

**Plaquette 2 - Divisibilité, PGCD et
lemme de Gauss : démonstrations**
Arithmétique dans $\mathbb{Z}$ — Licence 1 (L1)
Corrections détaillées

Boîte à outils

PGCD et combinaisons linéaires. Pour tous entiers a, b, k :

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

- Tout diviseur commun de a et b divise toute combinaison $au + bv$.
- **Bézout** : $a \wedge b = 1 \Leftrightarrow \exists (u, v) \in \mathbb{Z}^2, au + bv = 1$.
- **Gauss** : $a \mid bc$ et $a \wedge b = 1 \Rightarrow a \mid c$.
- **Corollaires** : si $a \wedge b = 1, a \mid c$ et $b \mid c$, alors $ab \mid c$; si $a \wedge b = a \wedge c = 1$, alors $a \wedge bc = 1$.
- **Réduction** : $d = a \wedge b, a = da', b = db'$ avec $a' \wedge b' = 1$, et $\text{ppcm}(a, b) = da'b'$.

Factorisation utile (pour $n \geq 1$) :

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + b^{n-1})$$

- En particulier $a - b \mid a^n - b^n$, et $2^d - 1 \mid 2^n - 1$ dès que $d \mid n$.

Correction de l'exercice 1 - PGCD dépendant d'un paramètre

a) On cherche une combinaison qui élimine n :

$$3(2n + 3) - 2(3n + 4) = 6n + 9 - 6n - 8 = 1$$

- Tout diviseur commun d de $2n + 3$ et $3n + 4$ divise cette combinaison, donc divise 1 : $d = 1$.
- C'est une **relation de Bézout** explicite, avec $u = 3$ et $v = -2$, valable pour tout n .

b) On effectue la division de $n^2 + 1$ par $n + 1$: $n^2 + 1 = (n + 1)(n - 1) + 2$. D'après la règle $\text{pgcd}(a, b) = \text{pgcd}(b, a - kb)$ avec $k = n - 1$:

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

- Ce PGCD divise 2 : il vaut 1 ou 2.
- Il vaut 2 si et seulement si $n + 1$ est pair, c'est-à-dire si n est **impair**.
- c)** $n = 7$: $\text{pgcd}(50, 8) = 2$ ($50 = 6 \times 8 + 2$, puis $8 = 4 \times 2$) ✓ (n impair).
- $n = 10$: $\text{pgcd}(101, 11) = 1$ ($101 = 9 \times 11 + 2, 11 = 5 \times 2 + 1$) ✓ (n pair).
- **Méthode** : pour un PGCD qui dépend de n , on fait la **division euclidienne polynomiale** pour faire baisser le degré, jusqu'à un reste constant.

Réponse. a) $3(2n + 3) - 2(3n + 4) = 1$; b) $\text{pgcd} = 2$ si n impair, 1 si n pair.

Correction de l'exercice 2 - PGCD de nombres de Mersenne

a) Si $n = dk$, on applique la factorisation $x^k - 1 = (x - 1)(x^{k-1} + \dots + 1)$ avec $x = 2^d$:

$$2^n - 1 = \left(2^d\right)^k - 1 = \left(2^d - 1\right)\left(2^{d(k-1)} + \dots + 2^d + 1\right)$$

- Donc $M_d \mid M_n$.

- b)** $2^b \equiv 1 \pmod{M_b}$ (car $M_b = 2^b - 1$). Donc $2^{bq} \equiv 1$ et
 — $2^a = 2^{bq} \times 2^r \equiv 2^r \pmod{M_b}$, d'où $M_a = 2^a - 1 \equiv 2^r - 1 = M_r \pmod{M_b}$ (avec $M_0 = 0$).
c) b) dit que $M_a = M_r + kM_b$, donc $\text{pgcd}(M_a, M_b) = \text{pgcd}(M_b, M_r)$. C'est exactement la même étape que dans l'algorithme d'Euclide pour $(a, b) \mapsto (b, r)$.
 — En itérant, les indices suivent l'algorithme d'Euclide pour a et b ; il s'arrête sur $(\text{pgcd}(a, b), 0)$, et $\text{pgcd}(M_d, M_0) = \text{pgcd}(M_d, 0) = M_d$.

$$\text{pgcd}(M_a, M_b) = M_{\text{pgcd}(a, b)}$$

d) Par c) : $\text{pgcd}(12, 18) = 6$, donc le PGCD vaut $2^6 - 1 = 63$.
 — Directement : $2^{12} - 1 = 4\,095$ et $2^{18} - 1 = 262\,143$. Euclide : $262\,143 = 64 \times 4\,095 + 63$, puis $4\,095 = 65 \times 63 + 0$. PGCD = 63 ✓
 — **Remarque** : le reste $63 = M_6$ apparaît dès la première division, comme le prévoit b) avec $18 = 1 \times 12 + 6$.

