Plaquette 2 – Degré, division euclidienne et restes

Polynômes — Prépa MPSI / MP2I (1re année)

Corrections détaillées

Boîte à outils

Degré et division euclidienne.

— $\deg(PQ) = \deg P + \deg Q$, $\deg(P \circ Q) = \deg P \times \deg Q$ (pour $\deg Q \geq 1$), et $\deg(P+Q) \leq \max(\deg P, \deg Q)$.

— **Division euclidienne** : pour $B \neq 0$, il existe un unique couple (Q, R) avec

$$A = BQ + R \qquad \text{et} \qquad \deg R < \deg B$$

— L'**unicité** transporte les propriétés : si A et B sont réels, Q et R le sont ; si A et B sont pairs, Q et R aussi.

— **Reste par** $X-a$: c'est $P(a)$. **Reste par** $(X-a)(X-b)$, $a \neq b$: $R = \alpha X + \beta$ avec $R(a) = P(a)$ et $R(b) = P(b)$.

— **Racine multiple du diviseur** : si $(X-a)^2 \mid B$, on écrit aussi $R'(a) = P'(a)$.

— **Formule de Taylor** : $P = \sum_k \frac{P^{(k)}(a)}{k!}(X-a)^k$; le reste de P par $(X-a)^m$ en est la troncature à l'ordre $m-1$.

— **Schéma de Horner** : $P(a)$ et le quotient par $X-a$ s'obtiennent en n multiplications.

— **Racines de l'unité** : $j = \mathrm{e}^{2\mathrm{i}\pi/3}$ vérifie $j^3 = 1$ et $1 + j + j^2 = 0$; $X^2 + X + 1 = (X-j)(X-j^2)$.

Correction de l'exercice 1 – Degré d'une différence

a) Par la formule du binôme, les termes en X^n se simplifient :

$$(X+1)^n - (X-1)^n = \sum_{k=0}^{n} \binom{n}{k}\left(1 - (-1)^{n-k}\right)X^k$$

— le coefficient de X^n est $1-1=0$, celui de X^{n-1} vaut $\binom{n}{n-1}(1+1) = 2n \neq 0$. Degré $n-1$, coefficient dominant $2n$.

b) Écrivons $P = aX^d + bX^{d-1} + \dots$ Dans $P(X+1) = a(X+1)^d + b(X+1)^{d-1} + \dots$, le coefficient de X^d est a et celui de X^{d-1} est $da + b$. En retranchant $P(X)$:

— X^d disparaît, et le coefficient de X^{d-1} vaut $da + b - b = da \neq 0$. Donc $\deg \Delta P = d - 1$.

c) Par b), $\deg \Delta P = 1$ impose $\deg P = 2$, et $2a = 1$: $P = \frac{1}{2}X^2 + bX$ (car $P(0) = 0$). La condition sur le coefficient constant de ΔP donne $a + b = 0$, soit $b = -\frac{1}{2}$:

— $P = \frac{X(X-1)}{2}$. Contrôle : $\frac{(X+1)X}{2} - \frac{X(X-1)}{2} = \frac{X \times 2}{2} = X$ ✓.

— En sommant $P(k+1) - P(k) = k$ pour $k = 0, \dots, n-1$ (somme télescopique) : $\sum_{k=0}^{n-1} k = P(n) - P(0) = \frac{n(n-1)}{2}$.

d) Si $\deg P \geq 1$, b) donne $\deg \Delta P = \deg P - 1 \geq 0$, donc $\Delta P \neq 0$. Les solutions sont les **constantes** (autre preuve : $P - P(0)$ s'annule en tout entier naturel, il a une infinité de racines).

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. a) degré $n-1$, dominant $2n$ · b) degré $d-1$, dominant da · c) $P = \frac{X(X-1)}{2}$, $\sum_{k<n} k = \frac{n(n-1)}{2}$ · d) les constantes.

