Plaquette 2 – Divisibilité, division euclidienne et PGCD

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

Corrections détaillées

Boîte à outils

Divisibilité et PGCD dans $\mathbb{Z}$.

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

— **Invariance du PGCD** : $\text{pgcd}(a, b) = \text{pgcd}(b, a - qb)$ pour tout $q \in \mathbb{Z}$ — c'est le moteur de l'algorithme d'Euclide.

— **Bézout** : $a \wedge b = d \Rightarrow \exists u, v \in \mathbb{Z}$, $au + bv = d$; $a \wedge b = 1 \Leftrightarrow \exists u, v$, $au + bv = 1$.

— **Gauss** : $a \mid bc$ et $a \wedge b = 1 \Rightarrow a \mid c$. Corollaire : $a \mid N$, $b \mid N$, $a \wedge b = 1 \Rightarrow ab \mid N$.

— **Homogénéité** : $\text{pgcd}(ka, kb) = k\text{pgcd}(a, b)$ pour $k \in \mathbb{N}^*$.

— **PGCD et PPCM** : $\text{pgcd}(a, b) \times \text{ppcm}(a, b) = |ab|$.

— **Factorisation** : $a^n - b^n = (a - b)\left(a^{n-1} + a^{n-2}b + \ldots + b^{n-1}\right)$, donc $a - b \mid a^n - b^n$.

— **Sous-groupes de** $\mathbb{Z}$: ce sont les $n\mathbb{Z}$; $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ et $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a, b)\mathbb{Z}$.

Correction de l'exercice 1 – Restes des carrés

a) On cherche q et r avec $-47 = 6q + r$ et $0 \leq r < 6$. Le reste doit être **positif** : $6 \times (-8) = -48 \leq -47$, donc
$$-47 = 6 \times (-8) + 1, \qquad q = -8, \quad r = 1$$

Piège : $-47 = 6 \times (-7) - 5$ n'est pas la division euclidienne, car $-5 < 0$.

b) On étudie la parité de n.

— $n = 2k$: $n^2 = 4k^2$, reste 0.

— $n = 2k + 1$: $n^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, reste 1.

c) Si $N = a^2 + b^2$, les restes de a^2 et b^2 modulo 4 valent 0 ou 1, donc celui de N vaut 0, 1 ou 2 — jamais 3. Or $2027 = 4 \times 506 + 3$: 2027 n'est pas somme de deux carrés.

d) Pour $n = 2k + 1$: $n^2 = 4k(k + 1) + 1$. Parmi k et $k + 1$, l'un est pair, donc $k(k + 1) = 2m$ et $n^2 = 8m + 1$. Contrôle : $3^2 = 9 = 8 + 1$, $5^2 = 25 = 3 \times 8 + 1$, $7^2 = 49 = 6 \times 8 + 1$ ✓.

Réponse. $-47 = 6 \times (-8) + 1$; $n^2 \equiv 0$ ou 1 modulo 4 ; 2027 n'est pas somme de deux carrés ; n impair $\Rightarrow n^2 \equiv 1 \pmod 8$.

Correction de l'exercice 2 – Produits d'entiers consécutifs

a) Parmi deux entiers consécutifs, l'un est pair : $2 \mid n(n + 1)(n + 2)$. Parmi trois entiers consécutifs, l'un est multiple de 3 (les restes modulo 3 sont $0, 1, 2$ dans un certain ordre) : $3 \mid n(n + 1)(n + 2)$. On conclut par le **corollaire de Gauss** :
$$2 \mid N, \quad 3 \mid N, \quad 2 \wedge 3 = 1 \quad \Longrightarrow \quad 6 \mid N$$

b) On développe selon l'indication :
$$n(n + 1)(2n + 1) = n(n + 1)(n + 2) + (n - 1)n(n + 1)$$

— Chaque terme est un produit de trois entiers consécutifs, divisible par 6 d'après a) ; leur somme aussi.

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).

— On retrouve que $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$ est bien un **entier**.

c) Parmi quatre entiers consécutifs, deux sont pairs et **l'un d'eux est multiple de** 4 : le produit est divisible par $4 \times 2 = 8$. L'un des quatre est aussi multiple de 3. Comme $8 \wedge 3 = 1$, le produit est divisible par 24.