Réponse. $\text{pgcd}(2^a - 1, 2^b - 1) = 2^{\text{pgcd}(a, b)} - 1$; en d) 63.

Correction de l'exercice 3 - Suite de Fibonacci et PGCD

- a)** Récurrence. **Initialisation** : $F_1^2 - F_0 F_2 = 1 - 0 = 1 = (-1)^0$ ✓
 — **Hérédité** : supposons $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$. On calcule le rang suivant en remplaçant $F_{n+3} = F_{n+2} + F_{n+1}$:

$$F_{n+2}^2 - F_{n+1} F_{n+3} = F_{n+2}^2 - F_{n+1} F_{n+2} - F_{n+1}^2 = F_{n+2}(F_{n+2} - F_{n+1}) - F_{n+1}^2$$

 — Or $F_{n+2} - F_{n+1} = F_n$: on obtient $F_n F_{n+2} - F_{n+1}^2 = -(-1)^n = (-1)^{n+1}$ ✓
b) Cassini s'écrit $F_{n+1} \times F_{n+1} + F_n \times (-F_{n+2}) = (-1)^n$. En multipliant par $(-1)^n$, on obtient une **relation de Bézout** entre F_{n+1} et F_n :
 — $F_{n+1}((-1)^n F_{n+1}) + F_n((-1)^{n+1} F_{n+2}) = 1$, donc $F_n \wedge F_{n+1} = 1$.
c) $F_{n+1} = F_n + F_{n-1}$, donc $\text{pgcd}(F_{n+1}, F_n) = \text{pgcd}(F_n, F_{n+1} - F_n) = \text{pgcd}(F_n, F_{n-1})$.
 — Par récurrence descendante : $\text{pgcd}(F_{n+1}, F_n) = \dots = \text{pgcd}(F_1, F_0) = \text{pgcd}(1, 0) = 1$.
 — **Remarque** : l'algorithme d'Euclide appliqué à deux Fibonacci consécutifs ne fait que des quotients égaux à 1 : c'est le **pire cas** de l'algorithme (théorème de Lamé).
d) Valeurs : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144 (jusqu'à F_{12}), puis $F_{18} = 2\,584$.
 — $\text{pgcd}(144, 2\,584)$: $2\,584 = 17 \times 144 + 136$, $144 = 1 \times 136 + 8$, $136 = 17 \times 8$. PGCD = 8 = F_6 ✓ ($\text{pgcd}(12, 18) = 6$).

Réponse. $F_{n+1}^2 - F_n F_{n+2} = (-1)^n$; $F_n \wedge F_{n+1} = 1$; $\text{pgcd}(144, 2\,584) = 8 = F_6$.

Correction de l'exercice 4 - Irrationalité par le lemme de Gauss

- a)** Si $\sqrt{2} = \frac{p}{q}$ (irréductible, $q \geq 1$), alors $p^2 = 2q^2$: $2 \mid p^2$. Comme 2 est premier, $2 \mid p$ (lemme d'**Euclide**, cas particulier de Gauss). On écrit $p = 2p'$:

$$4p'^2 = 2q^2 \Leftrightarrow q^2 = 2p'^2$$

 — Donc $2 \mid q^2$ puis $2 \mid q$: 2 divise p et q , ce qui contredit $p \wedge q = 1$. $\sqrt{2}$ est irrationnel.
b) Supposons $\sqrt{n} = \frac{p}{q}$ irréductible, donc $p^2 = nq^2$. Alors $q^2 \mid p^2$.
 — $p \wedge q = 1$ entraîne $p^2 \wedge q^2 = 1$ (les facteurs premiers de q^2 sont ceux de q , absents de p). Un diviseur de p^2 premier avec p^2 vaut 1 : $q^2 = 1$, $q = 1$.

