Report** : $2 + 5k \equiv 3 \pmod{7}$, donc $5k \equiv 1 \pmod{7}$.

- **Inverse de 5 modulo 7** : $5 \times 3 = 15 \equiv 1$, donc $k \equiv 3 [7]$, soit $k = 3 + 7m$.
- **Conclusion** : $x = 2 + 5(3 + 7m) = 17 + 35m$, donc $x \equiv 17 \pmod{35}$.
- **Vérifications** : $17 = 3 \times 5 + 2 \checkmark$ et $17 = 2 \times 7 + 3 \checkmark$
- **Interprétation** : les restes modulo 5 et modulo 7 déterminent **complètement** le reste modulo 35 — c'est le principe des systèmes de numération résiduels utilisés en cryptographie.

Réponse. $x \equiv 17 \pmod{35}$.

Correction de l'exercice 9 - Petit théorème de Fermat

- **Fermat** : 11 est premier et $11 \nmid 7$, donc $7^{10} \equiv 1 \pmod{11}$.
- **Réduction de l'exposant modulo 10** : $222 = 10 \times 22 + 2$.

$$7^{222} = (7^{10})^{22} \times 7^2 \equiv 7^2 = 49 \pmod{11}$$
- $49 = 4 \times 11 + 5$, donc le reste est 5.
- **Contrôle par le cycle** : $7^1 \equiv 7$, $7^2 \equiv 5$, $7^3 \equiv 2$, $7^4 \equiv 3$, $7^5 \equiv 10$, $7^{10} \equiv 100 \equiv 1 \checkmark$
- **Règle** : on réduit l'exposant modulo $p - 1$, jamais modulo p — c'est l'erreur la plus fréquente.
- **Application cryptographique** : ce théorème est au cœur du chiffrement **RSA**, via sa généralisation d'Euler.

Réponse. Le reste est 5.

Correction de l'exercice 10 - Inverse modulaire

- **Existence** : $\text{pgcd}(7, 26) = 1$, donc 7 est **inversible**.
- **Recherche** : on cherche u avec $7u \equiv 1 [26]$. En testant, $7 \times 15 = 105 = 4 \times 26 + 1 \checkmark$
- Donc $7^{-1} \equiv 15 \pmod{26}$.
- **Résolution** : on multiplie par 15,

$$x \equiv 15 \times 3 = 45 \equiv 45 - 26 = 19 \pmod{26}$$
- **Vérification** : $7 \times 19 = 133 = 5 \times 26 + 3 \checkmark$
- **Par Bézout** : $26 = 3 \times 7 + 5$, $7 = 1 \times 5 + 2$, $5 = 2 \times 2 + 1$; la remontée donne
 $1 = 5 - 2 \times 2 = 5 - 2(7 - 5) = 3 \times 5 - 2 \times 7 = 3(26 - 3 \times 7) - 2 \times 7 = 3 \times 26 - 11 \times 7$,
donc $7^{-1} \equiv -11 \equiv 15 \checkmark$
- **Contexte** : 26 est la taille de l'alphabet — c'est exactement le calcul du **déchiffrement affine** en cryptographie classique.

Réponse. $7^{-1} \equiv 15$ et $x \equiv 19 \pmod{26}$.

Correction de l'exercice 11 - Nombres premiers entre eux

Notons $d = \text{pgcd}(n^2 + n, 2n + 1)$.

- **Combinaison linéaire** : d divise $4(n^2 + n) = 4n^2 + 4n$ et $(2n + 1)^2 = 4n^2 + 4n + 1$.
- Par **différence**, d divise leur écart, soit 1.
- **Conclusion** : $d = 1$ — les deux nombres sont **premiers entre eux** $\checkmark$
- **Contrôles** : $n = 3$ donne $\text{pgcd}(12, 7) = 1 \checkmark$; $n = 5$ donne $\text{pgcd}(30, 11) = 1 \checkmark$
- **Autre voie** : $n^2 + n = n(n + 1)$, et $2n + 1$ est **impair**, premier avec n (car $2n + 1 - 2n = 1$) et avec $n + 1$ (car $2(n + 1) - (2n + 1) = 1$) ; par produit, il est premier avec $n(n + 1)$.

- **Technique clé** : chercher une **combinaison linéaire entière** des deux expressions égale à ± 1 .

Réponse. $(2n + 1)^2 - 4(n^2 + n) = 1$: Bézout conclut.

Correction de l'exercice 12 - Décomposition en facteurs premiers

- **Décompositions** : $360 = 2^3 \times 3^2 \times 5$ et $84 = 2^2 \times 3 \times 7$.
- **PGCD** (min des exposants) : $2^2 \times 3^1 = 12$.
- **PPCM** (max des exposants) : $2^3 \times 3^2 \times 5 \times 7 = 2\,520$.
- **Contrôle** : $12 \times 2520 = 30\,240 = 360 \times 84$ ✓
- **Nombre de diviseurs de 360** : on multiplie les (exposants + 1),
 $(3 + 1)(2 + 1)(1 + 1) = 4 \times 3 \times 2 = 24$
- **Vérification partielle** :
 $1, 2, 3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 90, 120, 180, 360$ — bien 24 diviseurs ✓
- **Formule générale** : si $n = \prod p_i^{\alpha_i}$, le nombre de diviseurs est $\prod (\alpha_i + 1)$.

Réponse. PGCD = 12, PPCM = 2 520 ; 360 a 24 diviseurs.