Correction de l'exercice 2 – Division par un trinôme à paramètres

a) $X^3 - 1 = (X-1)(X^2+X+1) : X^3 \equiv 1$. Puis $X^4 - X = X(X^3-1) : X^4 \equiv X$. On utilise aussi $X^2 \equiv -X - 1$. Ces congruences sont compatibles avec somme et produit, car

$$A \equiv A' \text{ et } B \equiv B' \pmod{P} \Rightarrow AB - A'B' = A(B-B') + B'(A-A') \equiv 0$$

b) On remplace chaque puissance par son reste :

— $A \equiv X + a(-X-1) + bX + 1 = (1-a+b)X + (1-a)$.

Ce polynôme est de degré < 2 : c'est le reste, $R = (1-a+b)X + (1-a)$.

c) $R = 0 \Leftrightarrow 1-a = 0$ et $1-a+b = 0 \Leftrightarrow a = 1$, $b = 0$.

— Alors $A = X^4 + X^2 + 1 = (X^2+1)^2 - X^2 = (X^2+X+1)(X^2-X+1)$: le quotient est $X^2 - X + 1$.

— Contrôle par les racines : j est racine de A si et seulement si $j^4 + aj^2 + bj + 1 = j + aj^2 + bj + 1 = 0$; avec $j^2 = -1 - j$, on retrouve $(1-a+b)j + (1-a) = 0$, et $j \notin \mathbb{R}$ impose les deux conditions.

Réponse. $R = (1-a+b)X + (1-a)$; division exacte $\Leftrightarrow a = 1$, $b = 0$, et $X^4 + X^2 + 1 = (X^2+X+1)(X^2-X+1)$.

Correction de l'exercice 3 – Reste par un diviseur scindé

Le reste a un degré strictement inférieur à celui du diviseur ; on le détermine en évaluant aux racines :

$$A = BQ + R \Rightarrow A(r) = R(r) \text{ pour toute racine } r \text{ de } B$$

a) $X^2 - 3X + 2 = (X-1)(X-2)$, $R = \alpha X + \beta$.

— $X = 1$: $\alpha + \beta = 1$; $X = 2$: $2\alpha + \beta = 2^n$.

— Donc $\alpha = 2^n - 1$ et $\beta = 2 - 2^n$: $R = (2^n - 1)X + 2 - 2^n$.

— Contrôle $n = 2$: $R = 3X - 2$ et $X^2 = (X^2 - 3X + 2) + 3X - 2$ ✓.

b) $X^3 - X = X(X-1)(X+1)$ et $R = \alpha X^2 + \beta X + \gamma$.

— $X = 0$: $\gamma = 0$; $X = 1$: $\alpha + \beta = 1$; $X = -1$: $\alpha - \beta = (-1)^n$.

— n pair : $\alpha = 1$, $\beta = 0$, $R = X^2$. n impair : $\alpha = 0$, $\beta = 1$, $R = X$.

— Cohérent : $X^n - X^2 = X^2(X^{n-2} - 1)$ est divisible par $X(X^2-1)$ quand $n-2$ est pair.

c) Avec $A = (X-3)^{2n} + (X-2)^n - 2$: $A(3) = 0 + 1 - 2 = -1$ et $A(2) = 1 + 0 - 2 = -1$.

— $R = \alpha X + \beta$ prend la valeur -1 en 2 et en 3 : $\alpha = 0$, $\beta = -1$, donc $R = -1$, quel que soit n.

Réponse. a) $(2^n - 1)X + 2 - 2^n$ · b) X^2 si n pair, X si n impair · c) -1.

Correction de l'exercice 4 – Reste modulo X² + 1 et formule de Moivre

a) $P = (X^2+1)Q + aX + b$ avec a, b **réels** (unicité de la division dans $\mathbb{R}[X]$, qui coïncide avec celle dans $\mathbb{C}[X]$). En évaluant en i :

$$P(\mathrm{i}) = a\,\mathrm{i} + b \qquad \text{donc} \qquad b = \mathrm{Re}P(\mathrm{i}), \quad a = \mathrm{Im}P(\mathrm{i})$$

b) $\mathrm{i}^{2026} = \mathrm{i}^{4\times 506 + 2} = -1$: le reste de X^{2026} est -1.