— Alors $n = p^2$ est un carré parfait : contradiction.

c) $\log_{10} 2 > 0$. Si $\log_{10} 2 = \frac{p}{q}$ avec $p, q \in \mathbb{N}^*$, alors $10^{p/q} = 2$, soit $10^p = 2^q$.

— Or 5 divise 10^p ($p \geq 1$) mais ne divise pas 2^q (décomposition en facteurs premiers **unique**) : contradiction.

d) Si $r = \sqrt{2} + \sqrt{3}$ était rationnel, alors $r^2 = 5 + 2\sqrt{6}$ le serait, donc $\sqrt{6} = \frac{r^2 - 5}{2}$ aussi.

— Or 6 n'est pas un carré parfait ($2^2 < 6 < 3^2$) : $\sqrt{6}$ est irrationnel par b). Donc $\sqrt{2} + \sqrt{3}$ est **irrationnel**.

— **Méthode** : un raisonnement par l'absurde avec une fraction **irréductible**, puis un argument de divisibilité.

Réponse. $\sqrt{2}$, $\sqrt{n}$ (n non carré), $\log_{10} 2$ et $\sqrt{2} + \sqrt{3}$ sont irrationnels.

Correction de l'exercice 5 - PGCD et PPCM imposés

a) Si k divise a' et b' , alors dk divise a et b , donc $dk \leq d$ et $k = 1$: $a' \wedge b' = 1$.

— $m = da'b'$ est un multiple commun ($m = ab' = a'b$). Tout multiple commun M s'écrit $M = ak = da'k$ avec $db' \mid da'k$, soit $b' \mid a'k$; par **Gauss** ($a' \wedge b' = 1$), $b' \mid k$, donc $m = da'b' \mid M$. Ainsi $\text{ppcm}(a, b) = da'b'$, et $\text{pgcd} \times \text{ppcm} = ab$.

b) $a = 12a'$, $b = 12b'$, $a' \wedge b' = 1$ et $12a'b' = 360$, soit :

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

— $30 = 2 \times 3 \times 5$. Les couples premiers entre eux de produit 30 : (1, 30), (2, 15), (3, 10), (5, 6).

— **Solutions** : (12, 360), (24, 180), (36, 120), (60, 72).

— **Contrôle** sur (60, 72) : $60 = 2^2 \times 3 \times 5$, $72 = 2^3 \times 3^2$; PGCD $2^2 \times 3 = 12$ ✓, PPCM $2^3 \times 3^2 \times 5 = 360$ ✓

c) $a = 18a'$, $b = 18b'$: $a' + b' = 8$, $a' \wedge b' = 1$, $a' \leq b'$.

— Candidats : (1, 7) ✓, (2, 6) ✗ (PGCD 2), (3, 5) ✓, (4, 4) ✗.

— **Solutions** : (18, 126) et (54, 90).

d) Le PGCD divise toujours le PPCM ; or $12 \nmid 100$. **Aucun** couple.

— **Méthode** : on se ramène toujours à des entiers **premiers entre eux** en divisant par le PGCD.

Réponse. b) (12, 360), (24, 180), (36, 120), (60, 72) ; c) (18, 126), (54, 90) ; d) impossible.

Correction de l'exercice 6 - Divisibilité par 30

a) $a \mid c$: on écrit $c = ak$. Alors $b \mid ak$ et $b \wedge a = 1$, donc par le lemme de **Gauss** $b \mid k$, $k = bk'$ et $c = abk'$: $ab \mid c$.

— **Contre-exemple** sans l'hypothèse : $4 \mid 12$ et $6 \mid 12$ mais $24 \nmid 12$.

b) $n^5 - n = n(n^4 - 1) = n(n^2 - 1)(n^2 + 1) = (n - 1)n(n + 1)(n^2 + 1)$.

c) $30 = 2 \times 3 \times 5$, facteurs **deux à deux premiers entre eux** : il suffit, par a) appliqué deux fois, de montrer que 2, 3 et 5 divisent $n^5 - n$.

— **Par 2 et 3** : $(n - 1)n(n + 1)$ est un produit de trois entiers consécutifs ; l'un est pair et l'un est multiple de 3.

