11 Solutions des exercices

I. Algèbre générale

11.1 Arithmétique dans $\mathbb{Z}$

Exercice 1.1.

1. Notons d le plus grand commun diviseur de a et b. Puisque δ est un diviseur commun à a et b, δ divise d. Comme d divise a et b, il existe deux entiers relatifs a' et b' tels que $a = da'$ et $b = db'$. Donc $\delta = au + bv = d(a'u + b'v)$ et d divise δ. Par suite $|\delta| = d$.
2. On a $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$, donc $ca\mathbb{Z} + cb\mathbb{Z} = cd\mathbb{Z}$. On en déduit que cd est le plus grand commun diviseur de ca et cb.

   Par définition du plus petit commun multiple de a et b, on a $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, donc $c(a\mathbb{Z}) \cap c(b\mathbb{Z}) = cm\mathbb{Z}$. Donc cm est bien le plus petit commun multiple de ac et bc.
3. Écrivons $a = a'd$ et $b = b'd$ avec a' et b' premiers entre eux. Alors le plus petit commun multiple de a' et b' est $a'b'$, donc le plus petit commun multiple de a et b est $a'b'd$. On a bien $md = a'db'd = ab$.

Exercice 1.2.

1. Comme a divise c, il existe un entier relatif a' tel que $c = aa'$ et ainsi b divise aa' avec a et b premiers entre eux. On en déduit, d'après le théorème de Gauss, que b divise a'. Alors ab divise $aa' = c$.
2. On suppose que a est premier à b et à c, donc d'après le théorème de Bézout, il existe des entiers relatifs u, v, u' et v' tels que : $au + bv = 1$ et $au' + cv' = 1$. Donc : $1 = (au + bv)(au' + cv') = a(auu' + ucv' + u'bv) + (bc)(vv')$, avec $(auu' + ucv' + u'bv) \in \mathbb{Z}$ et $vv' \in \mathbb{Z}$; donc a est premier à bc.
3. a) • Démontrons que a et b^n sont premiers entre eux par récurrence sur n :
     ∗ Il n'y a rien à démontrer pour $n = 1$.
     ∗ Supposons que a et b^n ($n \in \mathbb{N}^*$) soient premiers entre eux. Alors, comme a et b sont premiers entre eux, d'après la question précédente, a et $b^n b = b^{n+1}$ sont premiers entre eux.
   • On en déduit immédiatement que a^n et b^n sont premiers entre eux en appliquant ce qui précède à b^n et à a.

   b) Comme d est le plus grand commun diviseur de a et b, il existe deux entiers relatifs a' et b' tels que $a = da'$ et $b = db'$, avec a' et b' premiers entre eux. D'après la question précédente, on a alors $a^n = d^n a'^n$ et $b^n = d^n b'^n$, avec a'^n et b'^n premiers entre eux. Ainsi le plus grand commun diviseur de a^n et b^n est d^n.
4. Notons d le plus grand commun diviseur de a et b et écrivons $a = ed$ et $b = ed$ avec e et b' premiers entre eux. Comme $ed = a|bc = db'c$, il vient $e|b'c$ et comme e et b' sont premiers entre eux, il vient $e|c$.

Exercice 1.3.

1. Puisque e et N sont premiers entre eux, la classe de e est inversible dans $\mathbb{Z}/N\mathbb{Z}$; il existe un unique $d \in \mathbb{Z}$, avec $0 \leqslant d \leqslant N - 1$ dont la classe est l'inverse de celle de e modulo N.
2. On peut écrire $ed = k(p-1) + 1$. Si n n'est pas divisible par p, alors $n^{p-1} \equiv 1 \ [p]$ (théorème de Fermat), donc $n^{k(p-1)} \equiv 1 \ [p]$ et enfin $n^{ed} \equiv n \ [p]$. Cela reste vrai si p divise n : dans ce cas p divise aussi n^{ed}. De même $n^{ed} \equiv n[q]$.
3. La réciproque de cette application est l'application qui à a associe le reste dans la division de a^d par pq.

Exercice 1.4.

1. Notons d le pgcd de a et b et $S_c = \{(x,y) \in \mathbb{Z}\times\mathbb{Z};\ ax+by=c\}$. On remarque d'abord que $S_c \neq \emptyset \iff c \in a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$. Autrement dit, l'équation admet des solutions si et seulement si c est multiple de d.

   Supposons que c est un multiple de d et soit (x_0,y_0) une solution particulière. Alors l'équation devient $a(x-x_0)+b(y-y_0)=0$, soit $(x-x_0,y-y_0)\in S_0$. Il reste à décrire S_0 et une méthode pour trouver une solution particulière.

   Écrivons $a=a'd$ et $b=b'd$. L'équation $ax+by=0$ est équivalente à $a'x+b'y=0$ et maintenant a' et b' sont premiers entre eux. Si (x,y) est solution, b' divise $a'x=-b'y$ et est premier avec a', donc b' divise x. On écrit $x=kb'$. Notre équation devient $a'kb'+b'y=0$, soit $y=-ka'$. Inversement, pour tout $k\in\mathbb{Z}$, on a $(kb',-ka')\in S_0$, donc $S_0=\{(kb',-ka');\ k\in\mathbb{Z}\}$. Enfin $S_c=\{(x_0-kb',y_0+ka');\ k\in\mathbb{Z}\}$.

   L'algorithme d'Euclide qui permet de trouver d,a',b', permet aussi de trouver une solution particulière (x_0,y_0). En effet, en remontant l'algorithme d'Euclide, on trouve (u,v) tels que $au+bv=d$. Si on écrit $c=c'd$ (puisque c est multiple de d), on pourra poser $x_0=c'u$ et $y_0=c'v$.

   Remarque : On peut partir de *n'importe quelle* solution particulière. Une telle solution particulière peut être évidente (par exemple, si $c=a+b$...).

   Discussion. Pour la suite de l'exercice a et b sont supposés premiers entre eux. Supposons $c\geqslant 0$ et décrivons les solutions positives ou nulles. Pour cela, remarquons qu'il existe un unique $u\in[0,b-1]\cap\mathbb{N}$ tel que $c-au\in b\mathbb{Z}$. En effet, u est le représentant dans $[0,b-1]$ du quotient de la classe de c par celle de a (qui est inversible) dans $\mathbb{Z}/b\mathbb{Z}$. Alors $c=au+bv$. Les solutions sont $(u+kb,v-ka),\ k\in\mathbb{Z}$. Comme $0\leqslant u<b$, les solutions positives sont $(u+kb,v-ka),\ k\in\mathbb{N},\ ka\leqslant v$. Si $v<0$, il n'y a pas de solutions positives ; si $v\geqslant 0$, les solutions positives sont données par les entiers $k\in[0,E(v/a)]$, soit $k\in[0,E((c-au)/ab)]$. Il y a alors exactement $E\Big(\dfrac{c-au}{ab}\Big)+1$ solutions.

2. L'équation $ax+by=ab$ admet les solutions positives $(b,0)$ et $(0,a)$. Par ce qui précède, si l'équation $ax+by=c$ admet deux solutions positives, alors $c-ax_0\geqslant ab$ donc $c\geqslant ab$. Le plus petit entier qui s'écrit de deux façons sous la forme $ax+by$ est donc ab.

3. De la discussion ci-dessus, il résulte que $c\in A$ si et seulement s'il existe $u\in[0,b-1]$ et $v\in\mathbb{N}^*$ tels que $c=au-bv$.

   a) On a $ab-a-b=a(b-1)-b$ donc $ab-b-a\in A$. Si $c\in A$, il existe $u\leqslant b-1$ et $v\geqslant 1$ tels que $c=au-bv$, donc $c\leqslant a(b-1)-b$. Donc le plus grand élément de A est $ab-a-b$.

   b) On a vu que $c\in A$ si et seulement s'il s'écrit sous la forme $c=ua-vb$ avec $0\leqslant u\leqslant b-1$ et $v\geqslant 1$. Remarquons que, puisque $c\geqslant 0$, on a $ua\geqslant vb$. Or $ua<ab$ donc $v<a$ soit $v\leqslant a-1$ et $vb>0$ donc $u>0$ soit $u\geqslant 1$. Cela prouve que tout élément de A s'écrit $ua-vb;\ (u,v)\in\mathbb{N}^2,\ 1\leqslant u\leqslant b-1;\ 1\leqslant v\leqslant a-1$.
   Inversement, tout élément positif qui s'écrit comme ça est dans A. Si $c=-(ua-bv)$ avec $1\leqslant u\leqslant b-1;\ 1\leqslant v\leqslant a-1$, alors on a $c=(b-u)a-(a-v)c$; puisque $1\leqslant b-u\leqslant b-1$ et $1\leqslant a-v\leqslant a-1$, il vient encore $c\in A$.

   c) Par ce qui précède, lorsque (u,v) décrit $[\![1,b-1]\!]\times[\![1,a-1]\!]$, $ua-bv$ décrit $A\cup -A$. Si $ua-bv=u'a-bv'$, alors $(u-u')a=b(v-v')$, et par le théorème de Gauss, b divise $u-u'$; or puisque $1\leqslant u,u'\leqslant b-1$, il vient $|u-u'|\leqslant b-2$, donc la seule possibilité est $u=u'$ et $v=v'$. On a donc une bijection de $[\![1,b-1]\!]\times[\![1,a-1]\!]$ sur $A\cup -A$. Il s'ensuit que A a exactement $\dfrac{(a-1)(b-1)}{2}$ éléments.
   Notons que ce nombre est entier, puisque a et b étant premiers entre eux, il ne peuvent être tous deux pairs.

4. a) Lorsque $a=7$ et $b=5$, on trouve $ab-a-b=35-7-5=23$.

b) Il y a $\dfrac{(3-1)(5-1)}{2} = 4$ scores impossibles avec 3 et 5 qui sont $1, 2, 4, 7$ (nos calculs donnent les nombres positifs de la forme $5u-3v$ avec $v > 0$ et $u = 1$ ou $u = 2$ soit $5-3$ et $10-3$, $10-6$ et $10-9$). Le nombre 7 étant la valeur d'un essai transformé, les seuls scores impossibles sont $1, 2, 4$.

Exercice 1.5. [un peu rapide]

1. On commence par une remarque : si $p_1, \dots, p_k$ sont des nombres premiers distincts et ξ_i, η_i des nombres entiers (pouvant être nuls), alors $x = \prod_{i=1}^{k} p_i^{\xi_i}$ divise $y = \prod_{i=1}^{k} p_i^{\eta_i}$ si et seulement pour out i on a $\xi_i \leqslant \eta_i$.
   En effet,
   - si les $\eta_i - \xi_i$ sont positifs ou nuls on a $y = x \prod_{i=1}^{k} p_i^{\eta_i - \xi_i}$ donc x divise y.
   - si x divise y, alors on écrit $y = xz$ où $z = \prod_{i=1}^{k} p_i^{\zeta_i}$. D'après l'unicité de la décomposition en nombres premiers, il vient $\eta_i = \xi_i + \zeta_i$.

   Écrivons $a = \prod p_i^{\alpha_i}$ et $b = \prod_{i=1}^{k} p_i^{\beta_i}$. Les diviseurs communs sont de la forme $c = \prod p_i^{\gamma_i}$ avec $\gamma_i \leqslant \alpha_i$ et $\gamma_i \leqslant \beta_i$. Il vient $d = \prod p_i^{\delta_i}$ avec $\delta_i = \inf(\alpha_i, \beta_i)$. De même, ou en utilisant la formule $dm = ab$, on a $m = \prod p_i^{\mu_i}$ avec $\mu_i = \sup(\alpha_i, \beta_i)$.
   Pour des petits nombres, cette façon de calculer le pgcd peut être plus rapide que l'algorithme d'Euclide. Par contre, pour des nombres relativement grands la décomposition en nombres premiers est « impraticable », contrairement à l'algorithme d'Euclide.
2. Posons $A = \{i;\ \alpha_i < \beta_i\}$, puis $a_1 = \prod_{i \in A} p_i^{\alpha_i}$, $a_2 = \prod_{i \notin A} p_i^{\alpha_i}$, $b_1 = \prod_{i \in A} p_i^{\beta_i}$ et $b_1 = \prod_{i \notin A} p_i^{\beta_i}$. On a bien
   - $a = a_1 a_2$, $b = b_1 b_2$;
   - $a_1 | b_1$ puisque pour $i \in A$ on a $\alpha_i < \beta_i$ et $b_2 | a_2$ puisque pour $i \notin A$ on a $\alpha_i \geqslant \beta_i$;
   - a_2 et b_1 n'ont pas de diviseurs premiers communs, ils sont donc premiers entre eux.
3. Le nombre $d' = a_1 b_2$ divise clairement a et b ; comme a/d' divise a_2 et b/d' divise b_1, donc a/d' et b/d' sont premiers entre eux. Donc $d' = d$. De l'égalité $ab = md$ il vient $a_2 b_1 = m$.
4. D'après le théorème chinois, on a des isomorphismes

$$\begin{aligned} \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z} &\simeq (\mathbb{Z}/a_1 \times \mathbb{Z}/a_2\mathbb{Z}) \times (\mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_2\mathbb{Z}) \\ &\simeq (\mathbb{Z}/a_1 \times \mathbb{Z}/b_2\mathbb{Z}) \times (\mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/a_2\mathbb{Z}) \\ &\simeq \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. \end{aligned}$$

Exercice 1.6.

1. Les premiers nombres de Fibonacci sont :

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55
n	11	12	13	14	15	16	17	18	19	20	21
F_n	89	144	233	377	610	987	1597	2584	4181	6765	10946

D'après ce tableau, les F_{3k} sont pairs, les F_{4k} sont multiples de 3 et les F_{5k} sont multiples de 5...

2. a) Démontrons que $F_m | F_{km}$ par récurrence sur k.
C'est vrai pour $k = 0$ (car $F_0 = 0$) et $k = 1$.
On sait que $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^p = \begin{pmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{pmatrix}$. Il vient, pour tout $p, q \in \mathbb{N}$,

$$\begin{pmatrix} F_{p-1} & F_p \\ F_p & F_{p+1} \end{pmatrix} \begin{pmatrix} F_{q-1} & F_q \\ F_q & F_{q+1} \end{pmatrix} = \begin{pmatrix} F_{p+q-1} & F_{p+q} \\ F_{p+q} & F_{p+q+1} \end{pmatrix}.$$

En particulier, on a $F_{p+q} = F_p F_{q-1} + F_{p+1} F_q$. Prenant $p = m$ et $q = km$, si F_p et F_q sont des multiples de F_m, il en va de même pour F_{p+q}.

b) Pour $n \in \mathbb{N}$, notons $M_2(\mathbb{Z}/n\mathbb{Z})$ l'anneau des matrices 2×2 à coefficients dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ et $G_n = GL(2, \mathbb{Z}/n\mathbb{Z})$ le groupe formé par les éléments inversibles de cet anneau, *i.e.* les matrices 2×2 à coefficients dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ inversibles. Notons aussi Δ_n le sous-groupe de G_n formé des matrices diagonales.

L'application $\psi : \mathbb{Z} \to G_n$ qui à k associe la classe dans $GL(2, \mathbb{Z}/n\mathbb{Z})$ de la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^k$ est un homomorphisme de groupes. Pour $k \in \mathbb{N}$ on a $n | F_k \iff \psi(k) \in \Delta_n$. En d'autres termes, on a

$$\{k \in \mathbb{N};\ n | F_k\} = \mathbb{N} \cap \psi^{-1}(\Delta_n).$$

Or, puisque Δ_n est un sous-groupe de G_n et ψ est un homomorphisme de groupes, $\psi^{-1}(\Delta_n)$ est un sous-groupe de $\mathbb{Z}$; il existe un unique élément $a \in \mathbb{N}$ tel que $\psi^{-1}(\Delta_n) = a\mathbb{Z}$, donc $\mathbb{N} \cap \psi^{-1}(\Delta_n) = a\mathbb{N}$. Enfin, puisque G_n est fini, ψ n'est pas injective ; son noyau n'est pas réduit à $\{0\}$ et est contenu dans $\psi^{-1}(\Delta_n)$, donc $a \neq 0$.