Autre méthode : $n(n+1)(n+2)(n+3) = 24\binom{n+3}{4}$, et un coefficient binomial est un entier. Contrôle : $1 \times 2 \times 3 \times 4 = 24$, $2 \times 3 \times 4 \times 5 = 120 = 5 \times 24$ ✓.

Piège : « divisible par 2 et par 4 » ne donne pas 8 (car $2 \wedge 4 \neq 1$) ; c'est l'argument des **deux** nombres pairs distincts qui donne le facteur 8.

Réponse. $6 \mid n(n+1)(n+2)$ et $6 \mid n(n+1)(2n+1)$; 24 divise le produit de quatre entiers consécutifs.

Correction de l'exercice 3 – Homogénéité du PGCD

a) Notons $d = \text{pgcd}(a, b)$ et $D = \text{pgcd}(ka, kb)$. On montre $D \mid kd$ et $kd \mid D$.

— **Bézout** : il existe u, v tels que $au + bv = d$, donc

$$(ka)u + (kb)v = kd$$

Tout diviseur commun de ka et kb divise cette combinaison : $D \mid kd$.

— $d \mid a$ et $d \mid b$ donnent $kd \mid ka$ et $kd \mid kb$, donc $kd \mid D$.

Deux entiers positifs qui se divisent mutuellement sont égaux : $D = kd$.

b) $1500 = 300 \times 5$ et $2100 = 300 \times 7$ avec $5 \wedge 7 = 1$, donc $\text{pgcd}(1500, 2100) = 300 \times 1 = 300$.

c) On divise par $\text{pgcd}(12, 18) = 6$: $2x = 3y$.

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

— Réciproquement, $(3k, 2k)$ convient : $12 \times 3k = 36k = 18 \times 2k$.

Solutions : $(x, y) = (3k, 2k)$, $k \in \mathbb{N}^*$.

Piège : sans diviser par 6, on écrirait $12 \mid 18y$ et on ne pourrait rien conclure, car $12 \wedge 18 \neq 1$.

Réponse. $\text{pgcd}(ka, kb) = k\text{pgcd}(a, b)$; $\text{pgcd}(1500, 2100) = 300$; $(x, y) = (3k, 2k)$.

Correction de l'exercice 4 – PGCD et PPCM imposés

a) On utilise la relation du cours :

$$\text{pgcd}(a, b) \times \text{ppcm}(a, b) = ab$$

— donc $ab = 6 \times 180 = 1080$.

b) 6 divise a et b : $a = 6a'$, $b = 6b'$ avec $a' \wedge b' = 1$ (sinon le PGCD serait plus grand, par homogénéité). Alors $ab = 36a'b' = 1080$ donne

$$a'b' = 30, \qquad a' \wedge b' = 1, \qquad a' \leq b'$$

c) $30 = 2 \times 3 \times 5$ n'a que des facteurs premiers simples : pour être premiers entre eux, a' et b' se **répartissent** les facteurs 2, 3, 5 sans en partager aucun. Avec $a' \leq b'$: $(1, 30)$, $(2, 15)$, $(3, 10)$, $(5, 6)$.

— Solutions : $(a, b) \in \{(6, 180), (12, 90), (18, 60), (30, 36)\}$.

— Vérification pour $(30, 36)$: $30 = 2 \times 3 \times 5$, $36 = 2^2 \times 3^2$; PGCD $= 2 \times 3 = 6$, PPCM $= 2^2 \times 3^2 \times 5 = 180$ ✓.

Piège : on n'oublie pas la condition $a' \wedge b' = 1$. Si on imposait pgcd = 6 et ppcm = 216, on

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).

aurait $a'b' = 36$: le couple $(2, 18)$ vérifie le produit mais pas la condition, et donnerait $(12, 108)$, de PGCD 12.

Réponse. $(6, 180)$, $(12, 90)$, $(18, 60)$, $(30, 36)$.