— **Par 5** : on raisonne sur le reste de n modulo 5. Si $n \equiv 0, 1, 4$, l'un des facteurs n , $n - 1$, $n + 1$ est divisible par 5. Si $n \equiv 2$ ou 3, alors $n^2 \equiv 4$ et $n^2 + 1 \equiv 0 \pmod{5}$.

$$2 \mid n^5 - n, \quad 3 \mid n^5 - n, \quad 5 \mid n^5 - n \implies 30 \mid n^5 - n$$

— **Autre preuve** pour 5 : petit théorème de Fermat, $n^5 \equiv n \pmod{5}$.

d) $n = 2$: $32 - 2 = 30 \checkmark$; $n = 3$: $243 - 3 = 240 = 30 \times 8 \checkmark$; $n = 7$:
 $16\,807 - 7 = 16\,800 = 30 \times 560 \checkmark$

Réponse. $n^5 - n = (n - 1)n(n + 1)(n^2 + 1)$ est divisible par 2, 3 et 5, donc par 30.

Correction de l'exercice 7 - Euclide étendu en tableau

a) Divisions successives :

— $1\,769 = 3 \times 551 + 116$; $551 = 4 \times 116 + 87$; $116 = 1 \times 87 + 29$; $87 = 3 \times 29 + 0$.
 — Le dernier reste non nul est $d = 29$.

b) On remonte en exprimant chaque reste :

— $29 = 116 - 87 = 116 - (551 - 4 \times 116) = 5 \times 116 - 551$;
 — $= 5(1\,769 - 3 \times 551) - 551 = 5 \times 1\,769 - 16 \times 551$.

— **Vérification** : $8\,845 - 8\,816 = 29 \checkmark$ Donc $u = 5$, $v = -16$.

c) Chaque ligne s'obtient par $L_{k+1} = L_{k-1} - q_k L_k$ (le quotient q_k est celui de r_{k-1} par r_k) :

r_k	u_k	v_k	q_k
1 769	1	0	.
551	0	1	3
116	1	-3	4
87	-4	13	1
29	5	-16	3

— La dernière ligne donne directement $29 = 5 \times 1\,769 - 16 \times 551$, sans « remonter » :
 c'est la version programmable.

d) On divise par 29 : $1\,769 = 29 \times 61$ et $551 = 29 \times 19$, avec $61 \wedge 19 = 1$. Si
 $1\,769u + 551v = 29$, alors $61u + 19v = 1 = 61 \times 5 + 19 \times (-16)$, d'où
 $61(u - 5) = 19(-16 - v)$.

— Par **Gauss**, $19 \mid u - 5$: $u = 5 + 19k$, puis $v = -16 - 61k$.

$$(u, v) = (5 + 19k, -16 - 61k), \quad k \in \mathbb{Z}$$

Réponse. $d = 29 = 5 \times 1\,769 - 16 \times 551$; solutions $(5 + 19k, -16 - 61k)$.

Correction de l'exercice 8 - Trois nombres premiers dans leur ensemble

a) $6 \wedge 10 = 2$, $6 \wedge 15 = 3$, $10 \wedge 15 = 5$: aucun des trois couples n'est formé de nombres premiers entre eux.

— Un diviseur commun aux trois divise $6 \wedge 10 = 2$ et 15, donc divise $\text{pgcd}(2, 15) = 1$: les trois nombres sont **premiers entre eux dans leur ensemble**.

b) On combine : $6 + 10 = 16 = 15 + 1$, donc

$$6 \times 1 + 10 \times 1 + 15 \times (-1) = 1$$

— **Méthode systématique** : Bézout pour $(6, 10)$ donne $2 = 6 \times 2 - 10 \times 1$; puis Bézout pour $(2, 15)$: $1 = 15 - 7 \times 2 = 15 - 7(6 \times 2 - 10) = 15 - 14 \times 6 + 7 \times 10$. Autre solution : $(u, v, w) = (-14, 7, 1) \checkmark$ ($-84 + 70 + 15 = 1$).

c) On multiplie la relation par n : $n = 6n + 10n + 15 \times (-n)$, soit $(x, y, z) = (n, n, -n)$.

d) Un entier divise a , b et c si et seulement s'il divise $\text{pgcd}(a, b)$ et c (car les diviseurs communs de a et b sont exactement les diviseurs de leur PGCD). Les deux ensembles de

diviseurs communs coïncident, donc leurs plus grands éléments aussi.

— Ici : $\text{pgcd}(\text{pgcd}(6, 10), 15) = \text{pgcd}(2, 15) = 1 \checkmark$

— **Piège** : « premiers entre eux dans leur ensemble » n'entraîne **pas** « deux à deux » ; l'exemple 6, 10, 15 est le contre-exemple standard.