3. Soit $p \geqslant 7$ un nombre premier. Remarquons que $X^2 - X - 1$ admet une racine dans $\mathbb{F}_p$ si et seulement si 5 (le discriminant de ce trinôme) est un carré dans $\mathbb{F}_p$. En effet,
- Supposons qu'il existe $a \in \mathbb{F}_p$ tel que $a^2 = 5$. Comme $5 \neq 0$, il vient $a \neq 0$. De plus $p \neq 2$, donc 2 est inversible dans $\mathbb{F}_p$. Alors $\alpha = \dfrac{1+a}{2}$ et $\beta = \dfrac{1-a}{2}$ sont deux racines distinctes du polynôme $X^2 - X - 1$ dans $\mathbb{F}_p$.
- Supposons que $\alpha \in \mathbb{F}_p$ est racine du polynôme $X^2 - X - 1$; alors $\alpha^2 = \alpha + 1$, donc $(2\alpha - 1)^2 = 4\alpha^2 - 4\alpha + 1 = 4(\alpha + 1) - 4\alpha + 1 = 5$.

Notons J la matrice $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ à coefficients dans $\mathbb{F}_p$.

a) On suppose que 5 est un carré modulo p. Alors le polynôme caractéristique $X^2 - X - 1$ de J a deux racines distinctes α, β, donc J est diagonalisable. Il existe donc $P \in GL(2, \mathbb{F}_p)$ tel que $PJP^{-1} = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$. Par le petit théorème de Fermat on a $\alpha^{p-1} = \beta^{p-1} = 1$ (notons que α et β sont non nuls car J est inversible - son déterminant est -1). On a donc $J^{p-1} = P^{-1} \begin{pmatrix} \alpha^{p-1} & 0 \\ 0 & \beta^{p-1} \end{pmatrix} P = I_2$. La classe modulo p de $\begin{pmatrix} F_{p-2} & F_{p-1} \\ F_{p-1} & F_p \end{pmatrix}$ est donc I_2, et p divise F_{p-1}.

b) (i) L'ensemble K est un sous-espace vectoriel - donc un sous-groupe additif de $M_2(\mathbb{F}_p)$. Comme $J^2 = J + I_2$, pour $a, b, c, d \in \mathbb{F}_p$, on a

$$\begin{aligned} (aI_2 + bJ)(cI_2 + dJ) &= acI_2 + (ad + bc)J + bd(J + I_2) \\ &= (ac + bd)I_2 + (ad + bc + bd)J \end{aligned}$$

donc K est stable par le produit : c'est un sous-anneau de $M_2(\mathbb{F}_p)$. Comme I_2 et J commutent, l'anneau K est commutatif.

(ii) Pour $a \neq 0$, aI_2 est inversible dans K. On suppose que 5 n'est pas un carré modulo p. Alors le polynôme caractéristique $X^2 - X - 1$ de J n'a pas de racines dans $\mathbb{F}_p$. Donc bJ n'a pas de valeurs propres pour $b \neq 0$, donc $aI_2 + bJ$ est inversible dans $M_2(\mathbb{F}_p)$ pour $b \neq 0$. Or d'après la formule([3])

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \frac{1}{ad-bc}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \frac{1}{ad-bc}\left((a+d)I_2 - \begin{pmatrix} a & c \\ b & d \end{pmatrix}\right)$$

l'inverse d'une matrice inversible $A \in M_2(\mathbb{F}_p)$ est dans l'espace vectoriel engendré par I_2 et A ; donc $(aI_2 + bJ)^{-1} \in K$.
Cela prouve que K est un corps.

(iii) Posons $\varphi(x) = x^p$. On a $\varphi(I_2) = I_2$. Soient $x, y \in K$. Comme K est commutatif, on a $\varphi(xy) = \varphi(x)\varphi(y)$. La formule du binôme, puisque p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$, donne $\varphi(x+y) = \varphi(x) + \varphi(y)$.

(iv) Le polynôme $X^p - X$ admet dans K les p racines aI_2 avec $a \in \mathbb{F}_p$; comme un polynôme de degré k sur un corps commutatif K a au plus k racines, il n'en admet pas d'autre.

(v) D'après la question précédente, on a $J^p \neq J$. On a $J^2 = J + I_2$. Comme φ est un automorphisme de corps, il vient $\varphi(J^2) = \varphi(J) + I_2$.

(vi) Le polynôme $X^2 - X - 1$ admet dans K les racines J et $-J^{-1}$. Il ne peut en admettre d'autres donc J^p, qui est racine de ce polynôme et distinct de J est égal à $-J^{-1}$.

(vii) On a donc $J^{p+1} = -I_2$, en d'autres termes, la classe de $\begin{pmatrix} F_p & F_{p+1} \\ F_{p+1} & F_{p+2} \end{pmatrix}$ modulo p est $-I_2$.

Exercice 1.7.

1. Puisque $r_{n+1} = 0$, il vient $r_{n-1} = q_n r_n$; or $r_n < r_{n-1}$ (c'est un reste de division euclidienne), donc $q_n > 1$; enfin $q_n \geqslant 2$ (car c'est un entier).
2. a) L'égalité $r_{k-1} = q_k r_k + r_{k+1}$ se lit

$$(E_k) \qquad \begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}\begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_k \\ r_{k-1} \end{pmatrix}.$$

On procède par récurrence sur k. Pour $k = 1, \ldots, n$, notons (P_k) l'égalité

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}\begin{pmatrix} r_{k+1} \\ r_k \end{pmatrix} = \begin{pmatrix} r_1 \\ r_0 \end{pmatrix}.$$

L'identité (E_1) donne P_1.
Si (P_{k-1}) est vrai, l'identité (E_k) donne (P_k).

b) Ecrivons

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix} = \begin{pmatrix} a_k & c_k \\ b_k & d_k \end{pmatrix} = A_k.$$

On a $\begin{pmatrix} a_k & c_k \\ b_k & d_k \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_{k+1} \end{pmatrix} = \begin{pmatrix} a_{k+1} & c_{k+1} \\ b_{k+1} & d_{k+1} \end{pmatrix}$. Ce qui donne $a_{k+1} = c_k$, $b_{k+1} = d_k$,

3. Cette formule évidente est la formule de la comatrice en dimension 2. C'est aussi le théorème de Cayley-Hamilton en dimension 2.

c) et pour $1 \leqslant k \leqslant n-1$, $a_{k+2} = c_{k+1} = a_{k+1}q_{k+1}+a_k \geqslant a_{k+1}$ et, de même $b_{k+2} = b_{k+1}q_{k+1}+b_k \geqslant b_{k+1}$.
Pour $k = 1$, on trouve $a_1 = 0,\ a_2 = 1,\ b_1 = 1,\ b_2 = q_1$.
Si $n = 1$ on a $a_{n+1} = 1 > 2a_0 = 0$ et $b_{n+1} = q_n \geqslant 2 = 2b_n$.
Sinon, $b_{n+1} = q_n b_n + b_{n-1} \geqslant 2b_n + b_0 > 2b_n$ et $a_{n+1} = q_n a_n + a_{n-1} \geqslant 2a_n$ avec égalité possible si $a_{n-1} = 0$ ce qui impose $n = 1$ (car sinon $a_{n-1} \geqslant a_1 = 1$) et $a_2 = 2$.

d) La matrice A_k est produit de k matrices de déterminant -1. Son déterminant est $(-1)^k$.

e) L'égalité $A_n \begin{pmatrix} r_{n+1} \\ r_n \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ donne $\begin{pmatrix} r_{n+1} \\ r_n \end{pmatrix} = A_n^{-1} \begin{pmatrix} a \\ b \end{pmatrix}$. La formule de la comatrice donne $A_n^{-1} = (-1)^n \begin{pmatrix} b_{n+1} & -a_{n+1} \\ -b_n & a_n \end{pmatrix}$, ([4]) d'où le résultat.

3. a) L'égalité se démontre par récurrence sur k ; elle est vraie pour $k = 1$ car $F_0 = 0$, $F_1 = F_2 = 1$; si elle est vraie pour k, on a

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{k+1} = \begin{pmatrix} F_{k-1} & F_k \\ F_k & F_{k+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} F_k & F_{k-1}+F_k \\ F_{k+1} & F_k + F_{k+1} \end{pmatrix} = \begin{pmatrix} F_k & F_{k+1} \\ F_{k+1} & F_{k+2} \end{pmatrix}.$$

b) Les inégalités $b_k \geqslant F_k$ et $a_k \geqslant F_{k-1}$ se démontrent par récurrence forte sur k. Elles sont vraies pour $k = 1$ et $k = 2$. Si elles ont vraies pour k et $k+1$, on a $a_{k+2} = q_{k+1}a_{k+1} + a_k \geqslant a_{k+1} + a_k \geqslant F_k + F_{k-1} = F_{k+1}$ et $b_{k+2} = q_{k+1}b_{k+1} + b_k \geqslant b_{k+1} + b_k \geqslant F_{k+1} + F_k = F_{k+2}$.

4. On construit des suites a_k, b_k, r_k ; il suffit de garder en mémoire uniquement deux termes consécutifs de ces trois suites pour construire le suivant. On s'arrête quand $r_{n+1} = 0$; on a alors le pgcd de a, b (c'est r_n) et une relation de Bézout grâce à la question 2.e). La question 3 nous indique que la convergence est assez rapide : il faut moins de $k+1$ étapes si $b \leqslant F_k$. Or F_k croît géométriquement en k.

5. Puisque a et b sont premiers entre eux, il existe n tel que $r_n = 1$ et $r_{n+1} = 0$. On a donc

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Cela donne

$$\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix}.$$

6. Si on a une telle égalité, le calcul du déterminant nous donne une relation de Bézout $ub - va = (-1)^n$, donc a et b sont premiers entre eux. Démontrons par récurrence sur n que $a < b$ et que les quotients successifs de la division de a par b sont les q_j.
Si $n = 1$, on a $a = 1$ et $b = q_1 \geqslant 2$.
Supposons $n \geqslant 2$ et le cas de longueur $n-1$ traité. Ecrivons

$$\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & q_3 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & q_n \end{pmatrix} = \begin{pmatrix} u' & a' \\ v' & b' \end{pmatrix}.$$

D'après l'hypothèse de récurrence, $a' < b'$ et les quotients successifs de la division euclidienne de b' par a' sont $q_2, q_3, \ldots, q_n$. Or $\begin{pmatrix} u & a \\ v & b \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} \begin{pmatrix} u' & a' \\ v' & b' \end{pmatrix}$, soit $b' = a$ et $b = q_1 a + a'$. Donc le quotient de b par a est q_1 et le reste a', et la suite des quotients successifs de la division euclidienne de b par a est bien $q_1, q_2, \ldots, q_n$.

Exercice 1.8.

4. Plus généralement, pour une matrice 2×2 inversible on a $\begin{pmatrix} a & c \\ b & d \end{pmatrix}^{-1} = \dfrac{1}{ad-bc} \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}$.

1. a) Soit d le plus grand commun diviseur de a et b. Alors d^2 divise p, donc d divise p et $d \neq p$ soit $d = 1$.

   b) L'existence et unicité de $q_1, \ldots, q_n$ résultent de l'exercice 1.7.

   c) (*cf.* exerc. 1.7) Écrivons $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_{n-1} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, avec $\alpha, \beta\gamma \in \mathbb{N}$. Il vient $u = \beta$, $v = \gamma$, puis $a = q_n u + \alpha \geqslant 2u$ et $b = q_n v + \gamma \geqslant 2v$ (puisque $q_n \geqslant 2$).

   d) Écrivons $\begin{pmatrix} u & v \\ a & b \end{pmatrix}\begin{pmatrix} u & a \\ v & b \end{pmatrix} = \begin{pmatrix} x & \ell \\ k & p \end{pmatrix}$. Cette matrice est symétrique et donc $k = \ell$ et il est clair que $q = p$. On a $2\ell = 2(ua + bv) \leqslant p$ d'après la question précédente. Enfin le déterminant de cette matrice est 1 (c'est un produit pair de matrices de déterminant -1), donc $\ell^2 \equiv -1\ [p]$. Alors -1 a deux racines dans le corps $\mathbb{Z}/p\mathbb{Z}$: ℓ et $p - \ell$. Une seule des deux est $\leqslant p/2$.

2. D'après l'exercice 1.7, l'algorithme d'Euclide fournit un entier $m \in \mathbb{N}^*$, un m-uplet $(q_1, \ldots, q_m)$ d'entiers $\geqslant 1$ avec $q_m \geqslant 2$ et $\alpha, \beta \in \mathbb{N}$ tels que $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_m \end{pmatrix} = \begin{pmatrix} \alpha & \ell \\ \beta & p \end{pmatrix}$ et on a $\beta \leqslant p/2$. Prenant les déterminants, il vient $-\beta\ell \equiv (-1)^m\ [p]$, donc β est, au signe près l'inverse de ℓ modulo p, c'est à dire $\pm\ell$, et puisque $\beta < p/2$, il vient $\beta = \ell$ et m est pair. Prenant les transposées, on trouve $\begin{pmatrix} 0 & 1 \\ 1 & q_m \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_{m-1} \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix} = \begin{pmatrix} \alpha & \ell \\ \ell & p \end{pmatrix}$, et par unicité, on trouve $q_j = q_{m+1-j}$.

   Posons alors $m = 2k$ et $\begin{pmatrix} 0 & 1 \\ 1 & q_{k+1} \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_{k+2} \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_m \end{pmatrix} = \begin{pmatrix} u & a \\ v & b \end{pmatrix} = A$. On a $\begin{pmatrix} \alpha & \ell \\ \ell & p \end{pmatrix} = {}^tAA$, donc $p = a^2 + b^2$.

   Remarquons de plus que l'on a $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \ell \\ p \end{pmatrix}$. Comme la matrice $\begin{pmatrix} 0 & 1 \\ 1 & q_1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & q_2 \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & q_k \end{pmatrix}$ est inversible, $\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}$ d'après l'exercice 1.7. Notons aussi que $r_{k+2} \geqslant r_k + r_{k+1}$, donc $r_{k+2}^2 > p$. En d'autres termes, a et b sont les deux derniers restes inférieurs à $\sqrt{p}$ dans les divisions euclidiennes successives entre p et ℓ.

Exercice 1.9.

1. Pour $a \in \mathbb{Z}$ et $m \in \mathbb{N}$, on a $a \equiv 1\ [a-1]$, donc $a^m \equiv 1\ \ [a-1]$. De même $a \equiv -1\ \ [a+1]$, donc si m est impair, alors $a^m \equiv -1\ \ [a+1]$.

   Si k est un diviseur de n, prenant $a = 2^k$, on en déduit que $2^k - 1$ divise $2^n - 1$; donc si $2^n - 1$ est premier, on a $2^k - 1 = 1$ (*i.e.* $k = 1$) ou $2^k - 1 = 2^n - 1$, donc $k = n$. Autrement dit n est premier.

   Écrivons $n = 2^k m$ avec $k \in \mathbb{N}$ et m impair. Alors $2^{2^k} + 1$ divise $2^n + 1$, donc, si $2^n + 1$ est premier, alors $m = 1$.

2. On a $2^{2^k} \equiv -1\ [F_k]$, donc $2^{2^\ell} = (2^{2^k})^{2^{\ell-k}} \equiv 1\ [F_k]$. Enfin $F_\ell \equiv 2\ \ [F_k]$. Le pgcd de F_k et F_ℓ divise 2 et, puisque F_ℓ est impair, F_k et F_ℓ sont premiers entre eux.