Correction de l'exercice 5 – Engrenages, bus et carrelage

a) Après N dents passées, la roue de 24 dents a fait $\frac{N}{24}$ tours et la dent marquée revient au contact quand $24 \mid N$; de même $36 \mid N$ pour l'autre roue. On cherche le plus petit $N > 0$ multiple commun :

$$N = \text{ppcm}(24, 36) = \frac{24 \times 36}{\text{pgcd}(24, 36)} = \frac{864}{12} = 72$$

— La petite roue fait $\frac{72}{24} = 3$ tours, la grande $\frac{72}{36} = 2$ tours.

b) Même raisonnement avec trois durées : $12 = 2^2 \times 3$, $18 = 2 \times 3^2$, $30 = 2 \times 3 \times 5$. Le PPCM prend le **plus grand exposant** de chaque facteur premier :

$$\text{ppcm}(12, 18, 30) = 2^2 \times 3^2 \times 5 = 180 \text{ min} = 3 \text{ h}$$

— Elles repartent ensemble à 10 h.

c) Le côté c du carreau doit diviser 360 et 264 ; on veut le plus grand : $c = \text{pgcd}(360, 264)$. Euclide : $360 = 1 \times 264 + 96$, $264 = 2 \times 96 + 72$, $96 = 1 \times 72 + 24$, $72 = 3 \times 24$. Donc $c = 24$ cm.

— Nombre de carreaux : $\frac{360}{24} \times \frac{264}{24} = 15 \times 11 = 165$.

Réflexe : « revenir ensemble », « se retrouver » → **PPCM** ; « découper en parts égales les plus grandes possibles » → **PGCD**.

Réponse. a) 72 dents : 3 tours et 2 tours. b) 10 h. c) Carreaux de 24 cm, 165 carreaux.

Correction de l'exercice 6 – PGCD par élimination de n

a) Pour éliminer n, on multiplie par des coefficients qui égalisent les termes en n : $\text{ppcm}(35, 45) = 315 = 9 \times 35 = 7 \times 45$.

$$9a_n - 7b_n = (315n + 513) - (315n + 532) = -19$$

— d_n divise a_n et b_n, donc toute combinaison : $d_n \mid 19$.

— 19 est premier : $d_n \in \{1, 19\}$.

b) $d_n = 19 \Leftrightarrow 19 \mid a_n$ et $19 \mid b_n$.

— $57 = 3 \times 19$, donc $19 \mid a_n \Leftrightarrow 19 \mid 35n$; comme 19 est premier et ne divise pas 35, le **lemme d'Euclide** donne $19 \mid 35n \Leftrightarrow 19 \mid n$.

— Si $19 \mid n$, alors $19 \mid 45n + 76$ aussi ($76 = 4 \times 19$).

Donc $d_n = 19 \Leftrightarrow n \equiv 0 \pmod{19}$, et $d_n = 1$ sinon.

c) $n = 19$: $a_{19} = 722 = 19 \times 38$ et $b_{19} = 931 = 19 \times 49$, avec $38 \wedge 49 = 1$: $d_{19} = 19$ ✓. $n = 1$: $a_1 = 92$, $b_1 = 121 = 11^2$; $92 = 4 \times 23$: $d_1 = 1$ ✓.

Piège : la combinaison ne donne que « d_n **divise** 19 » ; il faut ensuite chercher quand 19 est effectivement atteint.

Réponse. $9a_n - 7b_n = -19$; $d_n = 19$ si $19 \mid n$, $d_n = 1$ sinon.

Correction de l'exercice 7 – Écriture en base b

a) On divise par 2 tant que le quotient est non nul ; les restes, lus **de bas en haut**, donnent les chiffres.

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).