Réponse. $\text{pgcd}(6, 10, 15) = 1$; $6 + 10 - 15 = 1$; $n = 6n + 10n - 15n$.

Correction de l'exercice 9 - Diviseurs d'une expression

a) $(n + 3)(n - 3) = n^2 - 9$, et $n^2 - 9 + 14 = n^2 + 5 \checkmark$

b) Si $n + 3 \mid n^2 + 5$, alors $n + 3$ divise la combinaison $(n^2 + 5) - (n - 3)(n + 3) = 14$. Réciproquement, si $n + 3 \mid 14$, il divise $(n + 3)(n - 3) + 14 = n^2 + 5$.

c) Les diviseurs de 14 dans $\mathbb{Z}$: $\pm 1, \pm 2, \pm 7, \pm 14$.

$$n + 3 \in \{-14, -7, -2, -1, 1, 2, 7, 14\} \Leftrightarrow n \in \{-17, -10, -5, -4, -2, -1, 4, 11\}$$

— **Vérifications** : $n = 4 : \frac{21}{7} = 3 \checkmark$; $n = 11 : \frac{126}{14} = 9 \checkmark$; $n = -17 : \frac{294}{-14} = -21 \checkmark$

— Il y a **huit** solutions ; oublier les diviseurs **négatifs** en ferait perdre quatre.

d) Division de $n^3 + 2$ par $n + 1$: $n^3 + 2 = (n + 1)(n^2 - n + 1) + 1$.

— Donc $n + 1 \mid n^3 + 2 \Leftrightarrow n + 1 \mid 1 \Leftrightarrow n + 1 = \pm 1 \Leftrightarrow n \in \{0, -2\}$.

— **Vérification** : $n = 0 : 1 \mid 2 \checkmark$; $n = -2 : -1 \mid -6 \checkmark$

— **Méthode** : le reste de la division par $n - a$ est $P(a)$; ici $P(-1) = 1$ et, en a), $(-3)^2 + 5 = 14$.

Réponse. $n \in \{-17, -10, -5, -4, -2, -1, 4, 11\}$; en d) $n \in \{0, -2\}$.

Correction de l'exercice 10 - Fractions irréductibles

a) Relation de Bézout qui élimine n :

$$3(14n + 3) - 2(21n + 4) = 42n + 9 - 42n - 8 = 1$$

— Le PGCD divise 1 : fraction irréductible (exercice des Olympiades internationales de 1959).

b) $\text{pgcd}(n + 7, n + 2) = \text{pgcd}(n + 2, 5)$, qui vaut 5 si $5 \mid n + 2$ et 1 sinon.

— Irréductible $\Leftrightarrow n \not\equiv 3 \pmod{5}$. **Contrôle** : $n = 3$ donne $\frac{10}{5}$, réductible $\checkmark$; $n = 4$ donne $\frac{11}{6}$, irréductible $\checkmark$

c) Par l'absurde : soit p premier divisant $a + b$ et ab . Par le lemme d'Euclide, $p \mid a$ ou $p \mid b$.

— Si $p \mid a$, alors $p \mid (a + b) - a = b$: p divise a et b , contradiction avec $a \wedge b = 1$. De même si $p \mid b$.

— Aucun nombre premier ne divise les deux : $(a + b) \wedge ab = 1$.

d) C'est c) appliqué à la fraction $\frac{a + b}{ab}$.

— $\frac{1}{2} + \frac{1}{3} = \frac{5}{6}$: ici $a = 2$, $b = 3$ et la somme des inverses $\frac{a + b}{ab} = \frac{5}{6}$ est bien irréductible $\checkmark$

— **Méthode** : pour prouver que deux nombres sont premiers entre eux, soit on exhibe une relation de Bézout (a), soit on raisonne sur un **facteur premier** commun (c).

Réponse. a) $3(14n + 3) - 2(21n + 4) = 1$; b) $n \not\equiv 3 \pmod{5}$; c) $(a + b) \wedge ab = 1$.