3. Puisque $q | M_p$, on a $2^p \ \equiv 1\ \ [q]$. Donc l'ordre de 2 dans $\mathbb{F}_q^*$ divise p ; ce ne peut être que p. Or l'ordre de p divise l'ordre du groupe $\mathbb{F}_q^*$, donc p divise $q - 1$. Comme q est impair $2p | q - 1$.

4. Si M_{13} n'était pas premier, son plus petit diviseur non nul q serait $< \sqrt{M_{13}} < 64\sqrt{2} < 100$ et un nombre premier de la forme $26k + 1$. Comme 27 n'est pas premier, il reste à teste 53 et 79. Or $2^6 \equiv 11\ [53]$, donc $2^{12} \equiv 121 \equiv 15\ \ [53]$ et enfin $M_{13} \equiv 2 \times 15 - 1 = 29 \neq 0\ \ [53]$ et $2^6 \equiv -15\ [53]$, donc $2^{12} \equiv 225 \equiv -12\ \ [79]$ et enfin $M_{13} \equiv -2 \times 12 - 1 = -25 \neq 0\ \ [79]$.

5. a) On a $2^{2^\ell} \equiv -1\ [q]$, donc $2^{2^{\ell+1}} \equiv 1\ [q]$. L'ordre de 2 dans le groupe $\mathbb{F}_q^*$ divise $2^{\ell+1}$ et ne divise pas 2^ℓ : c'est $2^{\ell+1}$.

b) L'ordre de 2 dans le groupe $\mathbb{F}_q^*$ divise l'ordre de $\mathbb{F}_q^*$, donc $2^{\ell+1}$ divise $q-1$.

c) Comme ω^4 est la classe de 2^{2^ℓ}, on a $\omega^4 = -1$, donc $\omega^2 + \omega^{-2} = 0$, donc $(\omega+\omega^{-1})^2 = 2$. On a $(\omega+\omega^{-1})^{2^{\ell+1}} = -1$, donc l'ordre de $\omega+\omega^{-1}$ divise $2^{\ell+2}$ et ne divise pas $2^{\ell+1}$: c'est $2^{\ell+2}$. On en déduit que $2^{\ell+2}$ divise $q-1$.

d) Si q est le plus petit nombre premier divisant F_5, alors $q \simeq 1 \ [2^7]$. Or 3 divise 129 et $4\times128+1 = 513$ et 5 divise $3\times128+1 = 385$. Enfin, $2\times128+1 = 257 = F_3$ est un nombre de Fermat donc premier à F_5. Le premier nombre à tester est donc $5\times128+1$.

e) On a $2^4 \equiv -5^4 \ [641]$, donc $F_5 = 2^{28}2^4 + 1 \equiv 1 - 5^4 2^{28} \ [641]$.

f) On a $52^7 = 640 \equiv -1 \ [641]$, donc $5^4 2^{28} = (52^7)^4 \equiv 1 \ [641]$ et 641 divise F_5.

Exercice 1.10.

Le cas $b=4$: 1. Écrivons $a^2+1 = kp$. C'est une identité de Bézout prouvant que a et p sont premiers entre eux.

2. Puisque $p|a^2+1$, on en déduit que $x^2+1=0$, donc $x^4-1 = (x^2+1)(x^2-1) = 0$.

3. Comme $p \neq 2$, on a $-1 \neq 1$. Or $x^2 = -1$ donc $x^2 \neq 1$.

4. L'ordre de x dans le groupe multiplicatif $\mathbb{F}_p^*$ divise 4 mais ne divise pas 2 : c'est 4. On en déduit que 4 divise l'ordre de $\mathbb{F}_p^*$, donc que $p \equiv 1 \ [4]$.

5. Soit $n \in \mathbb{N}$, tel que $n \geqslant 2$. Posons $a = n!$ et soit p un diviseur premier de a^2+1. Alors p est premier avec a, donc $p > n$ et $p \equiv 1 \ [4]$. On en déduit que l'ensemble des nombres premiers congrus à 1 modulo 4 n'est pas majoré : il est infini.

6. Si $n \geqslant 4$, alors $4|n!$, donc $n! - 1 \equiv -1 \ [4]$. Écrivons $n!-1 = p_1^{\alpha_1}\dots p_k^{\alpha_k}$ la décomposition de $n!-1$ en nombres premiers. Comme ce produit est congru à 3 modulo 4, un au moins de ses facteurs n'est pas congru à 1. Il existe donc j tel que $p_j \equiv 3 \ [4]$. Comme p_j divise $n!-1$, il ne divise pas $n!$, donc $p_j > n$. On en déduit que l'ensemble des nombres premiers congrus à 3 modulo 4 n'est pas majoré : il est infini.

Le cas $b=6$: 1. Écrivons $a^2+a+1 = kp$, soit $kp-(a+1)a = 1$. C'est une identité de Bézout prouvant que a et p sont premiers entre eux.

2. Puisque $p|a^2+a+1$, on en déduit que $x^2+x+1=0$, donc $x^3-1 = (x^2+x+1)(x-1) = 0$.

3. Comme $p \neq 3$, on a et $1^2+1+1 \neq 0$, donc $x \neq 1$.

4. L'ordre de x dans le groupe multiplicatif $\mathbb{F}_p^*$ divise 3 mais n'est pas 1 : c'est 3. On en déduit que 3 divise l'ordre de $\mathbb{F}_p^*$, donc que $p \equiv 1 \ [3]$. En particulier, $p \neq 2$, donc p est impair : donc $p \equiv 1 \ [6]$.

5. Soit $n \in \mathbb{N}$, tel que $n \geqslant 3$. Posons $a = n!$ et soit p un diviseur premier de a^2+a+1. Alors p est premier avec a, donc $p > n$ et $p \equiv 1 \ [6]$. On en déduit que l'ensemble des nombres premiers congrus à 1 modulo 6 n'est pas majoré : il est infini.

6. Si $n \geqslant 3$, alors $3|n!$, donc $n! - 1 \equiv -1 \ [6]$. Écrivons $n!-1 = p_1^{\alpha_1}\dots p_k^{\alpha_k}$ la décomposition de $n!-1$ en nombres premiers. Comme ce produit est congru à 5 modulo 6, un au moins de ses facteurs n'est pas congru à 1. Il existe donc j tel que $p_j \equiv 5 \ [6]$. Comme p_j divise $n!-1$, il ne divise pas $n!$, donc $p_j > n$. On en déduit que l'ensemble des nombres premiers congrus à 5 modulo 6 n'est pas majoré : il est infini.

Le cas $b=12$: 1. On a $a^4 - a^2 = 6a\binom{a+1}{3}$, donc $a^4 - a^2 + 1 \equiv 1 \ [6]$.

2. On a $a^{12}-1 = (a^4-1)(a^4+a^2+1)(a^4-a^2+1)$. Donc $x^{12} = 1$.

3. On a $x^6+1 = (x^2+1)(x^4-x^2+1) = 0$, donc $x^6 - 1 = -2 \neq 0$ (puisque $p \neq 2$). On a $(x^2-2)(x^2+1) = x^4-x^2-2 = -3 \neq 0$ (puisque $p \neq 3$), donc $x^4-1 = x^4-x^2+1+x^2-2 = x^2-2 \neq 0$. item L'ordre de x dans le groupe multiplicatif $\mathbb{F}_p^*$ divise 12 mais ne divise ni 4 ni 6 : c'est 12. On en déduit que 12 divise l'ordre de $\mathbb{F}_p^*$, donc que $p \equiv 1 \ [12]$.

4. Soit $n \in \mathbb{N}$, tel que $n \geqslant 2$. Posons $a = n!$ et soit p un diviseur premier de $a^4 - a^2 + 1$. Alors p est premier avec a, donc $p > n$ et $p \equiv 1 \ [12]$. On en déduit que l'ensemble des nombres premiers congrus à 1 modulo 12 n'est pas majoré : il est infini.

Le cas général 1. On démontre la première assertion par récurrence « forte » sur n.

- Si n est premier, $\Phi_n = \sum_{k=0}^{n-1} X^k$, donc $\Phi_n(0) = 1$.
- Dans le cas général, en utilisant l'égalité $\Phi_n \Phi_1 \prod_{d|n;\ 1<d<n} \Phi_d = X^n - 1$, on trouve $\Phi_n(0)\Phi_1(0) \prod_{d|n;\ 1<d<n} \Phi_d(0) = -1$. Or $\Phi_1 = X - 1$ donc $\Phi_1(0) = -1$ et l'on conclut par récurrence.

Pour la deuxième assertion, écrivons $\Phi_n = 1 + \sum_{k=1}^{N} \alpha_k X^k$. Il vient $\Phi_n(a) = 1 + a \sum_{k=1}^{N} \alpha_k a^{k-1}$, donc a et $\Phi_n(a)$ sont premiers entre eux d'après le théorème de Bézout.

2. On a $a^n - 1 = \Phi_n(a) \prod_{d|n;\ d<n} \Phi_d(a)$, donc $p | a^n - 1$, *i.e.* $x^n = 1$.
3. Remarquons que, puisque a et p sont premiers entre eux et $n|a$, n est inversible dans $\mathbb{F}_p$, donc nX^{n-1} et $X^n - 1$ sont premiers entre eux dans $\mathbb{F}_p[X]$. Si Q^2 divisait $X^n - 1$, on écrirait $X^n - 1 = Q^2 P$ donc, en dérivant, $nX^{n-1} = Q(2Q'P + QP')$, et Q serait un diviseur commun de nX^{n-1} et $X^n - 1$.
4. Soit $d \in \mathbb{N}$ un diviseur de n distinct de n. Écrivons $X^n - 1 = \prod_{k|n} \Phi_k$ et $X^d - 1 = \prod_{k|d} \Phi_k$, il vient $X^n - 1 = (X^d - 1)\Phi_n \prod_{k|n;\ k\not|d,\ k<n} \Phi_k$. Cela prouve que le produit $(X^d - 1)\Phi_n$ divise $X^n - 1$, donc n'a pas de facteur carré dans $\mathbb{F}_p[X]$. En particulier, les polynômes $X^d - 1$ et Φ_n sont premiers entre eux dans $\mathbb{F}_p[X]$. Ils n'ont donc pas de racine commune. Or, puisque $p|\Phi_n(a)$, x est racine de Φ_n, donc $x^d \neq 1$.
5. D'après ce qui précède, x est d'ordre n dans le groupe $\mathbb{F}_p^*$. L'ordre $p - 1$ de ce groupe est donc un multiple de n ; autrement dit, p est congru à 1 modulo n.
6. Soit $N \geqslant n$. Prenant $a = N!$, on a démontré (puisque $n|a$) que tout diviseur premier de $\Phi_n(a)$ est premier avec a - donc $p > N$, et congru à 1 modulo n. L'ensemble des nombres premiers congrus à 1 modulo n n'est donc pas majoré : il est infini.

Exercice 1.11.

1. a) Si $x = y^2$, l'équation $z^2 = x$ admet deux solutions $z = \pm y$ dans le corps $\mathbb{F}_p$; l'une des deux est congrue à un unique nombre $c \in \left\{1, \ldots, \frac{p-1}{2}\right\}$. L'application qui à $c \in \left\{1, \ldots, \frac{p-1}{2}\right\}$ associe la classe dans $\mathbb{F}_p$ de c^2 est donc une bijection de $\left\{1, \ldots, \frac{p-1}{2}\right\}$ sur C ; C a donc $\frac{p-1}{2}$ éléments.

   b) Si $x = y^2$, on a $x^{\frac{p-1}{2}} = y^{p-1} = 1$ d'après le petit théorème de Fermat.

   c) Le polynôme $X^{\frac{p-1}{2}} - 1$ admet donc $\frac{p-1}{2}$ racines : tous les éléments de C. Son degré étant $\frac{p-1}{2}$, il ne peut avoir d'autres racines.

   d) Par (c), -1 est un carré dans $\mathbb{F}_p$ si et seulement si $(-1)^{\frac{p-1}{2}} = 1$ (dans $\mathbb{F}_p$). Or $(-1)^{\frac{p-1}{2}} = 1$ si $p \equiv 1 \ [4]$ et $(-1)^{\frac{p-1}{2}} = -1$ si $p \equiv 3 \ [4]$. Notons que $-1 \neq 1$ dans $\mathbb{F}_p$ puisque on a supposé $p \neq 2$.

2. a) Puisque $p \neq 2$, on peut inverser 2 dans $\mathbb{F}_p$. On a $P = \left(X - \frac{a}{2}\right)^2 - \frac{a^2 - 4b}{4}\cdot$ Il s'ensuit que P a une racine dans $\mathbb{F}_p$ si et seulement si $a^2 - 4b$ est un carré dans $\mathbb{F}_p$.

   b) • L'équivalence entre (i) et (ii) résulte immédiatement de (a).
   • Si x est d'ordre 3 dans $\mathbb{F}_p^*$, alors x est racine de $X^3 - 1 = (X-1)(X^2+X+1)$ et $x \neq 1$, donc $x^2 + x + 1 = 0$. Inversement, si $x^2 + x + 1 = 0$, alors $x^3 = 1$ et, puisque $3 \neq 0$ dans $\mathbb{F}_p$, $x \neq 1$; donc x est d'ordre 3. Cela prouve (ii) $\iff$ (iii).
   • Si $\mathbb{F}_p^*$ admet un élément d'ordre 3, alors 3 divise l'ordre $p-1$ du groupe $\mathbb{F}_p^*$, donc $p \equiv 1\ [3]$. Inversement, si p s'écrit $3k+1$, l'ensemble des $x \in \mathbb{F}_p$ tels que $x^k = 1$ sont les racines du polynôme $X^k - 1$. Il y en a au plus k dans le corps commutatif $\mathbb{F}_p$. Si $y \in \mathbb{F}_p^*$ est tel que $y^k \neq 1$, on a $(y^k)^3 = y^{3k} = y^{p-1} = 1$, d'après le petit théorème de Fermat. L'élément y^k est alors d'ordre 3 dans $\mathbb{F}_p^*$.

3. a) Pour $x \in \mathbb{F}_p^*$, on a $\left(x^{\frac{p-1}{2}}\right)^2 = x^{p-1} = 1$, donc $x^{\frac{p-1}{2}} = \pm 1$; si $x \notin C$, il vient $x^{\frac{p-1}{2}} = -1$. Si $a, b \in \mathbb{F}_p^* \setminus C$, il vient $(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (-1)^2 = 1$, donc $ab \in C$.

   b) Si $-1 \notin C$ et $2 \notin C$, alors leur produit -2 est un carré par (a).

   c) Si $-1 = a^2$, il vient $X^4 + 1 = (X^2 - a)(X^2 + a)$; si $2 = a^2$, il vient $X^4 + 1 = (X^2 + aX + 1)(X^2 - aX + 1)$ et si $-2 = a^2$, il vient $X^4 + 1 = (X^2 + aX - 1)(X^2 - aX - 1)$. Dans tous les cas $X^4 + 1$ n'est pas irréductible. Notons que pour $p = 2$, on a $X^4 + 1 = (X+1)^4$.

   d) On a $X^4 + 1 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$. Comme $X^4 + 1$ n'a pas de racines dans $\mathbb{R}$, les polynômes $X^2 + \sqrt{2}X + 1$ et $X^2 - \sqrt{2}X + 1$ sont irréductibles.

   e) D'après (d) les polynômes $P \in \mathbb{R}[X]$ divisant $X^4 + 1$ sont des multiples scalaires de $1, X^4 + 1, X^2 + \sqrt{2}X + 1$ et $X^2 - \sqrt{2}X + 1$. Donc $X^4 + 1$ n'a pas de diviseurs dans $\mathbb{Q}[X]$ autres que les scalaires et les multiples scalaires de $X^4 + 1$. Il est irréductible sur $\mathbb{Q}$ (et sur $\mathbb{Z}$).