— $2026 = 2 \times 1013 + 0$, $1013 = 2 \times 506 + 1$, $506 = 2 \times 253 + 0$, $253 = 2 \times 126 + 1$;
— $126 = 2 \times 63 + 0$, $63 = 2 \times 31 + 1$, $31 = 2 \times 15 + 1$, $15 = 2 \times 7 + 1$;
— $7 = 2 \times 3 + 1$, $3 = 2 \times 1 + 1$, $1 = 2 \times 0 + 1$.

$$2026 = (11111101010)_2$$

b) $2026 = 16 \times 126 + 10$, $126 = 16 \times 7 + 14$, $7 = 16 \times 0 + 7$: $2026 = (7\mathrm{EA})_{16}$. Vérification : $7 \times 256 + 14 \times 16 + 10 = 1792 + 224 + 10 = 2026$ ✓. (Regrouper les bits par quatre donne la même chose : 0111 1110 1010.)

c) On écrit la différence :

$$N - s = \sum_{k=0}^{m} c_k \left(b^k - 1\right)$$

— Par la factorisation $b^k - 1 = (b-1)(b^{k-1} + \ldots + 1)$, chaque $b^k - 1$ est multiple de $b - 1$; donc $b - 1 \mid N - s$: N et s ont le même reste modulo $b - 1$.
— Pour $b = 10$, c'est la **preuve par 9**.

d) En base 16 : $s = 7 + 14 + 10 = 31 = 2 \times 15 + 1$. Donc 2026 a pour reste 1 modulo 15. Contrôle : $2025 = 15 \times 135$ ✓.

Réponse. $2026 = (11111101010)_2 = (7\mathrm{EA})_{16}$; $N \equiv s \pmod{b-1}$; reste 1 modulo 15.

Correction de l'exercice 8 – Divisibilité de a puissance n moins b puissance n

a) On vérifie par développement (le produit est télescopique) :

$$a^n - b^n = (a-b) \sum_{k=0}^{n-1} a^{n-1-k} b^k$$

— La somme est un entier, donc $a - b \mid a^n - b^n$.

b) $2^{3k} - 1 = 8^k - 1^k$ est divisible par $8 - 1 = 7$. Contrôle : $2^3 - 1 = 7$, $2^6 - 1 = 63 = 9 \times 7$ ✓.

c) On applique a) avec $a = 2$, $b = -1$: $3 = 2 - (-1)$ divise $2^n - (-1)^n$. Donc

$$2^n + 1 = \left(2^n - (-1)^n\right) + \left((-1)^n + 1\right)$$

— a le même reste modulo 3 que $(-1)^n + 1$, qui vaut 0 si n est impair et 2 si n est pair.
— Donc $3 \mid 2^n + 1 \Leftrightarrow n$ impair. Contrôle : $2^3 + 1 = 9$ ✓, $2^2 + 1 = 5$ n'est pas multiple de 3 ✓.

d) $2^n - 1 = (2^r)^s - 1^s$ est divisible par $2^r - 1$ d'après a). Si $2^n - 1$ est premier et $n = rs$ avec $1 < r < n$, alors $1 < 2^r - 1 < 2^n - 1$ serait un diviseur strict : impossible. Donc n **est premier**.

Piège : la réciproque est fausse : $n = 11$ est premier mais $2^{11} - 1 = 2047 = 23 \times 89$.

Réponse. $a - b \mid a^n - b^n$; $7 \mid 8^k - 1$; $3 \mid 2^n + 1 \Leftrightarrow n$ impair ; $2^n - 1$ premier $\Rightarrow n$ premier.

Correction de l'exercice 9 – Nombres de Fibonacci et algorithme d'Euclide

a) Initialisation : $F_1 \wedge F_0 = 1 \wedge 0 = 1$. **Hérédité** : on utilise l'invariance du PGCD,

$$\mathrm{pgcd}(F_{n+2}, F_{n+1}) = \mathrm{pgcd}(F_{n+1}, F_{n+2} - F_{n+1}) = \mathrm{pgcd}(F_{n+1}, F_n) = 1$$

b) Pour $n \geq 3$, on a $F_{n-1} \geq 1$ et $F_{n-1} < F_n$ (car $F_n = F_{n-1} + F_{n-2}$ avec $F_{n-2} \geq 1$ dès $n \geq 3$). Donc

$$F_{n+1} = 1 \times F_n + F_{n-1}, \qquad 0 \leq F_{n-1} < F_n$$

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).