— $\mathrm{i}^{2027} + \mathrm{i}^{2025} = \mathrm{i}^{2025}(\mathrm{i}^2 + 1) = 0$: le reste est nul, et en effet $X^{2027} + X^{2025} = X^{2025}(X^2+1)$.

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) On évalue en i grâce à la formule de Moivre :

— $(\cos\theta + \mathrm{i}\sin\theta)^n = \mathrm{e}^{\mathrm{i}n\theta} = \cos(n\theta) + \mathrm{i}\sin(n\theta)$.

— Par a), le reste est $\cos(n\theta) + X\sin(n\theta)$.

Lecture : calculer modulo X^2+1, c'est calculer dans $\mathbb{C}$ en remplaçant X par i ; le résultat de c) est la formule de Moivre écrite « en polynômes ».

Réponse. $R = \mathrm{Re}P(\mathrm{i}) + X\mathrm{Im}P(\mathrm{i})$; restes -1 et 0 ; $\cos(n\theta) + X\sin(n\theta)$.

Correction de l'exercice 5 – Divisibilité par X² + X + 1

$X^2+X+1 = (X-j)(X-\bar{j})$ a deux racines **simples** conjuguées. Pour un polynôme réel A :

$$X^2+X+1 \mid A \Leftrightarrow A(j) = 0$$

— (si $A(j)=0$, alors $A(\bar{j}) = \overline{A(j)} = 0$).

a) $j^{3p} + j^{3q+1} + j^{3r+2} = 1 + j + j^2 = 0$: divisibilité.

b) j^n ne dépend que de n modulo 3 :

— $n \equiv 0$: $1+1+1 = 3 \neq 0$;

— $n \equiv 1$: $j^2 + j + 1 = 0$;

— $n \equiv 2$: $j^4 + j^2 + 1 = j + j^2 + 1 = 0$.

Divisibilité si et seulement si $3 \nmid n$.

c) $j+1 = -j^2 = \mathrm{e}^{\mathrm{i}\pi/3}$, donc $(j+1)^n - j^n - 1 = \mathrm{e}^{\mathrm{i}n\pi/3} - j^n - 1$ ne dépend que de n modulo 6. On teste $n = 0, \ldots, 5$, en notant $u = \mathrm{e}^{\mathrm{i}\pi/3}$ ($u^2 = j$, $u^3 = -1$) :

— $n \equiv 0$: $1-1-1 = -1$; $n \equiv 1$: $u - j - 1 = u + j^2 = 0$ ✓ ($j^2 = -u$) ;

— $n \equiv 2$: $j - j^2 - 1 = 2j \neq 0$; $n \equiv 3$: $-1-1-1 = -3$;

— $n \equiv 4$: $u^4 - j - 1 = -u - j - 1 = -u + j^2 = -2u \neq 0$; $n \equiv 5$: $u^5 - j^2 - 1 = -j^2 - j - 1 = 0$ ✓.

Divisibilité si et seulement si $n \equiv 1$ ou $5 \pmod 6$.

Réponse. a) oui · b) si et seulement si $3 \nmid n$ · c) si et seulement si $n \equiv \pm 1 \pmod 6$.

Correction de l'exercice 6 – Schéma de Horner

a) On développe $(X-\alpha)\sum_{k=0}^{n-1} b_k X^k = \sum_k b_k X^{k+1} - \sum_k \alpha b_k X^k$. Le coefficient de X^n est $b_{n-1} = a_n$; pour $1 \leq k \leq n-1$, celui de X^k est

$$b_{k-1} - \alpha b_k = a_k$$

— par définition des b_k ; le coefficient constant est $-\alpha b_0 = a_0 - r$. D'où l'égalité. Par unicité de la division, c'est la division de P par $X-\alpha$, et $r = P(\alpha)$.

b) On range les coefficients $2, -3, 0, 1, -5$:

coefficients	2	-3	0	1	-5
×2 puis +	2	$-3+4=1$	$0+2=2$	$1+4=5$	$-5+10=5$

— Quotient $2X^3 + X^2 + 2X + 5$, reste 5. Contrôle : $P(2) = 32 - 24 + 2 - 5 = 5$ ✓.

c) Horner fait une multiplication par coefficient : n multiplications (et n additions). Le calcul naïf de $a_k\alpha^k$ en calculant chaque puissance séparément coûte k multiplications pour le terme k, soit $\frac{n(n+1)}{2}$ au total (encore $2n-1$ en réutilisant les puissances). Horner, qui revient à écrire

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).