Exercice 1.12.

1. a) On a $1^p = 1$, $(ab)^p = a^p b^p$ et, puisque $p \left| \binom{p}{k} \right.$ pour $0 < k < p$, $(a+b)^p = a^p + b^p$.

   b) D'après (a), l'ensemble des racines de ce polynôme forment un sous-corps de L, qui a au plus p éléments : c'est donc le sous-corps $\mathbb{F}_p$ de L (appelé sous-corps premier de L).

2. a) Puisque $\omega^4 = -1$, on a $\omega^2 = -\omega^{-2}$, donc $(\omega + \omega^{-1})^= \omega^2 + 2\omega\omega^{-1} + \omega^{-2} = 2$.

   b) Dans L, le polynôme $X^2 = 2$ possède les racines x et $-x$. Il a des racines dans $\mathbb{F}_p$ si et seulement si $x \in \mathbb{F}_p$, donc (i) $\iff$ (ii).

   D'après 1.b) pour $y \in L$, on a équivalence entre $y^p = y$ et $y \in \mathbb{F}_p$, soit (ii) $\iff$ (iii).

   Remarquons que $\omega^5 = 1$ et comme $p \neq 5$ est impair, il vient $\omega^p \in \{\omega, \omega^2, \omega^3, \omega^4\}$. Remarquons aussi que, puisque $2x + 1 \neq 0$, $x \neq -1 - x$, donc $\omega^2 + \omega^{-2} \neq x$. Remarquons aussi que $x^p = \omega^p + \omega^{-p}$, donc si $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$, il vient $x^p = x$; si $\omega^p = \omega^2$ ou $\omega^p = \omega^3$, il vient $x^p = -1 - x \neq x$. Cela prouve que (iii) $\iff$ (iv) $\iff$ (v).

3. a) On a $\omega^5 = 1$, donc $\omega^{-1} = \omega^4$ et enfin $\omega + \omega^2 + \omega^{-2} + \omega^{-1} = -1$, soit $\omega^2 + \omega^{-2} = -1 - x$. Enfin, $x^2 = \omega^2 + 2 + \omega^{-2} = -x + 1$.

   b) On a $(2x+1)^2 = 4x^2 + 4x + 1 = 5$. Dans L, le polynôme $X^2 = 5$ possède les racines $2x+1$ et $-2x-1$. Il a des racines dans $\mathbb{F}_p$ si et seulement si $2x + 1 \in \mathbb{F}_p$, ce qui a lieu (puisque $p \neq 2$) si et seulement si $x \in \mathbb{F}_p$, donc (i) $\iff$ (ii).

   D'après 1.b) pour $y \in L$, on a équivalence entre $y^p = y$ et $y \in \mathbb{F}_p$, soit (ii) $\iff$ (iii).

   Remarquons que $\omega^8 = 1$ et comme p est impair, il vient $\omega^p \in \{\omega, \omega^3, \omega^5, \omega^7\}$. Remarquons aussi que $\omega^5 = -\omega$ et $\omega^7 = \omega^{-1}$, donc $\omega^3 = -\omega^{-1}$. Remarquons aussi que $x^p = \omega^p + \omega^{-p}$, donc si $\omega^p = \omega$ ou $\omega^p = \omega^{-1}$, il vient $x^p = x$; si $\omega^p = \omega^3$ ou $\omega^p = \omega^5$, il vient $x^p = -x \neq x$. Cela prouve que (iii) $\iff$ (iv) $\iff$ (v).

Exercice 1.13.

Voir exercice 1.11.

Remarquons que $\dfrac{p+1}{4} \in \mathbb{N}$. Puisque $x^{\frac{p-1}{2}} = 1$, on a $\left(x^{\frac{p+1}{4}}\right)^2 = x^{\frac{p-1}{2}+1} = x$.

1. On a $b^{2^\ell} = a^{u2^\ell} = 1$ d'après le théorème de Fermat, donc l'ordre de b dans $\mathbb{F}_p^*$ divise 2^ℓ ; il est de la forme 2^k avec $0 \leqslant k \leqslant \ell$.
2. On a $a \mapsto a^u = \pm 1$ si et seulement si a est racine du polynôme $X^{2u} - 1$. Comme $X^{2u} - 1$ divise $X^{p-1} - 1$ qui est scindé a racines simples (il possède $p-1$ racines d'après le théorème de Fermat), donc $X^{2u} - 1$ possède $2u$ racines distinctes. En prenant au hasard un élément de $\mathbb{F}_p^*$, on a donc $\dfrac{2u}{p-1} = 2^{1-\ell}$ chances d'avoir $b = \pm 1$.
3. Si $b \neq \pm 1$, alors b est d'ordre 2^k avec $k \geqslant 2$, donc $c = b^{2^{k-2}}$ est d'ordre 4 : il vérifie $(c^2)^2 = 1$ et $c^2 \neq 1$, donc $c^2 = -1$. En pratique, si $b \neq \pm 1$, on pose $b_1 = b^2$ (modulo p) ; si le$b_1 = -1$, alors b est une racine de -1 ; sinon, on continue : on pose $b_2 = b_1^2$. Au bout d'u plus $n-1$ étapes, on aura trouvé notre racine de -1.

   NB C'est en pratique la méthode qu'on utilise pour trouver la racine de -1 dans $\mathbb{F}_p$: on essaie des nombres a au hasard, avec à chaque fois au moins une chance sur deux de succès. Le nombre d'opérations utilisées est un « petit » poynôme en $\log p$: c'est beaucoup plus rapide si p est grand que d'essayer tous les nombres de $\mathbb{F}_p^*$...

Exercice 1.14.

1. Prendre pour $a-2$ un nombre strictement positif qui est multiple de tous les nombres premiers $\leqslant n+1$. Alors, pour $0 \leqslant j \leqslant n-1$, $2+j$ a un diviseur premier qui divise aussi $a-2$, donc $a+j$ n'est pas premier.

   a) On décompose a comme produit de nombres premiers. Cela donne : $a = \prod_{j=1}^{k} p_j^{\alpha_j}$ $(\alpha_j \in \mathbb{N})$.

   On effectue alors la division euclidienne de α_j par 2 sous la forme $\alpha_j = 2\beta_j + \varepsilon_j$ avec $\beta_j \in \mathbb{N}$ et $\varepsilon_j \in \{0, 1\}$. On pose $b = \prod_{j=1}^{k} p_j^{\beta_j}$.

   Si $a \leqslant x$, il vient $1 \leqslant b \leqslant \sqrt{x}$; on a donc $E(\sqrt{x})$ choix pour b et 2 choix pour chaque ε_j. Notons que l'inégalité est en général stricte puisque pour $b \leqslant \sqrt{x}$ et ε_j donnés on n'a pas toujours $b^2 p_1^{\varepsilon_1} \dots p_k^{\varepsilon_k} \leqslant x$.

   b) Pour chaque $p \in \mathbb{N}$ le nombre des multiples de p dans $[1, x]$ est $E(x/p)$ donc leur proportion est $\dfrac{E(x/p)}{x} \leqslant \dfrac{1}{p}\cdot$ Or tout élément de $[1, x] \setminus A_k$ possède un diviseur premier dans $]p_k, x]$, d'où l'estimation.

   c) our $x = 4^{k+1}$, le nombre d'éléments de $A_k \cap [1, x]$ est $\leqslant 2^{2k+1}$ d'après (a), donc leur proportion est $\leqslant 1/2$. On en déduit que la la proportion d'éléments $\mathbb{N} \setminus A_k$ dans $[1, x]$ est $\geqslant 1/2$, donc $\sum_{p \in \mathcal{P},\ p_k < p \leqslant x} 1/p \geqslant 1/2$ par (b). La série $\sum_j 1/p_k$ ne peut converger car son reste $\sum_{j>k} 1/p_j$ ne tend pas vers 0.

   d) Soit $B \subset \mathbb{N}^*$ l'ensemble des nombres entiers ne comportant pas le chiffre 9 dans leur développement décimal. Il y a 8.9^k éléments de B à $k+1$ chiffres tous plus grands que 10^k. On a donc $\sum_{n \in B} \dfrac{1}{n} \leqslant 8 \sum_{k=1}^{+\infty} \dfrac{9^k}{10^k} < +\infty$. En particulier $\sum_{n \in \mathcal{P} \setminus B} \dfrac{1}{n} = +\infty$, donc $\mathcal{P} \setminus B$ est infini.

Exercice 1.15.

1. a) Remarquons que $v_p(n)$ est le nombre de $k \geqslant 1$ tels que np^{-k} soit entier, soit $\sum_{k=1}^{+\infty} E\big(np^{-k}\big) - E\big((n-1)p^{-k}\big)$. La formule s'en déduit par récurrence sur n puisque $v_p(1!) = 0$ et $v_p(n!) = \sum_{k=1}^{n} v_p(k) = v_p((n-1)!) + v_p(n)$.

   b) Pour $x \in \mathbb{R}$, on a $E(2x) - 2E(x) = 0$ si $E(2x)$ est pair et $E(2x) - 2E(x) = 1$ si $E(2x)$ est impair, d'où le résultat d'après (a).

   c) • De (b), on déduit que $v_p\binom{2n}{n}$ est inférieur ou égal au nombre des k tels que $E\big(2np^{-k}\big)$ soit non nul, c'est-à-dire $v_p\binom{2n}{n} \leqslant E\Big(\dfrac{\ln 2n}{\ln p}\Big)$.
   • Si $n < p \leqslant 2n$, alors $v_p(n!) = 0$ et $v_p((2n)!) = 1$.
   • Si $p \leqslant n < \dfrac{3p}{2}$, alors on ne peut avoir $p = 2$ (car $n \geqslant 3$) ; il vient $2n < p^2$; on a alors $E(2np^{-1}) = 2$ et, pour $k \geqslant 2$, on a $E(2np^{-k}) = 0$. Donc d'après (b), on a $v_p\binom{2n}{n} = 0$.

   d) On a $\ln\binom{2n}{n} = \sum_{p \text{ premier}} v_p\binom{2n}{n} \ln p$.

   (i) Il vient $\ln\binom{2n}{n} \geqslant \sum_{n<p<2n,\ p \text{ premier}} v_p\binom{2n}{n} \ln p \geqslant (\pi(2n) - \pi(n)) \ln n$.

   (ii) On a d'après (c),

$$\begin{aligned} \ln\binom{2n}{n} &= \sum_{p\leqslant 2n/3,\ p \text{ premier}} v_p\binom{2n}{n} \ln p + \sum_{n<p<2n,\ p \text{ premier}} \ln p \\ &\leqslant \pi(2n/3) \ln 2n + (\pi(2n) - \pi(n)) \ln 2n \end{aligned}$$

2. On a $\sum_{k=0}^{2n-1} \binom{2n-1}{k} = 2^{2n-1}$. Or pour tout k, on a $\binom{2n-1}{k} = \binom{2n-1}{2n-k-1}$ d'où l'égalité $\sum_{k=0}^{n-1} \binom{2n-1}{k} = 2^{2n-2}$.

   Remarquons que pour $0 \leqslant k < n-1$, on a $\binom{2n-1}{k+1} = \dfrac{2n-1-k}{k+1}\binom{2n-1}{k} \geqslant \binom{2n-1}{k}$; en d'autres termes, la suite $\binom{2n-1}{k}_{0\leqslant k\leqslant n-1}$ est croissante ; il vient $\binom{2n-1}{n-1} \leqslant 2^{2n-2} = \sum_{k=0}^{n-1} \binom{2n-1}{k} \leqslant n\binom{2n-1}{n-1}$. Or $\binom{2n}{n} = 2\binom{2n-1}{n-1}$, d'où $\binom{2n}{n} \leqslant 2^{2n-1} \leqslant n\binom{2n}{n}$

11.2 Anneaux

Exercice 2.1.

1. a) Comme G est commutatif, on a $(ab)^m = a^m b^m$ pour tout $m \in \mathbb{Z}$.
   Soit ℓ l'ordre de ab dans G. On a $(ab)^{k_a k_b} = a^{k_a k_b} b^{k_a k_b} = 1$, donc ℓ divise $k_a k_b$. Par ailleurs, on a $(ab)^\ell = 1$, donc $1 = (ab)^{\ell k_a} = (a^{k_a})^\ell b^{\ell k_a}$. On en déduit que $b^{\ell k_a} = 1$, donc $k_b | \ell k_a$, et $k_b | \ell$ d'après le théorème de Gauss. Puis, $b^\ell = 1$ et comme $(ab)^\ell = 1$, il vient aussi $a^\ell = 1$, ce qui implique que $k_a | \ell$. Enfin $k_a k_b | \ell$, donc $k_a k_b = \ell$.

b) On a $x^k = 1$ pour tout $x \in G$ si et seulement si k est multiple de l'ordre de x pour tout x, *i.e.* si et seulement si k est multiple du PPCM noté n des ordres des éléments de G. Comme l'ordre tout élément divise le cardinal de G, le PPCM des ordres divise le cardinal de G.

c) Il existe $y_j \in G$ tel que $\dfrac{n}{p_j}$ ne soit pas un multiple de l'ordre de y_j. L'ordre q de y_j est de la forme $q = p_j^k m$ avec m premier avec p_j. Comme q divise n mais pas $\dfrac{n}{p_j}$, il vient $k = m_j$. Posons alors $x_j = y_j^m$ qui est d'ordre $p_j^{m_j}$.

d) D'après la question a) et par récurrence, l'ordre de $\prod x_j$ est $\prod p_j^{m_j} = n$.

2. Soit K un corps commutatif et G un sous-groupe fini à N éléments de K^*. Soit n son exposant.

a) Les éléments de K qui vérifient $x^n = 1$ sont les racines du polynôme $X^n - 1$. Ce polynôme de degré n a au plus n racines. Tous les éléments de G vérifient $x^n = 1$, donc $N \leqslant n$.

b) On a vu que n divise l'ordre N de G. Comme $N \leqslant n$, il vient $n = N$. Il existe donc un élément d'ordre N : le groupe G est cyclique.

Exercice 2.2.

1. a) Pour tout $a \in \{0, \dots, d-1\}$ on a $\dfrac{a}{d} \in A_n$. L'écriture $\dfrac{a}{d}$ est irréductible si et seulement a et d sont premiers entre eux. Dans A_n, il y a donc $\varphi(d)$ éléments dont l'écriture irréductible est de la forme $\dfrac{a}{d}$.

b) En regroupant les éléments de A_n selon le dénominateur de leur écriture irréductible, on obtient l'égalité $\displaystyle\sum_{d|n} \varphi(d) = n$.

2. a) En regroupant les éléments de G suivant leur ordre, il vient $\displaystyle\sum_{d|n} s_d = n$.

b)
- Par définition de l'ordre d'un élément d'un groupe, H a d éléments. Le groupe H est cyclique d'ordre d ; il est isomorphe à $(\mathbb{Z}/d\mathbb{Z}, +)$; il a $\varphi(d)$ générateurs (éléments d'ordre d).
- Comme H est un groupe d'ordre d, tout élément de H vérifie $x^d = 1$.
- Les éléments de K qui vérifient $y^d = 1$ sont les racines du polynôme $X^d - 1$. Ce polynôme de degré d a au plus d racines.
- Posons $Z = \{y \in K^*;\ y^d = 1\}$. D'après ce qui précède, $H \subset Z$ et Z a au plus d éléments, donc $Z = H$.

c) D'après ce qui précède, si G a un élément x d'ordre d, alors les élément d'ordre d sont les générateurs du sous-groupe H engendré par x, et il y en a $\varphi(d)$.

d) On a $\displaystyle\sum_{d|n} s_d = n = \sum_{d|n} \varphi(d)$. Or pour tout d on a $s_d \leqslant \varphi(n)$. Les nombres positifs $\varphi(d) - s_d$ ont une somme nulle : ils sont tous nuls. En particulier $s_n = \varphi(n)$ n'est pas nul, donc G possède un élément d'ordre n : il est cyclique.