— est **la** division euclidienne : quotient 1, reste F_{n-1}. L'algorithme passe de (F_{n+1}, F_n) à (F_n, F_{n-1}).
— On descend ainsi jusqu'à $(F_3, F_2) = (2, 1)$, qui donne $2 = 2 \times 1 + 0$ et arrête l'algorithme.
— Les couples rencontrés sont (F_{k+1}, F_k) pour $k = n, n-1, \ldots, 2$: il y en a $n-1$, une division chacun.

c) $89 = F_{11}$ et $55 = F_{10}$: on attend 9 divisions.

— $89 = 55 + 34$, $55 = 34 + 21$, $34 = 21 + 13$, $21 = 13 + 8$, $13 = 8 + 5$;
— $8 = 5 + 3$, $5 = 3 + 2$, $3 = 2 + 1$, $2 = 2 \times 1 + 0$.

Neuf divisions ✓, PGCD = 1 ✓.

Remarque (théorème de Lamé) : les quotients valent tous 1, le pire cas possible ; on en déduit que le nombre de divisions est au plus de l'ordre de $\log_\varphi b$, avec $\varphi = \frac{1+\sqrt{5}}{2}$: l'algorithme d'Euclide est **rapide**.

Réponse. $F_{n+1} \wedge F_n = 1$; $n-1$ divisions, toutes de quotient 1 sauf la dernière ; 9 divisions pour $(89, 55)$.

Correction de l'exercice 10 – PGCD de nombres de Mersenne

a) On développe : $2^r(2^{bq} - 1) + 2^r - 1 = 2^{bq+r} - 2^r + 2^r - 1 = 2^a - 1$ ✓.

— $2^{bq} - 1 = (2^b)^q - 1^q$ est divisible par $2^b - 1$ (factorisation de $x^q - 1$).
— $0 \le 2^r - 1 < 2^b - 1$ car $0 \le r < b$.

C'est donc la division euclidienne de $2^a - 1$ par $2^b - 1$, de reste $2^r - 1$.

b) Notons $M_k = 2^k - 1$. La question a) et l'invariance du PGCD donnent

$$\operatorname{pgcd}(M_a, M_b) = \operatorname{pgcd}(M_b, M_r) \quad \text{où } r \text{ est le reste de } a \text{ par } b$$

— L'algorithme d'Euclide sur (M_a, M_b) suit **pas à pas** celui sur les exposants (a, b).
— Quand les exposants arrivent à $(\operatorname{pgcd}(a,b), 0)$, on obtient $\operatorname{pgcd}(M_{a\wedge b}, M_0) = \operatorname{pgcd}(M_{a\wedge b}, 0) = M_{a\wedge b}$.

c) $\operatorname{pgcd}(12, 18) = 6$, donc $\operatorname{pgcd}(4095, 262143) = 2^6 - 1 = 63$.

— Vérification : $4095 = 63 \times 65$ et $262143 = 63 \times 4161$; $4161 = 64 \times 65 + 1$ donc $65 \wedge 4161 = 1$ ✓.

Conséquence : $M_a \wedge M_b = 1 \Leftrightarrow a \wedge b = 1$. Par exemple $2^9 - 1 = 511$ et $2^{10} - 1 = 1023$ sont premiers entre eux.

Réponse. $\operatorname{pgcd}(2^a - 1, 2^b - 1) = 2^{a\wedge b} - 1$; $\operatorname{pgcd}(4095, 262143) = 63$.

Correction de l'exercice 11 – Points entiers sur un segment

a) Le segment S est l'ensemble des $tP = (ta, tb)$ pour $t \in [0, 1]$. Un point (x, y) est sur la **droite** (OP) si et seulement si ses coordonnées sont proportionnelles à (a, b) :

$$(x, y) \in (OP) \Leftrightarrow bx - ay = 0$$

— et il est sur le segment si de plus $0 \le x \le a$ (l'abscisse varie de 0 à a).

b) En divisant par d : $b'x = a'y$ avec $a' \wedge b' = 1$.

— $a' \mid b'x$ et $a' \wedge b' = 1$, donc par **Gauss** $a' \mid x$: $x = ka'$, puis $y = kb'$.
— La condition $0 \le ka' \le a = da'$ équivaut à $0 \le k \le d$.

Les points entiers de S sont les (ka', kb') pour $k = 0, 1, \ldots, d$: il y en a $d + 1$.