— $P(\alpha) = (\ldots((a_n\alpha + a_{n-1})\alpha + a_{n-2})\alpha + \ldots)\alpha + a_0$,

est optimal : c'est la méthode utilisée par les calculatrices.

Réponse. $r = P(\alpha)$; quotient $2X^3 + X^2 + 2X + 5$, reste 5 ; n multiplications.

Correction de l'exercice 7 – Divisibilité de $X^n - 1$ par $X^m - 1$

a) Avec $Y = X^m$, la factorisation $Y^q - 1 = (Y-1)(Y^{q-1} + \ldots + 1)$ donne

$$X^{qm} - 1 = (X^m - 1)\left(X^{(q-1)m} + \ldots + X^m + 1\right)$$

b) $X^n - 1 = X^r(X^{qm} - 1) + X^r - 1$. Le premier terme est multiple de $X^m - 1$ par a), et $\deg(X^r - 1) = r < m$ (ou $X^r - 1 = 0$ si $r = 0$). Par unicité, le reste est $X^r - 1$.

c) $X^m - 1 \mid X^n - 1 \Leftrightarrow X^r - 1 = 0 \Leftrightarrow r = 0 \Leftrightarrow m \mid n$.

d) $10 = 2 \times 4 + 2$: le reste de $X^{10} - 1$ par $X^4 - 1$ est $X^2 - 1$.

— $X^{100} = (X^{100} - 1) + 1$, avec $100 = 14 \times 7 + 2$: le reste de $X^{100} - 1$ est $X^2 - 1$, donc celui de X^{100} est X^2.

Analogie : c'est l'algorithme d'Euclide sur les exposants ; la partie suivante du chapitre en déduit $(X^m - 1) \wedge (X^n - 1) = X^{m \wedge n} - 1$.

Réponse. Reste $X^r - 1$; $X^m - 1 \mid X^n - 1 \Leftrightarrow m \mid n$; restes $X^2 - 1$ et X^2.

Correction de l'exercice 8 – Unicité de la division et symétries

Tout repose sur l'**unicité** du couple (Q, R) :

$$A = BQ + R, \quad \deg R < \deg B \quad \Rightarrow \quad (Q, R) \text{ unique}$$

a) On substitue $-X$: $A(-X) = B(-X)Q(-X) + R(-X)$, soit $A = B\,Q(-X) + R(-X)$, avec $\deg R(-X) = \deg R < \deg B$. C'est une autre division de A par B : par unicité, $Q(-X) = Q$ et $R(-X) = R$.

b) $A(-X) = -A$ donne $A = B(-Q(-X)) + (-R(-X))$, donc Q et R sont **impairs**.

c) $A = X^6 + 3X^2 + 1$ et $B = X^2 + 1$ sont pairs : R est pair, de degré < 2, donc constant. On évalue en i : $R = A(\mathrm{i}) = -1 - 3 + 1 = -3$.

— Contrôle : $X^6 + 3X^2 + 1 + 3 = X^6 + 3X^2 + 4$ s'annule en i ($-1 - 3 + 4 = 0$), donc est bien multiple de $X^2 + 1$ (réel, racines $\pm\mathrm{i}$).

d) L'algorithme de division n'effectue que des opérations rationnelles sur les coefficients (divisions par le coefficient dominant de B) : il produit $Q_0, R_0 \in \mathbb{Q}[X]$. Par unicité dans $\mathbb{R}[X]$, ce sont les mêmes que Q et R.

Réponse. Symétries transmises par unicité : A, B pairs $\Rightarrow Q, R$ pairs ; A impair, B pair $\Rightarrow Q, R$ impairs ; reste -3 ; coefficients rationnels.