Exercice 2.3.

1. a) Un sous-groupe d'un groupe cyclique est cyclique, donc si $G \times H$ est cyclique, G et H sont cycliques (car isomorphes à des sous-groupes de $G \times H$). Il reste à déterminer quand le produit de deux groupes cycliques est cyclique, autrement dit, pour quels $a, b \in \mathbb{N}^*$ le groupe $\mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$ est cyclique. Si a, b sont premiers entre eux, le groupe $\mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$ est cyclique d'après le théorème chinois (1.35). Inversement, soit m le PPCM de a et b. Pour tout $(x, y) \in \mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$, on a $m(x, y) = (mx, my) = 0$. Donc si $\mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$ est cyclique, il existe $(x, y) \in \mathbb{Z}/a\mathbb{Z} \times b\mathbb{Z}$ d'ordre ab, donc $ab = m$, ce qui implique que a et b sont premiers entre eux.

b) On a $\varphi(1) = \varphi(2) = 1$. Si $n \geqslant 3$ alors ou bien $n = 2^k$ avec $k \geqslant 2$ et $\varphi(n) = 2^{k-1}$ est pair ; ou bien n admet un diviseur premier p distinct de 2 donc s'écrit $n = p^k m$ où $k \geqslant 1$ et m est premier avec p. Alors $\varphi(n) = (p-1)p^{k-1}\varphi(m)$ est divisible par $p-1$, donc est pair.

c) D'après le théorème Chinois, $(\mathbb{Z}/nm\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*$. Les ordres $\varphi(n)$ et $\varphi(m)$ de $(\mathbb{Z}/n\mathbb{Z})^*$ et $(\mathbb{Z}/m\mathbb{Z})^*$ sont pairs et ne sont donc pas premiers entre eux. Leur produit n'est donc pas cyclique.

d) Les éléments du groupe $(\mathbb{Z}/8\mathbb{Z})^*$ vérifient tous $x^2 = 1$, puisque $3^2 - 1$, $5^2 - 1$ et $7^2 - 1$ sont multiples de 8. Donc $(\mathbb{Z}/8\mathbb{Z})^*$ n'a pas d'éléments d'ordre 4 : il n'est pas cyclique.

2. a) Cela est vrai pour $k = 0$. Supposons $k \geqslant 0$ et $(1+p)^{p^k} = 1 + p^{k+1}(1+pb)$. On a alors $(1+p)^{p^{k+1}} = (1+p^{k+1}(1+pb))^p = \sum_{j=0}^{p} \binom{p}{j} p^{j(k+1)}(1+pb)^j$. Or $p^{k+3} | \binom{p}{2}.p^{2k+2}$ et pour $j \geqslant 3$, $p^{k+3} | p^{j(k+1)}$, donc, modulo p^{k+3},

$$\begin{aligned}(1+p)^{p^{k+1}} &\equiv 1 + p.p^{k+1}(1+pb) \\ &\equiv 1 + p^{k+2}\end{aligned}$$

b) On a $(1+p)^{p^{n-1}} \equiv 1 \quad [p^n]$ et $(1+p)^{p^{n-2}} \not\equiv 1 \quad [p^n]$. Donc l'ordre de $1+p$ divise p^{n-1} et ne divise pas p^{n-2} ; c'est donc p^{n-1}.

c) Soit m l'ordre de x dans $(\mathbb{Z}/p^n\mathbb{Z})^*$. On a $a^m \equiv 1 \quad [p^n]$. En particulier $a^m \equiv 1 \quad [p]$, donc m est un multiple de $p-1$. Écrivons $m = (p-1)d$ ([5]). Alors x^d est d'ordre $p-1$.

d) On a vu que dans $(\mathbb{Z}/p^n\mathbb{Z})^*$ il y a un élément u d'ordre p^{n-1} et un élément v d'ordre $p-1$. Soit ℓ l'ordre de uv dans $(\mathbb{Z}/p^n\mathbb{Z})^*$; on a $(uv)^\ell = 1$, donc $1 = (uv)^{\ell(p-1)} = (u^{p-1})^\ell v^{\ell(p-1)}$. On en déduit que $v^{\ell(p-1)} = 1$, donc $p^{n-1} | \ell(p-1)$, donc $p^{n-1} | \ell$ (d'après le théorème de Gauss, puisque p^{n-1} et $p-1$ sont premiers entre eux). Enfin, $v^\ell = 1$ et comme $(uv)^\ell = 1$, il vient aussi $u^\ell = 1$, ce qui implique que $p-1 | \ell$. Enfin $p^{n-1}(p-1) = \varphi(p^n) | \ell$, d'où l'on déduit que uv engendre $(\mathbb{Z}/p^n\mathbb{Z})^*$.

Enfin, d'après le théorème Chinois, $(\mathbb{Z}/2p^n\mathbb{Z})^*$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p^n\mathbb{Z})^*$, lui même isomorphe à $(\mathbb{Z}/p^n\mathbb{Z})^*$ (car $(\mathbb{Z}/2\mathbb{Z})^*$ est le groupe à un seul élément) donc est cyclique

3. Ce sont $1, 2, 4$ et les nombres de la forme p^k ou $2p^k$ avec p premier distinct de 2 et $k \in \mathbb{N}^*$.

Exercice 2.4.

1. a) On a $v(x) = \overline{x}\, x \in x\mathbb{Z}[\tau]$. Soient $m, n \in \mathbb{Z}$, notons $r, s \in \{0, \ldots, v(x)-1\}$ leurs restes ans la division euclidienne par $v(x)$. Alors $(m+n\tau) - (r+s\tau) \in x\mathbb{Z}[\tau]$. Cela prouve que tout élément de $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ est la classe d'un $r+s\tau$ avec $r, s \in \{0, \ldots, v(x)-1\}$, donc $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ est fini.

b) Pour tout $z \in \mathbb{Z}[\tau]$, on a $z-(r_i+xs_j) \in xy\mathbb{Z}[\tau] \iff z-r_i \in x\mathbb{Z}[\tau]$ et $\dfrac{z-r_i}{x} - s_j \in y\mathbb{Z}[\tau]$. On en déduit qu'il existe un et un seul couple (i,j) tel que $z-(r_i+xs_j) \in xy\mathbb{Z}[\tau]$. L'application de $\{1, \ldots, n\} \times \{1, \ldots, m\}$ dans $\mathbb{Z}[\tau]/xy\mathbb{Z}[\tau]$ qui à (i,j) associe la classe de $r_i + xs_j$ est une bijection. On en déduit que $\mathbb{Z}[\tau]/xy\mathbb{Z}[\tau]$ a nm éléments, soit $v(xy) = v(x)v(y)$.

c) Pour $k \in \mathbb{Z}$, on a $a + b\tau \in k\mathbb{Z}[\tau] \iff a \in k\mathbb{Z}$ et $b \in k\mathbb{Z}$. Il y a donc k^2 classes : celles de $a + b\tau$ où $a, b \in \{0, \ldots, k-1\}$. Notons que l'application $x \mapsto \overline{x}$ est un automorphisme de l'anneau $\mathbb{Z}[\tau]$. On en déduit que $v(x) = v(\overline{x})$. On a alors $v(x)^2 = v(x)v(\overline{x}) = v(x\overline{x}) = (x\,\overline{x})^2$, donc $v(x) = x\,\overline{x} = |x|^2$.

2. a) Soit $z \in \mathbb{Z}[\tau]$. Il existe q et r tels que $z = qx + r$ avec $V(r) < V(x)$. Par minimalité de $V(x)$, il vient $r \in \{0, -1, 1\}$. On en déduit que $\mathbb{Z}[\tau]/x\mathbb{Z}[\tau]$ a au plus 3 éléments, soit $v(x) \leqslant 3$.

5. Remarquons que m divise l'ordre de $(\mathbb{Z}/p^n\mathbb{Z})^*$ qui est égal à $\varphi(p^n) = (p-1)p^{n-1}$, donc d est de la forme p^k avec $k \leqslant n-1$.

b) On a $v(x) = (\operatorname{Re} x)^2 + (\operatorname{Im} x)^2 \leqslant \sqrt{3}$. On en déduit que $|\operatorname{Re} x| \leqslant \sqrt{3}$ et $|\operatorname{Im} x| \leqslant \sqrt{3}$. En particulier, $x \notin \mathbb{Z}$ (puisque $x \notin \{0, -1, 1\}$) et $\operatorname{Im} x \neq 0$. Or $x = a + b\tau$ avec $a, b \in \mathbb{Z}$. Il vient $|b| \geqslant 1$. Comme $|\operatorname{Im} x| = |b| \operatorname{Im} \tau$, il vient $\operatorname{Im} \tau \leqslant \sqrt{3}$.

Exercice 2.5.

1. Puisque $\alpha \in G$ et G est un sous-groupe de $(\mathbb{C}, +)$, il vient $\mathbb{Z}\alpha \subset G$, donc $\mathbb{Z}\alpha \subset G \cap \mathbb{R}\alpha$. Soit $t \in \mathbb{R}$ tel que $t\alpha \in G$ et notons n sa partie entière. Alors $t\alpha - n\alpha \in G$. Or $|t\alpha - n\alpha|^2 = |t-n|^2|\alpha|^2 < |\alpha|^2$; il vient $t\alpha - n\alpha = 0$ par minimalité de $|\alpha|$.
2. Posons $\dfrac{\beta}{\alpha} = u$. Puisque $|\alpha| \leqslant |\beta|$, il vient $|u| \geqslant 1$. Puisque $|\beta - \alpha| \leqslant |\beta|$, on a $|u - 1| \leqslant |u|$, donc $\operatorname{Re} u \leqslant 1/2$; de même $|\beta + \alpha| \leqslant |\beta|$ donc $\operatorname{Re} u \geqslant -1/2$.
3. Posons $y = \dfrac{x}{\alpha}$. Soit n l'entier le plus proche de $\dfrac{\operatorname{Im} y}{\operatorname{Im} u}$. On a donc $\left|\dfrac{\operatorname{Im} y}{\operatorname{Im} u} - n\right| \leqslant 1/2$, soit $|\operatorname{Im}(y - nu)| \leqslant (\operatorname{Im} u)/2$.
   Soit alors m l'entier le plus proche de $\operatorname{Re}(y - nu)$. On a $|\operatorname{Re}(y - nu - m)| \leqslant 1/2$. Il vient $|y - nu - m|^2 = |\operatorname{Re}(y - nu - m)|^2 + |\operatorname{Im}(y - nu)|^2 \leqslant 1/4(1 + (\operatorname{Im} u)^2) \leqslant |u|^2/2$. On a donc $|y - nu - m| < |u|$, soit $|x - (m\alpha + n\beta)| < |\beta|$.
   Par minimalité de $|\beta|$, il vient $x - (m\alpha + n\beta) \in \mathbb{Z}\alpha$. Or $\left|\operatorname{Re}\dfrac{x - (m\alpha + n\beta)}{\alpha}\right| < 1$, donc $x = m\alpha + n\beta$.

Exercice 2.6.

1. On a $\tau\alpha \in J$ et $\tau\beta \in J$!
2. On a $\tau = a + b\dfrac{\beta}{\alpha}$ et, comme les parties imaginaires de τ et $\dfrac{\beta}{\alpha}$ sont positives, $b > 0$.
3. On a $M \begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \tau \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$; donc τ est une valeur propre de M. L'autre valeur propre est donc $\overline{\tau}$ et les espaces propres respectifs sont $\mathbb{C}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ et $\mathbb{C}\begin{pmatrix}\overline{\alpha}\\ \overline{\beta}\end{pmatrix}$.
   La trace et le déterminant de cette matrice sont donc $a + d = \tau + \overline{\tau} = 1$ et $ad - bc = \tau\overline{\tau} = 5$.
   Comme a et d sont entiers et $a + d = 1$, ces deux nombres ne peuvent être strictement positifs ou strictement négatifs. Leur produit est négatif ou nul. Par ailleurs a et d ne sont pas de même parité (leur somme est impaire) donc ad est pair. Comme $ad - bc = 5$ est impair, bc est impair, bonc b et c sont impairs. Enfin, $4bc + (a - d)^2 = 4(bc - ad) + (a + d)^2 = -20 + 1 = -19$.
4. Divisant par α les égalités $\tau\alpha = a\alpha + b\beta$ et $\tau\beta = c\alpha + d\beta$, il vient $\begin{pmatrix}a + bx\\ c + dx\end{pmatrix} = \tau\begin{pmatrix}1\\ x\end{pmatrix}$. Donc
   a) $bx^2 + (a - d)x - c = 0$; l'autre racine du trinôme $bX^2 + (a - d)X - c$ est $\overline{x}$.
   b) Le produit $\overline{x}x$ de ces racines est $-\dfrac{c}{b}$, et la somme $x + \overline{x}$ des racines est $\dfrac{a - d}{b}$.
   c) Ces inégalités proviennent des inégalités $|x| \geqslant 1$ et $|\operatorname{Re} x| \leqslant 1$.
5. On a $-4bc \geqslant 4b^2$ et $(a - d)^2 \leqslant b^2$, donc $19 = -4bc - (a - d)^2 \geqslant 4b^2 - b^2 = 3b^2$.
6. Puisque b est impair et $3b^2 \leqslant 19$, il vient $b = 1$.
7. Donc $\beta = (\tau - a)\alpha$. On en déduit que le sous-groupe de J de base $(\alpha, \tau\alpha)$ contient β : c'est J. Par suite $J = \alpha\mathbb{Z}[\tau]$. Ceci étant vrai pour tout idéal, $\mathbb{Z}[\tau]$ est principal. D'après l'exercice 2.4, il n'est pas euclidien.

Exercice 2.7.

1. L'idéal J engendré par 2 et X est l'ensemble des $P \in \mathbb{Z}[X]$ tels que $P(0)$ est pair. Si $P \in J$ qui divise 2 alors $\partial P \leqslant \partial 2 = 0$, donc P est un polynôme constant, et comme $P \in J$ et $P|2$, il vient $P = \pm 2$; donc P ne divise pas X (dans $\mathbb{Z}[X]$). L'idéal J n'est pas engendré par P.

2. Remarquons que, si la partie imaginaire de τ est $> \sqrt{2}$, alors l'élément 2 est irréductible dans $\mathbb{Z}[\tau]$: si $2 = uv$ avec $u, v \in \mathbb{Z}[\tau]$, alors $u\overline{u}v\overline{v} = 4$ et puisque $u\overline{u}, v\overline{v} \in \mathbb{Z}[\tau] \cap \mathbb{R}_+ = \mathbb{N}$, $u\overline{u} \leqslant 2$, ou $v\overline{v} \leqslant 2$. La partie imaginaire de tout élément de $\mathbb{Z}[\tau]$ est un multiple de celle de τ qui est $> \sqrt{2}$. Donc si $u\overline{u} \leqslant 2$, alors $u \in \mathbb{Z}$, donc $u = \pm 1$. Donc 2 est bien irréductible. Si $\mathbb{Z}[\tau]$ est factoriel, une écriture $x\overline{x} = 2b$ avec $x \in \mathbb{Z}[\tau]$ et $b \in \mathbb{N}$ impose que 2 divise un des facteurs, donc $x/2 \in \mathbb{Z}[\tau]$.
Si $\tau = i\sqrt{2k}$ avec $k \geqslant 2$, on a $\tau\overline{\tau} = 2k$; si $\tau = i\sqrt{2k+1}$, avec $k \geqslant 1$, on a $(1+\tau)(1+\overline{\tau}) = 2(k+1)$, et puisque $\dfrac{\tau}{2} \notin \mathbb{Z}[\tau]$ et $\dfrac{1+\tau}{2} \notin \mathbb{Z}[\tau]$. On en déduit que $\mathbb{Z}[\tau]$ n'est pas factoriel. Même raisonnement pour $\tau = \dfrac{1+i\sqrt{15}}{2}$ vu que $\tau\overline{\tau} = 4$.