Correction de l'exercice 13 - Racines rationnelles d'un polynôme

- a) On multiplie $P\left(\frac{p}{q}\right) = 0$ par q^3 :

$$2p^3 + 3p^2q - q^3 = 0$$

- On isole $q^3 = p(2p^2 + 3pq)$: p divise q^3 . Or $p \wedge q = 1$ entraîne $p \wedge q^3 = 1$; p divise q^3 et lui est premier : p divise 1 (conséquence du lemme de **Gauss** : $p \mid q^2 \cdot q$ et $p \wedge q = 1$ donnent $p \mid q^2$, puis $p \mid q$, puis $p \mid 1$).
- De même $2p^3 = q(q^2 - 3p^2)$: q divise $2p^3$ et $q \wedge p^3 = 1$, donc par **Gauss** q divise 2.

- b) $p \in \{-1, 1\}$ et $q \in \{1, 2\}$: les candidats sont $1, -1, \frac{1}{2}, -\frac{1}{2}$.

- $P(1) = 2 + 3 - 1 = 4 \neq 0$; $P(-1) = -2 + 3 - 1 = 0$ ✓
- $P\left(\frac{1}{2}\right) = \frac{1}{4} + \frac{3}{4} - 1 = 0$ ✓ ; $P\left(-\frac{1}{2}\right) = -\frac{1}{4} + \frac{3}{4} - 1 = -\frac{1}{2} \neq 0$.

- c) On factorise par $(x + 1)$ puis $(2x - 1)$:

$$2x^3 + 3x^2 - 1 = (x + 1)^2(2x - 1)$$

- **Vérification** : $(x^2 + 2x + 1)(2x - 1) = 2x^3 + 4x^2 + 2x - x^2 - 2x - 1 = 2x^3 + 3x^2 - 1$ ✓
- Solutions réelles : -1 (racine **double**) et $\frac{1}{2}$.
- **Méthode générale** : une racine rationnelle irréductible $\frac{p}{q}$ d'un polynôme à coefficients entiers a son numérateur qui divise le coefficient constant et son dénominateur qui divise le coefficient dominant.

Réponse. Candidats $\pm 1, \pm \frac{1}{2}$; $P = (x + 1)^2(2x - 1)$; racines -1 (double) et $\frac{1}{2}$.

Correction de l'exercice 14 - Congruence à coefficient non inversible

- a) $\text{pgcd}(6, 10) = 2$ divise 4 : on peut diviser **les trois** nombres par 2 (on ne divise jamais seulement les deux membres) :

$$6x \equiv 4 \pmod{10} \Leftrightarrow 10 \mid 6x - 4 \Leftrightarrow 5 \mid 3x - 2 \Leftrightarrow 3x \equiv 2 \pmod{5}$$

- 3 est inversible modulo 5 : $3 \times 2 = 6 \equiv 1$, donc l'inverse de 3 est 2.
- On multiplie par 2 : $x \equiv 4 \pmod{5}$.
- **Solutions** : $x = 4 + 5k$, $k \in \mathbb{Z}$, c'est-à-dire $x \equiv 4$ ou $x \equiv 9 \pmod{10}$.
- **Vérification** : $6 \times 4 = 24 \equiv 4$ et $6 \times 9 = 54 \equiv 4 \pmod{10}$ ✓
- b)** Si $6x \equiv 5 \pmod{10}$, alors $6x - 5 = 10k$, donc $5 = 6x - 10k$ serait **pair**, ce qui est absurde. Aucune solution.
- c)** Soit $d = \text{pgcd}(a, n)$.
 - Si $d \nmid b$: **aucune** solution (même argument qu'en b) : d divise $ax - kn = b$.
 - Si $d \mid b$: l'équation équivaut à $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$, où $\frac{a}{d}$ est inversible modulo $\frac{n}{d}$; il y a une solution unique modulo $\frac{n}{d}$, donc d **solutions** modulo n .
 - Ici $d = 2$: deux solutions modulo 10 ✓
 - **Piège** : « simplifier par 2 » en écrivant $3x \equiv 2 \pmod{10}$ (sans diviser le module) donne $x \equiv 4 \pmod{10}$ seulement et fait perdre la solution 9.
- Réponse.** a) $x \equiv 4 \pmod{5}$; b) aucune solution ; c) solutions $\Leftrightarrow d \mid b$, et alors d solutions modulo n .

Correction de l'exercice 15 - Synthèse : chiffre des unités et divisibilité

Méthode par congruences.

- $3^{2n+1} = 3 \times 9^n$, et $9 \equiv 2 \pmod{7}$, donc $3^{2n+1} \equiv 3 \times 2^n \pmod{7}$.
- $2^{n+2} = 4 \times 2^n$.
- **Somme** :

$$3^{2n+1} + 2^{n+2} \equiv 3 \times 2^n + 4 \times 2^n = 7 \times 2^n \equiv 0 \pmod{7}$$
- **Conclusion** : 7 divise l'expression pour tout n ✓

Contrôles numériques.

- $n = 0$: $3 + 4 = 7 = 7 \times 1$ ✓
- $n = 1$: $27 + 8 = 35 = 7 \times 5$ ✓
- $n = 2$: $243 + 16 = 259 = 7 \times 37$ ✓
- $n = 3$: $2187 + 32 = 2219 = 7 \times 317$ ✓
- **Méthode alternative (récurrence)** : avec $u_n = 3^{2n+1} + 2^{n+2}$, on vérifie $u_{n+1} = 9u_n - 7 \times 2^{n+2}$; si $7 \mid u_n$, alors $7 \mid u_{n+1}$. C'est juste, mais il faut deviner la relation : les **congruences** sont l'outil adapté.

Réponse. $3^{2n+1} + 2^{n+2} \equiv 7 \times 2^n \equiv 0 \pmod{7}$.