Correction de l'exercice 9 – Polynômes à coefficients entiers

a) Pour chaque monôme, $a^k - b^k = (a-b)\sum_{i=0}^{k-1} a^i b^{k-1-i}$, avec une somme entière. Donc, en écrivant $P = \sum c_k X^k$:

$$P(a) - P(b) = \sum_k c_k\left(a^k - b^k\right) \text{ est multiple de } a - b$$

b) $3 - 1 = 2$ devrait diviser $P(3) - P(1) = 3$: **impossible**.

c) Soit k un entier et $\varepsilon \in \{0, 1\}$ de même parité que k. Alors $2 \mid k - \varepsilon$, donc $2 \mid P(k) - P(\varepsilon)$ par a) : $P(k)$ a la parité de $P(\varepsilon)$, qui est **impair**. Donc $P(k) \neq 0$: aucune racine entière.

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).

— Exemple : $X^3 + X + 1$ ($P(0) = 1$, $P(1) = 3$) n'a pas de racine entière.

d) $15 - 7 = 8$ devrait diviser $9 - 5 = 4$: impossible.

Portée : la propriété a) est une condition **nécessaire** ; elle sert surtout à prouver des impossibilités, comme en b) et d).

Réponse. $a - b \mid P(a) - P(b)$; b) non ($2 \nmid 3$) ; c) $P(k)$ toujours impair ; d) non ($8 \nmid 4$).

Correction de l'exercice 10 – Degré d'une composée

a) Si $P = \sum_{k \le p} a_k X^k$ avec $a_p \neq 0$ et Q de degré q et de coefficient dominant b, alors Q^k est de degré kq, et dans $P \circ Q = \sum a_k Q^k$ seul le terme $k = p$ atteint le degré pq, avec le coefficient $a_p b^p \neq 0$.

$$\deg(P \circ Q) = \deg P \times \deg Q$$

b) P n'est pas constant (sinon $P \circ P$ le serait). Par a), $(\deg P)^2 = 1$, donc $P = aX + b$ avec $a \neq 0$. Alors $P \circ P = a^2 X + ab + b$:

— $a^2 = 1$ et $b(a + 1) = 0$. Solutions : $P = X$, ou $a = -1$ et b quelconque, $P = -X + b$ (symétries de centre $\frac{b}{2}$).

c) Avec $P = \sum a_k X^k$: $P(2X) = \sum 2^k a_k X^k$. L'identification donne $2^k a_k = 2a_k$, soit $a_k = 0$ pour $k \neq 1$. Solutions : $P = aX$.

d) $P = 0$ convient. Si $\deg P = d$, le degré de gauche est $2d$ et celui de droite $d + 2$: $d = 2$. Avec $P = aX^2 + bX + c$:

— $P(X^2) = aX^4 + bX^2 + c$ et $X^2 P(X) = aX^4 + bX^3 + cX^2$. Identification : $b = 0$, $b = c$, $c = 0$.

Solutions : $P = aX^2$, $a \in \mathbb{R}$.

Réponse. $\deg(P \circ Q) = \deg P \deg Q$; b) $P = X$ ou $P = -X + b$ · c) $P = aX$ · d) $P = aX^2$.

Correction de l'exercice 11 – Reste par $(X - 1)^3$ et formule de Taylor

a) Les dérivées de X^n en 1 sont $\frac{n!}{(n-k)!}$, d'où, par la formule de Taylor,

$$X^n = \sum_{k=0}^{n} \binom{n}{k} (X - 1)^k$$

— (c'est aussi le binôme appliqué à $X = 1 + (X - 1)$). Les termes $k \geq 3$ sont multiples de $(X - 1)^3$; les autres forment un polynôme de degré ≤ 2 : c'est le reste,

$$R = 1 + n(X - 1) + \frac{n(n-1)}{2}(X - 1)^2$$

b) $n = 3$: $R = 1 + 3(X - 1) + 3(X - 1)^2$, et $X^3 - R = (X - 1)^3$ par le binôme ✓.

c) $P(2) = 8 - 4 + 1 = 5$, $P' = 3X^2 - 2$ donne $P'(2) = 10$, $P'' = 6X$ donne $\frac{P''(2)}{2} = 6$, et $\frac{P'''(2)}{6} = 1$:

— $P = (X - 2)^3 + 6(X - 2)^2 + 10(X - 2) + 5$.
— Contrôle en $X = 3$: $27 - 6 + 1 = 22$ et $1 + 6 + 10 + 5 = 22$ ✓.