Exercice 2.8.

1. Si P est un polynôme non nul à coefficients dans K tel que $P(x) = 0$, alors $P \in K_1[X]$, donc x est algébrique sur K_1 !
2. Remarquons qu'un sous-anneau A de L contenant K et qui est un K-espace vectoriel de dimension finie est un corps. En effet, si $a \in A$ n'est pas nul, l'application K-linéaire $y \mapsto ay$ de A dans A est injective (vu que A est intègre : c'est un sous-anneau de l'anneau intègre K), donc bijective puisque A est de dimension finie ; il existe donc $b \in A$ tel que $ab = 1$, ce qui prouve que $a^{-1} \in A$.
Si x est algébrique sur K, alors l'ensemble $\{P(x);\ P \in K[X]\}$ est un sous-corps de K isomorphe à $K[X]/\varpi$ où ϖ est le polynôme minimal de x. Il est de dimension finie sur x et contient x.
Si A est un sous-anneau de L contenant K et x et qui est un K-espace vectoriel de dimension finie disons n. Alors $(1, x, \ldots, x^n)$ sont liés : il existe donc un polynôme P de degré $\leqslant n$ tel que $P(x) = 0$.
3. Si K_2 est de dimension finie sur K, alors le K-espace vectoriel K_1 qui est un sous-K-espace vectoriel de K_2 est de dimension finie. Tout système générateur $(a_1, \ldots, a_m) \in K_2^m$du K-espace vectoriel K_2 est un système générateur du K_1-espace vectoriel K.
Inversement, soit $(a_1, \ldots, a_p)$ une base du K espace vectoriel K_1 et $(b_1, \ldots, b_q)$ une base du K_1-espace vectoriel K_2. On démontre que $(a_ib_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ est une base du K-espace vectoriel K_2, ce qui démontrera que K_2 est un K-espace vectoriel de dimension pq.
Soit $x \in K_2$. Il existe $(\mu_1, \ldots, \mu_q) \in K_1^q$ tels que $x = \displaystyle\sum_{j=1}^{n} \mu_j b_j$ et, pour chaque j, il existe $(\lambda_{1,j}, \ldots, \lambda_{p,j}) \in K^p$ tels que $\mu_j = \displaystyle\sum_{i=1}^{p} \lambda_{i,j} a_i$. on a alors $x = \displaystyle\sum_{j=1}^{q}\sum_{i=1}^{p} \lambda_{i,j} a_i b_j$ donc le système $(a_ib_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ est générateur.
Soient $(\lambda_{i,j}) \in K^{pq}$ tels que $\displaystyle\sum_{j=1}^{q}\sum_{i=1}^{p} \lambda_{i,j} a_i b_j = 0$; posons $\mu_j = \displaystyle\sum_{i=1}^{p} \lambda_{i,j} a_i$; il vient $\displaystyle\sum_{j=1}^{n} \mu_j b_j = 0$ et puisque (b_j) est libre (sur K_1) il vient $\mu_j = 0$ pour tout j ; enfin puisque (a_i) est libre (sur K) il vient $\lambda_{i,j} = 0$ pour tout i, j. Donc le système $(a_ib_j)_{1\leqslant i\leqslant p;\ 1\leqslant j\leqslant q}$ est libre.
4. a) On a $\alpha^{-1} \in K_1$, donc α^{-1} est algébrique.
   b) Comme β est algébrique sur K donc sur K_1, il existe un sous corps K_2 de L contenant β et K_1 de dimension finie sur K_1 donc sur K. Alors $\alpha + \beta \in K_2$ et $\alpha\beta \in K_2$, donc $\alpha + \beta$ et $\alpha\beta$ sont algébriques sur K.
5. La première assertion est claire. Si x est algébrique sur K', il existe $P \in K'[X]$ non nul tel que $P(x) = 0$; écrivons $P = \displaystyle\sum_{k=0}^{n} a_k X^k$. On démontre immédiatement par récurrence sur $n \in \mathbb{N}$ qu'il existe un sous corps K_1 de L contenant $a_0, \ldots, a_n$ et K de dimension finie sur K. Alors x est algébrique sur K_1 donc sur K.

11.3 Polynômes et fractions rationnelles

Exercice 3.1. Si p/q est racine avec p et q premiers entre eux, on écrit $0 = q^n P(p/q) = \sum_{k=0}^{n} a_k p^k q^{n-k}$.

Comme p et q divisent cette somme, il vient $p|q^n a_0$ et $q|p^n a_n$, donc $p|a_0$ et $q|a_n$ d'après le théorème de Gauss.

Exercice 3.2. Successivement sur $\mathbb{Q}$ sur $\mathbb{R}$ et sur $\mathbb{C}$, on trouve

$$\begin{aligned} P &= (X-1)(X^2+5)(X^2-3X+1) \\ &= (X-1)(X-\frac{3+\sqrt{5}}{2})(X-\frac{3-\sqrt{5}}{2})(X^2+5) \\ &= (X-1)(X-\frac{3+\sqrt{5}}{2})(X-\frac{3-\sqrt{5}}{2})(X+i\sqrt{5})(X-i\sqrt{5}) \end{aligned}$$

Exercice 3.3. On trouve $F = \frac{2}{X^3} + \frac{4}{X^2} + \frac{7}{X} - \frac{7}{X-1} + \frac{3}{(X-1)^2}\cdot$ Donc une primitive de $t \mapsto F(t)$ est $t \mapsto -\frac{1}{t^2} - \frac{4}{t} - \frac{3}{t-1} + 7\ln\left|\frac{t}{t-1}\right| + c$ où c est une constante.

Exercice 3.4. Les conditions $P(0) = 1$ et $P'(0) = 0$ s'écrivent $P = 1 + aX^2 + bX$. On a alors $P(1) = 1 + a + b = 0$ et $P'(1) = 2a + 3b = 1$, donc $a = -4$ et $b = 3$.

Le polynôme $Q - P$ s'annule en 0 et en 1 ainsi que sa dérivée si et seulement s'il est divisible par $X^2(X-1)^2$. Donc les polynômes qui conviennent sont $1 - 4X^2 + 3X^3 + X^2(X-1)^2 B$ avec $B \in K[X]$.

Exercice 3.5.

a) On a $\frac{1}{x^4 - x^2 - 2} = \frac{1}{3}\left(\frac{1}{x^2-2} - \frac{1}{x^2+1}\right) = \frac{1}{6\sqrt{2}}\left(\frac{1}{x-\sqrt{2}} - \frac{1}{x+\sqrt{2}}\right) - \frac{1}{3(x^2+1)}$. Une primitive est $x \mapsto \frac{1}{6\sqrt{2}}\ln\left|\frac{x-\sqrt{2}}{x+\sqrt{2}}\right| + \frac{1}{3}\mathrm{Arctan}\, x + c$.

b) On a $\int \frac{x\,dx}{(x^2+1)^2} = -\frac{1}{2(x^2+1)} + c$. Or, la dérivée de $x \mapsto \frac{x}{x^2+1}$ est $x \mapsto \frac{(x^2+1)-2x^2}{(x^2+1)^2} = \frac{2}{(x^2+1)^2} - \frac{1}{x^2+1}$, donc $\int \frac{dx}{(x^2+1)^2} = \frac{x}{2(x^2+1)} + \frac{1}{2}\mathrm{Arctan}\, x + c$.

c) Posons $y = 1 - x$. On a $\frac{2-y}{(1-y)y^6} = \frac{1}{1-y} + \frac{2-y-y^6}{(1-y)y^6} = \frac{1}{1-y} + \frac{2+y+y^2+y^3+y^4+y^5}{y^6}\cdot$
Donc $\int \frac{x+1}{x(x-1)^6} = \ln\left|\frac{x}{x-1}\right| + \frac{1}{1-x} + \frac{1}{2(1-x)^2} + \frac{1}{3(1-x)^3} + \frac{1}{4(1-x)^4} + \frac{2}{5(1-x)^5} + c$.

d) (Règles de Bioche : on pose $u = \sin x$) $\int \frac{dx}{\cos^3 x} = \int \frac{\cos x\,dx}{\cos^4 x} = \int \frac{du}{(1-u^2)^2}\cdot$
Or $\frac{1}{(1-u^2)^2} = \frac{1}{4(u-1)^2} + \frac{1}{4(u+1)^2} + \frac{1}{4(u+1)} - \frac{1}{4(u-1)}\cdot$
Donc $\int \frac{dx}{\cos^3 x} = \frac{1}{4}\ln\frac{1+\sin x}{1-\sin x} + \frac{1}{4}\left(\frac{1}{1-\sin x} - \frac{1}{1+\sin x}\right) + c$.

Exercice 3.6. On a

$$\begin{aligned} x^3+y^3+z^3-3xyz &= (x+y+z)((x^2+y^2+z^2)-(xy+yz+zx)) \\ &= (x+y+z)((x+y+z)^2-3(xy+yz+zx)). \end{aligned}$$

On en déduit que $3xyz = x^3+y^3+z^3-(x+y+z)((x+y+z)^2-3(xy+yz+zx)) = 15-3(9-3) = -3$. Donc x, y, z sont les trois racines du polynôme $X^3 - 3X^2 + X + 1$. Ce polynôme possède la racine « évidente » 1, donc $X^3 - 3X^2 + X + 1 = (X-1)(X^2-2X-1) = (X-1)(X-1-\sqrt{2})(X-1+\sqrt{2})$. Donc x, y, z sont égaux à permutation près à $1, 1+\sqrt{2}, 1-\sqrt{2}$.

Exercice 3.7. Notons d le PGCD de a et b.

1. Remarquons d'abord que, pour tout $p, q \in \mathbb{N}$, le polynôme $X^p - 1$ divise le polynôme $X^{pq} - 1$. Notons $a = bq + r$ la division euclidienne de a par b. On a $X^a - 1 = X^r(X^{bq} - 1) + X^r - 1$. Puisque $X^b - 1$ divise $X^r(X^{bq} - 1)$ et $r < b$, le reste de la division euclidienne de $X^a - 1$ par $X^b - 1$ est $X^r - 1$.
2. On peut supposer que $a \geqslant b > 0$. Effectuons l'algorithme d'Euclide : on obtient une suite décroissante $r_0 = a \geqslant r_1 = b > r_2 > \ldots > r_n = d$ tels que, pour $2 \leqslant j \leqslant n$, r_j soit le reste de la division euclidienne de r_{j-2} par r_{j-1} et r_n divise r_{n-1}. On déduit de la question 1, que le reste de la division euclidienne de $X^{r_{j-2}} - 1$ par $X^{r_{j-1}} - 1$ est $X^{r_j} - 1$; de plus $X^{r_n} - 1$ divise $X^{r_{n-1}} - 1$. D'après l'algorithme d'Euclide, le PGCD de $X^a - 1$ et $X^b - 1$ est donc $X^d - 1$.
3. Donnons-nous une relation de Bézout $au - bv = d$. On a donc $(X^{au} - 1) - X^d(X^{bv} - 1) = X^d - 1$. Puisque $X^a - 1$ divise $X^{au} - 1$ et $X^b - 1$ divise $X^{bv} - 1$ cette égalité est une relation de Bézout.
4. Les polynômes A et B sont scindés à racines simples sur $\mathbb{C}$. Les racines communes sont les $\lambda \in \mathbb{C}$ tels que $\lambda^a = \lambda^b = 1$ c'est à dire les éléments de $\mathbb{C}^*$ dont l'ordre dans le groupe $\mathbb{C}^*$ divise à la fois a et b, *i.e.* qui divise d. On en déduit que le PGCD de A et B vus comme polynômes sur $\mathbb{C}$ est $\prod_{k=0}^{d-1}(X - e^{\frac{2ik\pi}{d}}) = X^d - 1$.
   Pour finir, démontrons le résultat fort utile suivant :

   Théorème. *Soit L un corps commutatif et K un sous-corps de L. Soient $A, B \in K[X]$. Notons D leur PGCD vus comme polynômes sur K. Alors D est le PGCD de A et B vus comme polynômes sur L.*

   Démonstration. On a une relation de Bézout $D = AU + BV$ avec $U, V \in K[X] \subset L[X]$, et puisque D est un diviseur commun de A et B (sur K donc sur L) c'est leur PGCD. □

Exercice 3.8.

1. Notons $\lambda_1, \ldots, \lambda_k$ les racines de P de partie imaginaire strictement positive écrites avec leur multiplicité. On a $P = \prod_{j=1}^{k}(X - \lambda_j)(X - \overline{\lambda_j}) = A\overline{A}$ où $A = \prod_{j=1}^{k} X - \lambda_j$. Les polynômes A et $\overline{A}$ n'ont pas de racines communes : ils sont premiers entre eux.
2. Existence : Comme A et $\overline{A}$ sont premiers entre eux, il existe $U, V \in \mathbb{C}[X]$ tels que $AU + \overline{A}V = 1$. Alors AU est congru à 1 modulo $\overline{A}$, donc $i(1 - 2AU)$ est congru à i modulo A, et à $-i$ modulo $\overline{A}$. Écrivons $i(1 - 2AU) = PQ + J$ la division euclidienne de $i(1 - 2AU)$ par P. Alors J convient.
   Unicité : Si J_1 et J_2 vérifient ces conditions alors $J_1 - J_2$ est divisible par A et $\overline{A}$ donc par leur PPCM qui est P - puisque A et $\overline{A}$ sont premiers entre eux. Comme $J_1 - J_2$ est de degré $< 2k$, il vient $J_1 - J_2 = 0$.
3. Le polynôme $\overline{J}$ vérifie les mêmes conditions : écrivons $J - i = AB$: et $J + i = \overline{A}C$ il vient $\overline{J} + i = \overline{AB}$ et $\overline{J} - i = A\overline{C}$. Donc $J = \overline{J}$ (d'après l'unicité) soit $J \in \mathbb{R}[X]$.
   Enfin $J^2 \equiv -1$ modulo A et modulo $\overline{A}$ donc $J^2 \equiv -1$ $[P]$.
4. Il s'agit de vérifications plutôt longues - mais sans surprises...
5. Soit $P \in \mathbb{R}[X]$ un polynôme unitaire annulateur de f sans racines réelles : par exemple le polynôme minimal ou le polynôme caractéristique de f. Soit $J \in \mathbb{R}[X]$ comme ci-dessus. On pose $j = J(f)$. Puisque $P | J^2 + 1$, il vient $j^2 = -\mathrm{id}_E$; enfin $fJ(f) = J(f)f$, d'où le résultat.

Exercice 3.9.

1. Si A et B sont deux polynômes, on a $\dfrac{(AB)'}{AB} = \dfrac{A'}{A} + \dfrac{B'}{B}$. Décomposons P en facteurs irréductibles : $P = a\prod_{i=1}^{k} P_i^{m_i}$. On a $\dfrac{P'}{P} = \sum_{i=1}^{k} \dfrac{m_i P_i'}{P_i}$.

2. *Théorème de Lucas.* Écrivons $P = a\prod_{i=1}^{k}(X-\lambda_i)^{m_i}$. Si z est une racine de P' qui n'est pas un des λ_i, on a
$$0 = \frac{P'(z)}{P(z)} = \sum_{i=1}^{k} \frac{m_i}{z-\lambda_i} = \sum_{i=1}^{k} \frac{m_i\overline{(z-\lambda_i)}}{|z-\lambda_i|^2}.$$
Prenant le complexe conjugué de cette égalité, on trouve $\sum_{i=1}^{k} \dfrac{m_i(z-\lambda_i)}{|z-\lambda_i|^2} = 0$, donc z est barycentre des λ_i affectés des coefficients strictement positifs $\dfrac{m_i}{|z-\lambda_i|^2}$.