Correction de l'exercice 11 - Phares et engrenages

a) Les instants communs sont les multiples communs de 18 et 24 ; le premier après 0 est leur PPCM. Avec $18 = 2 \times 3^2$ et $24 = 2^3 \times 3$ (exposants **maximaux**) :

$$\text{ppcm}(18, 24) = 2^3 \times 3^2 = 72$$

— Ils émettent ensemble toutes les 72 **secondes**, soit à minuit 1 min 12 s.

b) $30 = 2 \times 3 \times 5$: $\text{ppcm}(18, 24, 30) = 2^3 \times 3^2 \times 5 = 360$ secondes, soit 6 **minutes**.

c) On compte les dents qui passent au point de contact : elles sont les mêmes pour les deux roues. Les dents marquées se retrouvent quand ce nombre est multiple de 42 **et** de 30 : $\text{ppcm}(42, 30) = 210$ dents.

— La grande roue a fait $\frac{210}{42} = 5$ tours (et la petite $\frac{210}{30} = 7$ tours).

d) Avec $d = \text{pgcd}(a, b)$, $a = da'$, $b = db'$ et $a' \wedge b' = 1$, on a vu que $\text{ppcm}(a, b) = da'b' = \frac{da' \cdot db'}{d} = \frac{ab}{d}$.

— **Vérification** : $\text{pgcd}(18, 24) = 6$ et $\frac{18 \times 24}{6} = 72$ ✓ ; $\text{pgcd}(42, 30) = 6$ et $\frac{42 \times 30}{6} = 210$ ✓

— **Piège** : pour trois nombres, $\text{ppcm}(a, b, c) \neq \frac{abc}{\text{pgcd}(a, b, c)}$ en général : ici $\frac{18 \times 24 \times 30}{6} = 2160 \neq 360$.

Réponse. a) 72 s ; b) 360 s ; c) 5 tours de la grande roue ; $\text{ppcm} = \frac{ab}{\text{pgcd}}$.

Correction de l'exercice 12 - Critères de divisibilité démontrés

a) $10 \equiv 1 \pmod{9}$, donc $10^i \equiv 1$ pour tout i (compatibilité avec les puissances) :

$$n = \sum_{i=0}^k a_i 10^i \equiv \sum_{i=0}^k a_i \pmod{9}$$

— n est divisible par 9 si et seulement si la somme de ses chiffres l'est ; comme $3 \mid 9$, la même congruence vaut modulo 3.

b) $10 \equiv -1 \pmod{11}$, donc $10^i \equiv (-1)^i$ et $n \equiv \sum (-1)^i a_i = a_0 - a_1 + a_2 - \dots \pmod{11}$.

c) Somme alternée en partant des unités : $2 - 5 + a - 8 + 3 = a - 8$.

— Il faut $11 \mid a - 8$ avec $0 \leq a \leq 9$, donc $a - 8 \in \{-8, \dots, 1\}$ contient seulement 0 comme multiple de 11 : $a = 8$.

— **Vérification** : $38852 = 11 \times 3532$ ✓

d) Somme des chiffres : $2 + x + 7 + x = 9 + 2x$. Il faut $9 \mid 9 + 2x$, soit $9 \mid 2x$, soit (Gauss, $9 \wedge 2 = 1$) $9 \mid x$: $x = 0$ ou $x = 9$.

— **Vérification** : $2070 = 9 \times 230$ ✓ et $2979 = 9 \times 331$ ✓

— **Méthode** : un critère de divisibilité par m vient toujours du reste de 10 (ou d'une puissance de 10) modulo m .

Réponse. $n \equiv \sum a_i [9]$, $n \equiv \sum (-1)^i a_i [11]$; $a = 8$; $x \in \{0, 9\}$.

Correction de l'exercice 13 - Premier avec un produit

a) Bézout : $au + bv = 1$ et $au' + cw = 1$. On multiplie membre à membre :

$$1 = (au + bv)(au' + cw) = a(uau' + ucw + bvu') + bc(vw)$$

— C'est une relation de Bézout entre a et bc : $a \wedge bc = 1$.

b) Par récurrence avec a) : $a \wedge b^n = 1$ (en prenant $c = b^{n-1}$), puis, les rôles étant symétriques, $b^n \wedge a^m = 1$.

c) $(n^2 + 1) - n \times n = 1$: relation de Bézout, donc $n \wedge (n^2 + 1) = 1$.

— Par b) : $n^3 \wedge (n^2 + 1)^5 = 1$.

— **Contrôle** $n = 2$: 8 et $5^5 = 3125$ sont premiers entre eux (le second est impair et seul 5 le divise) ✓

d) On décompose $ab = \prod p^{\gamma_p}$ avec tous les γ_p **pairs** (carré parfait).