Méthode : le reste par $(X - a)^m$ est la partie de degré $< m$ du développement de Taylor en a.

Réponse. $R = 1 + n(X - 1) + \frac{n(n-1)}{2}(X - 1)^2$; $P = (X - 2)^3 + 6(X - 2)^2 + 10(X - 2) + 5$.

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).

Correction de l'exercice 12 – Reste par $X^2 - 2X\cos\theta + 1$

a) $\Delta' = \cos^2\theta - 1 = -\sin^2\theta < 0$: racines $\cos\theta \pm i\sin\theta = e^{\pm i\theta}$, distinctes car $\sin\theta \neq 0$.

b) $R = aX + b$ avec a, b réels, et en évaluant en $e^{i\theta}$:

$$a\,e^{i\theta} + b = e^{in\theta}$$

— Partie imaginaire : $a\sin\theta = \sin(n\theta)$, donc $a = \dfrac{\sin(n\theta)}{\sin\theta}$.

— Partie réelle : $b = \cos(n\theta) - a\cos\theta = \dfrac{\cos(n\theta)\sin\theta - \sin(n\theta)\cos\theta}{\sin\theta} = -\dfrac{\sin((n-1)\theta)}{\sin\theta}$.

(L'évaluation en $e^{-i\theta}$ donne l'équation conjuguée : rien de nouveau.)

$$R = \frac{\sin(n\theta)X - \sin((n-1)\theta)}{\sin\theta}$$

c) $n = 1$: $R = \dfrac{\sin\theta X - 0}{\sin\theta} = X$ ✓. $n = 2$: $\sin 2\theta = 2\sin\theta\cos\theta$, donc $R = 2\cos\theta X - 1$, et $X^2 = B + 2X\cos\theta - 1$ ✓.

d) $\theta = \dfrac{\pi}{2}$: $B = X^2 + 1$ et $R = \sin\dfrac{n\pi}{2}X - \sin\dfrac{(n-1)\pi}{2} = \sin\dfrac{n\pi}{2}X + \cos\dfrac{n\pi}{2}$; pour $n = 2026$, $\sin(1013\pi) = 0$ et $\cos(1013\pi) = -1$: $R = -1$, comme trouvé directement.

Réponse. Racines $e^{\pm i\theta}$; $R = \dfrac{\sin(n\theta)X - \sin((n-1)\theta)}{\sin\theta}$.

Correction de l'exercice 13 – Quotient par $X - a$ et dérivée

a) Pour chaque monôme, on factorise :

$$X^k - a^k = (X-a)\left(X^{k-1} + aX^{k-2} + \ldots + a^{k-1}\right)$$

— donc $P - P(a) = \sum a_k(X^k - a^k) = (X-a)Q$ avec le Q annoncé ; comme $\deg P(a) < 1$, c'est la division euclidienne, de reste $P(a)$.

b) En $X = a$, chaque parenthèse vaut $k\,a^{k-1}$ (k termes égaux) : $Q(a) = \sum k a_k a^{k-1} = P'(a)$.

— a est racine double (au moins) $\Leftrightarrow (X-a)^2 \mid P \Leftrightarrow P(a) = 0$ et $(X-a) \mid Q \Leftrightarrow P(a) = 0$ et $P'(a) = 0$. On retrouve le critère par les dérivées.

c) $P(1) = 1 - 5 + 4 = 0$. Division (Horner avec les coefficients $1, 0, -5, 4, 0$) :

— 1 ; $0 + 1 = 1$; $-5 + 1 = -4$; $4 - 4 = 0$; $0 + 0 = 0$: $Q = X^3 + X^2 - 4X$ et reste 0.

— $Q(1) = 1 + 1 - 4 = -2$, et $P'(1) = 4 - 10 + 4 = -2$ ✓. $Q(1) \neq 0$: 1 est racine **simple** de P.

En fait $P = X(X-1)(X^2 + X - 4)$.