3. a) Le triplet $(1, j, j^2)$ est un repère affine d'où l'existence et unicité de ℓ. Toute application affine est de cette forme... On peut aussi résoudre le système et trouver $a = \dfrac{\alpha + j^2\beta + j\gamma}{3}$, $b = \dfrac{\alpha + j\beta + j^2\gamma}{3}$ et $c = \dfrac{\alpha+\beta+\gamma}{3}$. Écrivant $(u+v)^3 = 3uv(u+v) + u^3 + v^3$, on trouve immédiatement que α, β et γ sont racines de $(X-c)^3 - 3ab(X-c) - a^3 - b^3$.

   b) Convenons d'appeler *ellipse de Steiner* d'un triangle toute ellipse tangente au milieu des trois côtés du triangle. Nous devons donc établir l'existence et unicité d'une ellipse de Steiner.
   - La transformation ℓ transforme le cercle inscrit $\mathcal{C}$ du triangle équilatéral $(1, j, j^2)$ en une ellipse de Steiner - d'où son existence.
   - Si $\mathcal{E}$ est une ellipse de Steiner du triangle $T = (\alpha, \beta, \gamma)$, il existe une transformation affine ℓ' telle que $\ell'(\mathcal{E})$ soit un cercle. C'est le cercle inscrit du triangle $\ell(T)$, et une ellipse de Steiner pour ce triangle. Notons (A, B, C) le triangle $\ell'(T)$ et A', B', C' les milieux et points de tangence. On a $AC' = BC'$, $AB' = CB'$ et $BA' = CA'$ (milieu) et $AB' = AC'$, $BA' = BC'$ et $CA' = CB'$ (cercle inscrit). Donc $\ell'(T)$ est équilatéral. Alors, $\ell' \circ \ell$ est une similitude, donc $\ell' \circ \ell(\mathcal{C})$ est le cercle inscrit $\ell'(\mathcal{E})$, donc $\mathcal{E} = \ell(\mathcal{C})$, d'où l'unicité.

   Enfin, écrivons $a = |a|uv$ et $b = |b|u\overline{v}$ où u et v sont des nombres complexes de module 1. On a $\ell = T_c \circ R_u \circ D \circ \mathbb{R}_v$ où R_u, R_v sont des rotations $R_v(z) = vz$, $R_u(z) = uz$, T_c est la translation $T(z) = z + c$; enfin $D(z) = |a|z + |b|\overline{z}$, soit $D(x+iy) = (|a|+|b|)x + i(|a|-|b|)y$. Notons que comme α, β, γ ne sont pas alignés, ℓ est bijective, donc $|a| \neq |b|$.

   On a $R_v(\mathcal{C}) = \mathcal{C}$; l'image par D de ce cercle de centre 0 et de rayon 1/2 est l'ellipse d'équation $\left(\dfrac{x}{|a|+|b|}\right)^2 + \left(\dfrac{y}{|a|-|b|}\right)^2 = \dfrac{1}{4}$; ses foyers ont donc comme coordonnées $y = 0$ et $x = \pm\dfrac{\sqrt{(|a|+|b|)^2 - (|a|-|b|)^2}}{2} = \pm\sqrt{|ab|}$.

   Enfin $T_c \circ R_u$ est une isométrie donc les foyers de l'ellipse de Steiner ont pour affixes $c \pm u\sqrt{|ab|} = c \pm z$ où z est une racine carrée de $ab = u^2|ab|$.

Dans une ellipse d'équation $\dfrac{x^2}{a^2} + \dfrac{y^2}{b^2} = 1$ (dans un repère orthonormé) de demi grand axe a et demi petit axe b (avec $a > b > 0$), les foyers ont pour coordonnées $(\pm\sqrt{a^2-b^2}, 0)$. Pour se le rappeler, notons $A = (a, 0)$ et $B = (0, b)$. Si F et F' sont les foyers de coordonnées $(\pm c, 0)$, on a $AF + AF' = 2a = BF + BF' = 2\sqrt{b^2+c^2}$.

Exercice 3.10. Fixons un repère orthonormé $(0, i, j)$ dans lequel l'équation de H soit $xy = c$. Notons (p, q) les coordonnées de P dans ce repère. On a $c = pq$. Celles de P' sont donc $(-p, -q)$. Quitte à changer i en son opposé, on peut supposer que $p > 0$. L'équation du cercle $\mathcal{C}$ est $x^2 + y^2 - 2px - 2qy =$

$3(p^2+q^2)$. Le point de coordonnées (x,y) est dans l'intersection $H \cap \mathcal{C}$ si et seulement si $xy = pq$ et $x^2+y^2-2px-2qy = 3(p^2+q^2)$. Multipliant par x^2, on trouve (puisque $xy = pq$)

$$x^4 + p^2q^2 - 2px^3 - 2pq^2x - 3(p^2+q^2)x^2 = 0.$$

Posons $g(x) = x^4 - 2px^3 - 3(p^2+q^2)x^2 - 2pq^2x + p^2q^2$. Les points d'intersection de $H \cap \mathcal{C}$ sont les couples $(x, \dfrac{pq}{x})$, avec $x \in \mathbb{R}^*$ racine de g. On sait déjà que $-p$ est un racine de cette équation.

1. On a $g(0) = p^2q^2 > 0$ et $g(p) = -p^2(p^2+q^2) < 0$, enfin $\lim\limits_{x\to\pm\infty} g(x) = +\infty$. On en déduit que g a une racine dans $]0,p[$, une racine dans $]p,+\infty[$ et un nombre pair de racines (avec leur multiplicité) dans $]-\infty,0[$. Comme $-p$ est racine, ce polynôme du 4e degré est scindé sur $\mathbb{R}$.
2. Les trois autres racines satisfont $x_A + x_B + x_C - p = 2p$, donc $x_A + x_B + x_C = 3p$. Par symétrie $(x,y) \mapsto (y,x)$, on trouve que les ordonnées des points d'intersection vérifient $y_A + y_B + y_C = 3q$. [Ou, mieux, $y_A + y_B + y_C - q = \dfrac{pq}{x_A} + \dfrac{pq}{x_B} + \dfrac{pq}{x_C} - \dfrac{pq}{p} = \dfrac{pq\sigma_3}{\sigma_4} = 2q$.] Cela prouve que P est le centre de gravité du triangle ABC. Par ailleurs, P étant le centre du cercle circonscrit du triangle ABC, médianes et médiatrices sont confondues. Donc ABC est équilatéral.

Exercice 3.11.

1. a) Le plus simple est d'utiliser la matrice compagnon de P : c'est une matrice à coefficients entiers $A \in M_n(\mathbb{Z})$ dont le polynôme caractéristique est $(-1)^n P$. Alors le polynôme caractéristique de A^ℓ est $(-1)^n P_\ell$ (il suffit pour voir cela de trigonaliser A). Il est à coefficients entiers.

   b) On sait que $(-1)^{n-j}a_j$ est la somme des produits $x_{i_1}\dots x_{i_j}$ où $1 \leqslant i_1 < i_2 < \dots < i_j \leqslant n$. Il y a $\binom{n}{j}$ tous de module 1.

   On peut aussi raisonner par récurrence sur n, écrivant $Q = (X-x_n)Q_1$ où $Q_1 = \prod\limits_{j=1}^{n-1} X - x_j$.

   Si on écrit $Q_1 = \sum\limits_{j=0}^{n} b_j X_j$ (avec $b_n = 1$), on a $a_0 = -x_n b_0$ et, pour $j \neq 1$, $a_j = b_{j-1} - x_n b_j$.

   Donc $|a_0| \leqslant 1$ (en fait $|a_0| = 1$) et $|a_j| \leqslant |b_j| + |b_{j-1}|$; d'après l'hypothèse de récurrence, il vient $|a_j| \leqslant \binom{n-1}{j} + \binom{n-1}{j-1} = \binom{n}{j}$.

   c) D'après b), il y a un nombre fini de polynômes de degré n à coefficients entiers dont toutes les racines (complexes) sont de module 1. L'application ℓ mapsto P_ℓ n'est donc pas injective.

   d) On a $\prod\limits_{k=1}^{n} X - x_k^\ell = \prod\limits_{k=1}^{n} X - x_k^m$. L'énoncé résulte de la décomposition en facteurs irréductibles.

   e) Démontrons cette propriété par récurrence sur r. C'est vrai pour $r = 0$ et 1. Supposons-la vérifiée pour r. Soit alors $k \in \{1,\dots,n\}$ et posons $j = \sigma(k)$. On a

   $$(x_k)^{\ell^{r+1}} = (x_k^\ell)^{\ell^r} = (x_j^m)^{\ell^r} = (x_j^{\ell^r})^m = x_{\sigma^r(j)}^{m^r})^m = (x_{\sigma^{r+1}(k)}^{m^{r+1}}.$$

   f) Notons r l'ordre de la permutation σ. On a $x_k^{m^r - \ell^r} = 1$.

   Remarque. En utilisant le fait que les polynômes cyclotomiques sont irréductibles sur $\mathbb{Q}$, on en déduit que P est un produit de polynômes cyclotomiques.

2. En effet, il existe $Q \in \mathbb{Z}[X]$ unitaire de degré $2n$ tel que $x^n P(x+1/x) = Q(x)$ pour tout $x \in \mathbb{C}^*$. Écrivant $P = \prod\limits_{j=1}^{n} X - b_j$, on a $Q = \prod\limits_{j=1}^{n} X^2 - b_j X + 1$. Puisque on a $b_j \in \mathbb{R}$ et $|b_j| \leqslant 2$, le polynôme

$X^2 - b_jX + 1$ a deux racines complexes conjuguées x_j et $\overline{x}_j$ de module 1 (éventuellement toutes deux égales à 1 ou -1).

D'après ce qui précède x_j est une racine de l'unité $x_j = e^{iq_j\pi}$ avec $q_j \in \mathbb{Q}$, donc $b_j = x_j + \overline{x}_j = 2\cos q_j\pi$.

3. Les racines du polynôme caractéristique de A sont réelles comprises entre -2 et 2. Elles sont donc de la forme $2\cos q\pi$ avec $q \in \mathbb{Q}$ d'après la question précédente.

Exercice 3.12.

1. Si f est surjective, il existe $P \in E_n$ et $Q \in E_m$ tels que $f_{A,B}(P,Q) = 1$ donc A et B sont premiers entre eux. Donc (ii)⇒(i).

   Si A et B sont premiers entre eux et $f_{A,B}(P,Q) = 0$, alors $AP = -BQ$; ce polynôme est un multiple commun de A et B, donc de leur PPCM AB. Comme son degré est $< m+n$, il est nul, donc $P = Q = 0$; l'application linéaire f est alors injective, donc surjective par égalité des dimensions. Donc (i)⇒(ii).

   La matrice de $f_{A,B}$ de la base $\mathcal{B}_0 = ((1,0),(X,0),\dots,(X^{n-1},0),(0,1),(0,X),\dots,(0,X^{m-1}))$ de $E_n \times E_m$ dans la base $\mathcal{B}_1 = (1,X,\dots,X^{m+n-1})$ de E_{n+m} est la matrice carrée de colonnes $C_0,\dots,C_{n-1},D_0,\dots,D_{m-1}$. L'équivalence (ii) $\iff$ (iii) en résulte.

2. Le polynôme A a des racines multiples si et seulement si A et A' ne sont pas premiers entre eux, donc si et seulement si $\mathrm{Res}_{A,A'} = 0$.

3. a) Dans ce cas $\mathrm{Res}_{A,B} = \begin{vmatrix} c & b & 0 \\ b & 2a & b \\ a & 0 & 2a \end{vmatrix} = -a(b^2 - 4ac)$.

   b) On a $\mathrm{Res}_{A,B} = \begin{vmatrix} q & 0 & p & 0 & 0 \\ p & q & 0 & p & 0 \\ 0 & p & 3 & 0 & p \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = 4p^3 + 27q^2$.

   c) Démontrons par récurrence sur le degré n de A que $\mathrm{Res}_{A,X-b} = A(b)$.

   Pour $n = 1$, on a $\mathrm{Res}(a_0 + a_1X, X - b) = \begin{vmatrix} a_0 & -b \\ a_1 & 1 \end{vmatrix} = a_0 + a_1b$.

   Écrivons $A = \sum_{k=0}^{n} a_kX^k = a_0 + XA_1$, où $A_1 = \sum_{k=1}^{n} a_kX^{k-1}$.

   On a

$$\mathrm{Res}(A, X-b) = \begin{vmatrix} a_0 & -b & 0 & \dots & 0 & 0 \\ a_1 & 1 & -b & \dots & 0 & 0 \\ a_2 & 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & 0 & 0 & \dots & 1 & -b \\ a_n & 0 & 0 & \dots & 0 & 1 \end{vmatrix}.$$

   Développant par la première ligne, il vient $\mathrm{Res}(A, X-b) = a_0 + b\mathrm{Res}(A_1, X-b)$. D'après l'hypothèse de récurrence il vient $\mathrm{Res}(A, X-b) = a_0 + bA_1(b) = A(b)$.

   NB On peut aussi développer par rapport à la dernière ligne, ou la première colonne...

   On peut aussi effectuer un changement de base :
   Considérons la base $\mathcal{B}_2 = (1, X-b, X(X-b), X^2(X-b), \dots, X^{n-1}(X-b))$. Décomposons A dans cette base en écrivant $A = A(b) + \sum_{k=0}^{m-1} \alpha_kX^k(X-b)$. La matrice de passage de $\mathcal{B}_1$ à $\mathcal{B}_2$

est triangulaire supérieure avec des 1 sur la diagonale. Donc $\mathrm{Res}_{A,B}$ est égal au déterminant de la matrice de f allant de la base $\mathcal{B}_0$ dans la base $\mathcal{B}_2$:

$$Mat_{\mathcal{B}_2,\mathcal{B}_0}(f) = \begin{pmatrix} A(b) & 0 & 0 & \dots & 0 \\ \alpha_0 & 1 & 0 & \dots & 0 \\ \alpha_1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_{n-1} & 0 & 0 & \dots & 1 \end{pmatrix}$$

donc $\mathrm{Res}_{A,(X-b)} = A(b)$.

4. a) Echanger A et B revient à permuter les colonnes de la matrice par la permutation σ définie par $\sigma(i) = m + i$ si $1 \leqslant i \leqslant n$ et $\sigma(i) = i - n$ si $n + 1 \leqslant i \leqslant m + n$. La signature de cette permutation est $(-1)^{mn}$.

   b) Remplacer B par bB revient à multiplier les m dernières colonnes par b.

   c) À l'aide de (b), on peut supposer que B_1 est unitaire. Notons n_1 et n_2 les degrés respectifs de B_1 et B_2 et posons $B = B_1B_2$ et $n = n_1 + n_2$.
   Considérons les applications linéaires

$$\begin{array}{lll} \varphi : E_{n_1} \times E_{n_2} \times E_m \to E_n \times E_m, & \text{définie par} & \varphi(P_1, P_2, Q) = (P_1 + B_1P_2, P) \\ g : E_{n_1} \times E_{n_2} \times E_m \to E_{n_1} \times E_{m+n_2}, & \text{définie par} & g(P_1, P_2, Q) = (P_1, AP_2 + B_2Q) \\ h : E_{n_1} \times E_{m+n_2} \to E_{m+n}, & \text{définie par} & h(P_1, R) = AP_1 + B_1R, \end{array}$$

   de sorte que $f_{A,B} \circ \varphi = h \circ g$.
   On considère les matrices de ces applications dans les bases $\mathcal{B}_0$ de $E_n \times E_m$ et et $\mathcal{B}_1$ de E_{m+n}, ainsi que les bases analogues $\hat{\mathcal{B}}$ de $E_{n_1} \times E_{m+n_2}$ et $\tilde{\mathcal{B}}$ de $E_m \times E_{n_1} \times E_{n_2}$:

$$\hat{\mathcal{B}} = ((1,0),(X,0),\dots,(X^{n_1-1},0),(0,1),(0,X),\dots,(0,X^{m+n_2-1}))$$

$$\tilde{\mathcal{B}} = ((1,0,0),(X,0,0),\dots,(X^{m-1},0,0),(0,1,0),\dots,(0,X^{n_1-1},0),(0,0,1),\dots,(0,0,X^{n_2-1}))$$

   Dans ces bases :
   - la matrice $Mat(\varphi)$ de φ est triangulaire supérieure avec des 1 sur la diagonale et son déterminant vaut 1 (car le polynôme B_1 est supposé unitaire) ;
   - la matrice $Mat(g)$ de g est diagonale par blocs $Mat(g) = \begin{pmatrix} I_{n_1} & 0 \\ 0 & Mat(f_{A,B_2}) \end{pmatrix}$; son déterminant vaut R_{A,B_2} ;
   - celle de h est triangulaire par blocs de la forme $Mat(h) = \begin{pmatrix} Mat(f_{A,B_2}) & Q \\ 0 & T \end{pmatrix}$ où T est triangulaire supérieure avec des 1 sur la diagonale et son déterminant vaut 1 (car B_1 est supposé unitaire).