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).

c) $P(12,8)$: $d = 4$, donc 5 points, $(0,0), (3,2), (6,4), (9,6), (12,8)$ — ceux de la figure. $P(2024,1155)$: $d = 11$ (calculé par Euclide : $2024 = 1155 + 869$, $1155 = 869 + 286$, $869 = 3 \times 286 + 11$, $286 = 26 \times 11$), donc 12 points.

Interprétation : si $a \wedge b = 1$, le segment ne rencontre **aucun** nœud entre ses extrémités.

Réponse. $d + 1$ points entiers ; 5 pour $(12,8)$; 12 pour $(2024,1155)$.

Correction de l'exercice 12 – Sous-groupes de Z

a) H contient un élément non nul h, donc aussi $-h$: $H \cap \mathbb{N}^*$ est une partie non vide de $\mathbb{N}$, qui admet un **plus petit élément** n.

— $n\mathbb{Z} \subset H$: H est stable par addition et opposé, donc contient tous les kn.

— $H \subset n\mathbb{Z}$: pour $h \in H$, on écrit $h = nq + r$ avec $0 \leq r < n$. Alors

$$r = h - qn \in H$$

— et $0 \leq r < n$; par minimalité de n, r ne peut pas être strictement positif : $r = 0$ et $h \in n\mathbb{Z}$.

b) $a\mathbb{Z} + b\mathbb{Z}$ contient 0, et $(au + bv) - (au' + bv') = a(u - u') + b(v - v')$: c'est un sous-groupe, donc égal à $\delta\mathbb{Z}$ avec $\delta > 0$ d'après a).

— $a = a \times 1 + b \times 0$ et b sont dans $\delta\mathbb{Z}$: δ est un **diviseur commun**, $\delta \leq a \wedge b$.

— $\delta = au + bv$ pour certains u, v : tout diviseur commun de a et b divise δ, en particulier $a \wedge b \mid \delta$.

Donc $\delta = a \wedge b$, et l'écriture $\delta = au + bv$ est la **relation de Bézout**.

c) Une intersection de sous-groupes est un sous-groupe : $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ avec $m > 0$ (elle contient $ab \neq 0$). Ses éléments sont les multiples communs de a et b, et m est le plus petit strictement positif : $m = \text{ppcm}(a,b)$. Au passage : **tout multiple commun est multiple du PPCM**.

Réponse. $H = n\mathbb{Z}$; $a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\mathbb{Z}$ (Bézout) ; $a\mathbb{Z} \cap b\mathbb{Z} = \text{ppcm}(a,b)\mathbb{Z}$.

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

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

$$a_n p^n + a_{n-1} p^{n-1} q + \ldots + a_1 p q^{n-1} + a_0 q^n = 0$$

— Tous les termes sauf le dernier sont multiples de p, donc $p \mid a_0 q^n$. Comme $p \wedge q = 1$, on a $p \wedge q^n = 1$, et **Gauss** donne $p \mid a_0$.

— De même, tous les termes sauf le premier sont multiples de q : $q \mid a_n p^n$, d'où $q \mid a_n$.

b) Candidats : $p \mid -2$ et $q \mid 2$, soit $\frac{p}{q} \in \{\pm 1, \pm 2, \pm\frac{1}{2}\}$. On teste : $P(1) = 3$, $P(-1) = -9$, $P(2) = 18$, $P(-2) = -30$, $P(-\frac{1}{2}) = -\frac{9}{2}$, et

$$P\left(\frac{1}{2}\right) = \frac{1}{4} - \frac{1}{4} + 2 - 2 = 0$$

— Factorisation : $2X^3 - X^2 + 4X - 2 = (2X - 1)(X^2 + 2)$ (développer pour vérifier). $X^2 + 2$ n'a pas de racine réelle : $\frac{1}{2}$ est **la seule** racine rationnelle.

c) Les candidats sont ± 1 : $1 - 3 - 1 = -3 \neq 0$ et $-1 + 3 - 1 = 1 \neq 0$. Aucune racine rationnelle.

— Avec $\theta = \frac{\pi}{9}$ et $x = 2\cos\theta$: $x^3 - 3x = 8\cos^3\theta - 6\cos\theta = 2\cos 3\theta = 2\cos\frac{\pi}{3} = 1$.