Réponse. $Q(a) = P'(a)$; racine double $\Leftrightarrow P(a) = P'(a) = 0$; $Q = X^3 + X^2 - 4X$, $Q(1) = -2$: racine simple.

Correction de l'exercice 14 – Polynômes et arithmétique des restes

a) $A + B - (A' + B') = (A - A') + (B - B')$, et, en ajoutant et retranchant $A'B$,

$$AB - A'B' = (A - A')B + A'(B - B')$$

— les deux termes sont multiples de P.

b) $X^2 + X + 2 \equiv 1\ [X^2 + X + 1]$, donc par a), $(X^2 + X + 2)^{10} \equiv 1^{10} = 1$: le reste est 1.

c) $(X+1)^2 = X^2 + 2X + 1 \equiv 2X\ [X^2 + 1]$. Donc $(X+1)^4 \equiv 4X^2 \equiv -4$, puis

— $(X+1)^7 = (X+1)^4(X+1)^2(X+1) \equiv -4 \times 2X \times (X+1) = -8X^2 - 8X \equiv 8 - 8X$.

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).

— Contrôle par évaluation en i : $(1+\mathrm{i})^7 = \left(\sqrt{2}\,\mathrm{e}^{\mathrm{i}\pi/4}\right)^7 = 8\sqrt{2}\,\mathrm{e}^{7\mathrm{i}\pi/4} = 8-8\mathrm{i}$, soit $R(\mathrm{i}) = 8-8\mathrm{i}$ ✓.

d) Les racines de X^2-X+1 sont $-j$ et $-\bar{j}$, de module 1 et d'ordre 6 : $(-j)^6 = j^6 = 1$. Pour $6 \mid n$, $(-j)^{2n} + (-j)^n + 1 = 1+1+1 = 3 \neq 0$: pas de divisibilité.

Réponse. Congruences compatibles ; b) 1 · c) $8-8X$ · d) la valeur en $-j$ vaut $3 \neq 0$.

Correction de l'exercice 15 – Synthèse : X^n modulo X^2-X-1 et Fibonacci

a) Pour $n=1$: $X = 0\times B + F_1 X + F_0$ ✓. Si $X^n \equiv F_n X + F_{n-1}$ $[B]$, on multiplie par X et on utilise $X^2 \equiv X+1$:

$$X^{n+1} \equiv F_n X^2 + F_{n-1}X \equiv F_n(X+1) + F_{n-1}X = F_{n+1}X + F_n$$

— de degré < 2 : c'est le reste. La récurrence est établie.

b) $F_9 = 34$, $F_{10} = 55$ (suite $0,1,1,2,3,5,8,13,21,34,55$) : le reste est $55X+34$.

c) $X^n = BQ + F_nX + F_{n-1}$ évalué en φ (où B s'annule) donne $\varphi^n = F_n\varphi + F_{n-1}$; de même $\psi^n = F_n\psi + F_{n-1}$. En soustrayant :

— $\varphi^n - \psi^n = F_n(\varphi-\psi) = F_n\sqrt{5}$, d'où $F_n = \dfrac{\varphi^n-\psi^n}{\sqrt{5}}$.

d) $|\psi| = \dfrac{\sqrt{5}-1}{2} \approx 0{,}618 < 1$, donc $\left|\dfrac{\psi^n}{\sqrt{5}}\right| < \dfrac{1}{\sqrt{5}} < \dfrac{1}{2}$: F_n est à distance $< \frac{1}{2}$ de $\dfrac{\varphi^n}{\sqrt{5}}$.

— Contrôle $n=10$: $\varphi^{10} \approx 122{,}99$ et $\dfrac{122{,}99}{2{,}236} \approx 55{,}004$; l'entier le plus proche est $55 = F_{10}$ ✓.

Réponse. $X^n \equiv F_nX + F_{n-1}$ $[X^2-X-1]$; reste de X^{10} : $55X+34$; $F_n = \dfrac{\varphi^n-\psi^n}{\sqrt{5}}$, entier le plus proche de $\dfrac{\varphi^n}{\sqrt{5}}$.

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).