   Les formules (d), (e) et (f) en résultent facilement.

Exercice 3.13.

1. Tout diviseur commun de P_{k+1} et P_k divise $P_{k-1} = Q_{k+1}P_k - P_{k+1}$, donc il divise P_{k-2} et par récurrence, il divise P et P'. Or P et P' sont supposés premiers entre eux.
2. Sur tout intervalle ne rencontrant pas A, les polynômes P_k gardent un signe constant. Le dernier reste non nul est le pgcd de P et P'. Il est constant (et non nul).
3. Puisque P_k et P_{k+1} sont premiers entre eux, ils n'ont pas de racines communes, donc $P_{k+1}(x) \neq 0$. Comme $P_{k-1}(x) = Q_{k+1}(x)P_k - P_{k+1}(x) = -P_{k+1}(x)$, $P_{k-1}(x)$ et $P_{k+1}(x)$ sont non nuls et (de signes) opposés. L'ensemble A est fini. Il existe donc un intervalle ouvert J contenant x tel que $J \cap A = \{x\}$.

a) Sur J et P_{k-1} et P_{k+1} gardent des signes contraires ; donc pour $y \in J \setminus \{x\}$, quel que soit le signe de $P_k(y)$, le nombre de changements de signe dans la suite $P_{k-1}(y), P_k(y), P_{k+1}(y)$ est égal à 1.

b) Notons $N_x = \{k;\ \ 1 \leqslant k < m;\ P_k(x) = 0\}$ et écrivons $N_x = \{k_1, \ldots, k_r\}$, avec $r \geqslant 1$ et $0 < k_1 < \ldots < k_r < m$. Par (a), si $r \geqslant 2$ et $1 \leqslant j < r$, alors $k_{j+1} \geqslant k_j + 2$; de plus, pour $y \in J \setminus \{x\}$, $n(y)$ est le nombre de changements de signes dans la suite formée de $P_j(y)$ pour $j \notin N_x$. Il est constant sur J.

4. Comme ci-dessus, posons $N_x = \{k,\ 1 \leqslant k < m;\ P_k(x) = 0\}$. Par 3.a), $1 \notin N_x$ et le nombre n_0 de changements de signes dans la suite formée de $P_j(y)$ pour $1 \leqslant j \leqslant m,\ j \notin N_x$ est constant sur J. De plus, si $P'(x) > 0$, alors P est croissante sur J, donc pour $y \in J$, on a $P(y) > 0$ si $y > x$ et $P(y) < 0$ si $y < x$. Il s'ensuit que $n_d(x) = n_0$ et $n_g(x) = n_0 + 1$.

5. Notons $x_1 < \ldots < x_p$ les points de $A \cap]a, b[$. On a $n(a) = n_g(x_1)$, $n_d(x_j) = n_g(x_{j+1})$ et $n_d(x_p) = n(b)$. Donc $n(a) - n(b) = \sum_{j=1}^{p} n_g(x) - n_d(x)$. Notons $B \subset A$ l'ensemble des racines de P. On a $n_g(x) - n_d(x) = 0$ si $x \notin B$ et $n_g(x) - n_d(x) = 1$ pour $x \in B$. Le théorème de Sturm en résulte.

Exercice 3.14.

1. Écrivons $P = \prod_{i=1}^{4} X - z_i = X^4 - aX^3 + bX^2 - cX + d$ et $\prod_{i=1}^{3} X - u_i = X^3 - \alpha X^2 + \beta X - \gamma$ où $a = z_1 + z_2 + z_3 + z_4$, $b = z_1z_2 + z_1z_3 + z_1z_4 + z_2z_3 + z_2z_4 + z_3z_4$, $c = z_1z_2z_3 + z_1z_2z_4 + z_1z_3z_4 + z_2z_3z_4$ et $d = z_1z_2z_3z_4$; $\alpha = u_1 + u_2 + u_3$, $\beta = u_1u_2 + u_1u_3 + u_2u_3$ et $\gamma = u_1u_2u_3$.
On trouve

$$\begin{aligned}
\alpha &= b \\
\beta &= z_1^2(z_2z_3 + z_2z_4 + z_3z_4) + z_2^2(z_1z_3 + z_1z_4 + z_3z_4) + z_3^2(z_1z_2 + z_1z_4 + z_2z_4) + \\
&\qquad + z_4^2(z_1z_2 + z_1z_3 + z_2z_3) \\
&= ac - 4d \\
\gamma &= z_1^2z_2^2z_3^2 + z_1^2z_2^2z_4^2 + z_1^2z_3^2z_4^2 + z_2^2z_3^2z_4^2 + z_1^3z_2z_3z_4 + z_1z_2^3z_3z_4 + z_1z_2z_3^3z_4 + z_1z_2z_3z_4^3 \\
&= (c^2 - bd) + (a^2 - 2b)d
\end{aligned}$$

2. Une fois trouvé u_1, on peut trouver $(z_1 + z_2)(z_3 + z_4) = u_2 + u_3$, et puisque on connait aussi $z_1 + z_2 + z_3 + z_4 = a$ on trouve $z_1 + z_2$ et $z_3 + z_4$. De même on trouve $z_i + z_j$ pour $i \neq j$. Donc on trouve enfin $2z_1 = (z_1 + z_2) + (z_1 + z_3) + (z_1 + z_4) - a$.

Exercice 3.15.

1. D'après le (petit) théorème de Fermat, tout élément de $\mathbb{F}_p$ est racine du polynôme $X^p - X$. Donc $\prod_{x \in \mathbb{F}_p} (X - x)$ divise $X^p - X$. Ces polynômes sont donc égaux car ils sont unitaires et ont même degré.

2. On a donc $X^{p-1} - 1 = \prod_{x \in \mathbb{F}_p^*} (X - x)$, et prenant la valeur en 0, il vient $-1 \equiv (-1)^{p-1}(p-1)!\ \ [p]$.

Exercice 3.16.

1. Notons $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ la réduction modulo p. C'est un morphisme d'anneaux. Si p divise tous les c_k, on a $\pi(AB) = 0$, et comme $\mathbb{F}_p[X]$ est intègre il vient $\pi(A) = 0$ ou $\pi(B) = 0$.

2. Si $c(A) = c(B) = 1$, aucun nombre premier ne divise tous les a_j ou tous les b_j. Donc par 1., aucun nombre premier ne divise tous les c_j, donc $c(AB) = 1$. Dans le cas général, on peut écrire $A = c(A)A_1$ et $B = c(B)B_1$ avec $A_1, B_1 \in \mathbb{Z}[X]$ de contenu 1. On a alors $AB = c(A)c(B)A_1B_1$ et donc $c(AB) = c(A)c(B)c(A_1B_1) = c(A)c(B)$.

3. Soit $P \in \mathbb{Z}[X]$ non scalaire. Si P est irréductible sur $\mathbb{Z}$, on a $c(P) = 1$ (puisque P est divisible par $c(P)$). Supposons donc que $c(P) = 1$ et que P n'est pas irréductible sur $\mathbb{Q}$ et donnons-nous une décomposition $P = AB$ avec $A, B \in \mathbb{Q}[X]$ non scalaires. Il existe $a, b \in \mathbb{N}^*$ tels que $aA \in \mathbb{Z}[X]$ et $bB \in \mathbb{Z}[X]$ (prendre les PPCM des dénominateurs des coefficients de A et B respectivement). Écrivons $aA = c(aA)A_1$ et $bB = c(bB)B_1$. On a alors $c(aA)c(bB) = c(abAB) = c(abP) = ab$, donc $abA_1B_1 = c(aA)c(bB)A_1B_1 = aAbB = abP$, ce qui donne $P = A_1B_1$, donc P n'est pas irréductible sur $\mathbb{Z}$.

Exercice 3.17. Supposons que $P = AB$ avec $A, B \in \mathbb{Z}[X]$. Comme P est unitaire, on peut supposer (quitte à les remplacer par leur opposé) que A et B sont unitaires. Notons n, a, b les degrés respectifs de P, A et B. Notons $\pi : \mathbb{Z}[X] \to \mathbb{F}_p[X]$ la réduction modulo p. C'est un morphisme d'anneaux. On a $p(P) = X^n = \pi(A)\pi(B)$. Or le seul polynôme unitaire de degré a divisant X^n est X^a, donc $\pi(A) = X^a$ et de même $\pi(B) = X^b$. En d'autres termes tous les coefficients sauf le coefficient dominant de A et B sont divisibles par p. Si A et B était non constants, p divise $A(0)$ et $B(0)$, donc p^2 divise $P(0)$, ce qui est contraire à l'hypothèse.

NB Cette démonstration marche aussi si au lieu de supposer que P est unitaire, on suppose juste que le contenu de P est 1 (*cf.* exerc. 3.16).

Application. Posons $P = \Phi_p(X + 1)$. On a $(X - 1)\Phi_p = X^p - 1$, donc $XP = (X + 1)^p - 1$. Il vient $X\pi(P) = X^p + 1 - 1 = X^p$, donc $\pi(P) = X^{p-1}$. Par ailleurs $P(0) = \Phi_p(1) = p$. On peut appliquer le critère d'Eisenstein : P est irréductible sur $\mathbb{Q}$, donc Φ_p est irréductible sur $\mathbb{Q}$.

Exercice 3.18.

1. Les racines multiples sont les racines du pgcd de P et P'.
2. Comme $X^p - X = \prod_{a \in \mathbb{F}_p} X - a$, le pgcd de P et $X^p - X$ est le produit des $X - a$ pour a racine de P.
3. a) On pose $A = \text{pgcd}(P, X^{\frac{p+1}{2}} - X)$ et $B = \text{pgcd}(P, X^{\frac{p-1}{2}} + 1)$.
   b) Pour $x \in \mathbb{F}_p^*$, on a $x^{\frac{p-1}{2}} \in \{-1, 1\}$. On a donc l'équivalence entre les assertions suivantes
      (i) Q sépare a et b ;
      (ii) $(a - c)^{\frac{p-1}{2}} \neq (b - c)^{\frac{p-1}{2}}$;
      (iii) $\left(\frac{c-a}{c-b}\right)^{\frac{p-1}{2}} = -1$;
      (iv) $\frac{c-a}{c-b}$ n'est pas un carré.

      L'application $c \mapsto \frac{c-a}{c-b}$ est une bijection de $\mathbb{F}_p \setminus \{a, b\}$ sur $\mathbb{F}_p \setminus \{0, 1\}$. Donc on a bien (un peu plus d') une chance sur deux de séparer a et b en prenant c au hasard.
   c) En prenant c au hasard puis en regardant le pgcd de P et $Q_c = (X-c)^{\frac{p-1}{2}} - 1$ on a beaucoup de chances de se retrouver avec deux facteurs de degré plus petit. Puis on recommence avec un nouveau c...

Exercice 3.19. Solution très rapide...

1. a) est clair une fois que l'on remarque que m et n étant premiers entre eux, si mn a des facteurs carrés, alors m ou n aussi.
   b) On démontre que, pour tout $n \in \mathbb{N}^*$, les matrices $U = (u_{i,j}) \in M_n(\mathbb{C})$ et $V = (v_{i,j}) \in M_n(\mathbb{C})$ définie par $u_{i,j} = 1$ si $j|i$ et 0 sinon et $v_{i,j} = \mu(i/j)$ si $i \neq j$ sont inverse l'une de l'autre. En effet, $UV = (w_{i,j})$, où $w_{i,j} = \sum_k u_{i,k}v_{k,j}$. Donc $w_{i,j} = 0$ si j ne divise pas i, $w_{i,i} = 1$ et,

pour $q \in \mathbb{N}$, $q \geqslant 2$, on a $w_{jq,j} = \sum_{d|q} \mu(d)$. Or on démontre (en décomposant q en produit de nombres premiers) que, pour tout $q \geqslant 2$, on a $\sum_{d|q} \mu(d) = 0$.

2. a) La première égalité résulte de ce qu'il y a exactement p^n polynômes unitaires de degré n ; la dernière est un regroupement des polynômes irréductibles par leur degré. Écrivant $(R_k)_{k\in\mathbb{N}}$ les polynômes irréductibles unitaires, on a

$$\prod_{k=0}^{m} \frac{1}{1-t^{\partial R_k}} = \prod_{k=0}^{m} \sum_{j_k=0}^{+\infty} t^{j_k \partial R_k} = \sum_{(j_0,\dots,j_m)\in\mathbb{N}^{m+1}} t^{\sum_{k=1}^m j_k \partial R_k} = \sum_{(j_0,\dots,j_m)\in\mathbb{N}^{m+1}} t^{\partial(\prod_{k=1}^m R_k^{j_k})} = \sum_{A\in Q_m} t^{\partial A}$$

où l'on a noté Q_m l'ensemble des polynômes n'ayant d'autres diviseurs irréductibles que $R_0, \dots, R_m$ et qui donc s'écrivent de manière unique sous la forme $\prod_{k=1}^{m} R_k^{j_k}$, d'où l'égalité du milieu, en prenant la limite quand $m \to \infty$.
Cela dit, il faut bien justifier ces formules qui convergent absolument pour $|t| < 1/p$.

b) On a $\dfrac{(fg)'}{fg} = \dfrac{f'}{f} + \dfrac{g'}{g}$, d'où (après justification du passage à la limite), $\dfrac{p}{1-pt} = \sum_{n=1}^{+\infty} \dfrac{nN_n t^{n-1}}{1-t^n}$.
Multipliant par t, on trouve $\sum_{k=1}^{+\infty} p^k t^k = \sum_{n=1}^{+\infty}\sum_{k=1}^{+\infty} nN_n t^{kn}$. Donc, prenant le terme d'ordre ℓ dans cette série entière $p^\ell t^\ell = \sum_{n|\ell} nN_n$.

c) résulte immédiatement de 1.b) et 2.b).

d) On a donc $nN = p^n + \sum_{d|n;d\neq n} \mu(\frac{n}{d}) p^d \geqslant p^n - \sum_{d|n;\ d\neq n} p^d \geqslant p^n - \sum_{1\leqslant d\leqslant n/2} p^d \geqslant p^n - (n/2)p^{n/2}$.
On a $p^{n/2} > n/2$, d'ou $N_n > 0$.

e) Il existe donc au moins un polynôme irréductible P de degré n dans $\mathbb{F}_p[X]$. Alors $\mathbb{F}_p[X]/(P)$ est un corps à p^n éléments.