— Donc x est racine de $X^3 - 3X - 1$: il est irrationnel, et $\cos\frac{\pi}{9} = \frac{x}{2}$ aussi (sinon x serait rationnel).

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).

Valeur : $2\cos\frac{\pi}{9} \approx 1{,}8794$, et $1{,}8794^3 - 3\times 1{,}8794 \approx 1{,}000$ ✓.

Réponse. $p \mid a_0$, $q \mid a_n$; $2X^3 - X^2 + 4X - 2 = (2X-1)(X^2+2)$; $\cos\frac{\pi}{9} \notin \mathbb{Q}$.

Correction de l'exercice 14 – Nombres de Fermat

a) Récurrence sur n. **Initialisation** : $F_0 = 3 = 5 - 2 = F_1 - 2$. **Hérédité** : on utilise $x^2 - 1 = (x-1)(x+1)$ avec $x = 2^{2^n}$,

$$F_{n+1} - 2 = 2^{2^{n+1}} - 1 = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = (F_n - 2)F_n$$

— puis l'hypothèse de récurrence : $(F_n - 2)F_n = \left(\prod_{k=0}^{n-1} F_k\right)F_n = \prod_{k=0}^{n} F_k$.

b) Soient $m < n$ et d un diviseur commun de F_m et F_n.

— F_m figure dans le produit $\prod_{k=0}^{n-1} F_k = F_n - 2$, donc $d \mid F_n - 2$.
— $d \mid F_n$, donc d divise la différence : $d \mid 2$.
— Les F_n sont **impairs**, donc d est impair : $d = 1$.

c) Chaque $F_n \geq 3$ admet au moins un diviseur premier p_n. D'après b), les p_n sont **deux à deux distincts** (un premier commun diviserait deux F_n distincts). On obtient une infinité de nombres premiers.

d) $F_0F_1F_2F_3 = 3\times 5\times 17\times 257 = 65535$ et $F_4 - 2 = 65537 - 2 = 65535$ ✓.

Remarque : F_0 à F_4 sont premiers ; on ne connaît aucun autre nombre de Fermat premier.

Réponse. $\prod_{k<n} F_k = F_n - 2$; $F_m \wedge F_n = 1$ pour $m \neq n$; d'où une infinité de nombres premiers.

Correction de l'exercice 15 – Synthèse : une fraction toujours irréductible

a) $nA_n = n^4 + 2n^2$, donc $B_n - nA_n = n^2 + 1$:

$$B_n = nA_n + (n^2+1), \qquad R_n = n^2 + 1$$

b) $nR_n = n^3 + n$, donc $A_n - nR_n = n$: $A_n = nR_n + n$, soit $S_n = n$. Puis $R_n = n\times n + 1$.

c) À chaque étape on utilise $\gcd(a,b) = \gcd(b, a - qb)$ avec un quotient q **entier** (ici $q = n$) :

$$\gcd(B_n, A_n) = \gcd(A_n, R_n) = \gcd(R_n, n) = \gcd(n, 1) = 1$$

— Le cas $n = 0$ est inclus : $\gcd(0,1) = 1$.

Les « restes » $n^2 + 1$ et n ne sont pas forcément inférieurs aux diviseurs (ce ne sont pas des divisions euclidiennes d'entiers), mais la propriété d'invariance ne l'exige pas.

d) Numérateur et dénominateur sont premiers entre eux : la fraction est irréductible.

— $n = 2$: $\frac{8+4}{16+12+1} = \frac{12}{29}$, et 29 est premier sans diviser 12 ✓.
— $n = 3$: $\frac{27+6}{81+27+1} = \frac{33}{109}$, et 109 est premier ✓.

Réflexe : dès que les coefficients dominants valent 1, la division de polynômes en n donne des quotients entiers et l'algorithme d'Euclide s'applique tel quel.

Réponse. $B_n = nA_n + n^2 + 1$, $A_n = n(n^2+1) + n$, $n^2 + 1 = n\cdot n + 1$: $\gcd(A_n, B_n) = 1$.

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).