— $a \wedge b = 1$: chaque premier p divise **au plus un** des deux nombres. Donc l'exposant de p dans a est soit 0, soit γ_p tout entier : il est pair.

— Tous les exposants de a sont pairs : a est un carré ; de même pour b .

— **Contre-exemple** sans l'hypothèse : $2 \times 8 = 16$ est un carré, mais ni 2 ni 8 n'en sont.

Réponse. $a \wedge b = a \wedge c = 1 \Rightarrow a \wedge bc = 1$; $a^m \wedge b^n = 1$; $n \wedge (n^2 + 1) = 1$; ab carré et $a \wedge b = 1 \Rightarrow a, b$ carrés.

Correction de l'exercice 14 - Somme des diviseurs et nombres parfaits

a) Les diviseurs de p^k sont $1, p, \dots, p^k$ (décomposition unique). Somme géométrique de raison $p \neq 1$:

$$\sigma(p^k) = 1 + p + \dots + p^k = \frac{p^{k+1} - 1}{p - 1}$$

b) $360 = 2^3 \times 3^2 \times 5$, facteurs deux à deux premiers entre eux :

— $\sigma(2^3) = 15$, $\sigma(3^2) = 13$, $\sigma(5) = 6$.

— $\sigma(360) = 15 \times 13 \times 6 = 1170$.

c) $q = 2^p - 1$ est premier et **impair**, donc $2^{p-1} \wedge q = 1$:

$$\sigma(n) = \sigma(2^{p-1})\sigma(q) = (2^p - 1)(q + 1) = (2^p - 1)2^p = 2n$$

— n est donc parfait.

d) $p = 2$: $q = 3$, $n = 2 \times 3 = 6$; diviseurs $1 + 2 + 3 + 6 = 12 = 2 \times 6$ ✓

— $p = 3$: $q = 7$, $n = 4 \times 7 = 28$; $1 + 2 + 4 + 7 + 14 + 28 = 56$ ✓

— $p = 5$: $q = 31$, $n = 16 \times 31 = 496$; $\sigma(496) = 31 \times 32 = 992 = 2 \times 496$ ✓

— **Remarques** : $p = 4$ ne convient pas ($2^4 - 1 = 15$ non premier). Euler a montré que **tous** les parfaits pairs sont de cette forme ; on ne sait pas s'il existe un parfait impair.

Réponse. $\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}$; $\sigma(360) = 1170$; $2^{p-1}(2^p - 1)$ parfait si $2^p - 1$ premier ; 6, 28, 496.

Correction de l'exercice 15 - Synthèse : les nombres de Mersenne

a) Avec $b = 1$ dans la factorisation du cours :

$$a^n - 1 = (a - 1)(a^{n-1} + \dots + a + 1)$$

— Le second facteur vaut au moins $a + 1 \geq 3 > 1$ (car $n \geq 2$). Si $a^n - 1$ est premier, ses seuls diviseurs positifs sont 1 et lui-même ; comme le second facteur est > 1 , il faut $a - 1 = 1$, soit $a = 2$.

b) $n = rs$: par la même factorisation avec $x = 2^r$,

— $2^n - 1 = (2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + \dots + 1)$, donc $2^r - 1 \mid 2^n - 1$.

— $1 < r < n$ donne $1 < 2^r - 1 < 2^n - 1$: diviseur **non trivial**.

c) Contraposée de b) : si n n'est pas premier ($n \geq 4$ composé), $2^n - 1$ a un diviseur non trivial, donc n'est pas premier.

d) $2^{11} - 1 = 2\,047 = 23 \times 89$: 11 est premier mais $2^{11} - 1$ ne l'est pas.

— $n = 2 : 3 \checkmark$; $n = 3 : 7 \checkmark$; $n = 4 : 15 = 3 \times 5 \text{ ✗}$; $n = 5 : 31 \checkmark$; $n = 6 : 63 \text{ ✗}$; $n = 7 : 127 \checkmark$ (aucun premier ≤ 11 ne le divise).

— **Bilan** : $n \in \{2, 3, 5, 7\}$. Ces nombres premiers $2^p - 1$ sont les **nombre de Mersenne premiers** ; ils donnent les nombres parfaits pairs de l'exercice précédent.

Réponse. $a = 2$ et n premier sont nécessaires ; $2\,047 = 23 \times 89$; premiers pour $n \in \{2, 3, 5, 7\}$.