CORRIGÉ

Agrégation interne · CORRIGÉ

DM n°05 — Anneaux Z/nZ, éléments inversibles et théorème des restes chinois

CHAPITRES

Congruences et PGCD · Anneaux Z/nZ et éléments inversibles · Diviseurs de zéro et idéaux · Théorème des restes chinois · Indicatrice d'Euler, idempotents et équations polynomiales

I Multiplier modulo N

1

(a) Pour $a = 5$, les valeurs successives de $5x$ modulo 12, pour $x = 0, \dots, 11$, sont

$$0, 5, 10, 3, 8, 1, 6, 11, 4, 9, 2, 7.$$

Les douze restes apparaissent exactement une fois : T_5 est bijective.

(b) Pour $a = 8$,

$$8x \equiv 0, 8, 4, 0, 8, 4, \dots \pmod{12}.$$

L'image est $\{0, 4, 8\}$ et chacun de ces trois éléments possède quatre antécédents.

(c) On obtient

$$5x \equiv 7 \pmod{12} \iff x \equiv 11 \pmod{12},$$
$$8x \equiv 4 \pmod{12} \iff x \equiv 2, 5, 8, 11 \pmod{12},$$

tandis que $8x \equiv 2 \pmod{12}$ n'a aucune solution. La distinction suggérée est

$$\mathrm{PGCD}(5, 12) = 1, \qquad \mathrm{PGCD}(8, 12) = 4.$$

2

(a) Si $\mathrm{PGCD}(u, v) = 1$, Bézout fournit $r, s \in \mathbb{Z}$ tels que $ru + sv = 1$. En multipliant par w,

$$ruw + svw = w.$$

Si $v \mid uw$, alors v divise les deux termes du membre de gauche ; donc $v \mid w$.

(b) Écrivons $a = da_0$ et $N = dN_0$, avec $\mathrm{PGCD}(a_0, N_0) = 1$. Alors

$$\begin{aligned} ax \equiv ay \pmod{N} &\iff N \mid a(x - y) \\ &\iff dN_0 \mid da_0(x - y) \\ &\iff N_0 \mid a_0(x - y). \end{aligned}$$

D'après (a), ceci équivaut à $N_0 \mid x - y$, soit

$$\boxed{ax \equiv ay \pmod{N} \iff x \equiv y \pmod{N/d}.}$$

(c) Pour un x fixé, les y ayant la même image sont exactement ceux qui satisfont $y \equiv x \pmod{N/d}$. Modulo N, ils sont représentés par

$$x, \quad x + \frac{N}{d}, \quad \ldots, \quad x + (d-1)\frac{N}{d}.$$

Il y en a exactement d. Ainsi T_a est injective, donc bijective sur un ensemble fini de cardinal N, si et seulement si $d = 1$. Par conséquent

$$\boxed{T_a \text{ est bijective} \iff \mathrm{PGCD}(a, N) = 1.}$$

3

Supposons d'abord $ax \equiv b \pmod{N}$. Alors $b = ax - kN$ pour un certain $k \in \mathbb{Z}$; tout diviseur commun de a et N divise donc b. Ainsi $d \mid b$.

Réciproquement, si $d \mid b$, écrivons $a = da_0$, $N = dN_0$, $b = db_0$, avec $\mathrm{PGCD}(a_0, N_0) = 1$. La congruence équivaut à

$$a_0 x \equiv b_0 \pmod{N_0}.$$

Bézout donne un inverse de a_0 modulo N_0, donc au moins une solution x_0.

Si x est une autre solution, alors $ax \equiv ax_0 \pmod{N}$. La question 2 donne

$$x \equiv x_0 \pmod{N/d}.$$

Les solutions modulo N sont donc exactement

$$\boxed{x_0 + k\frac{N}{d}, \qquad k = 0, \ldots, d-1.}$$

Il y en a d.

4

La congruence $ax \equiv 1 \pmod{N}$ admet une solution si et seulement si $\mathrm{PGCD}(a, N) \mid 1$, donc si et seulement si $\mathrm{PGCD}(a, N) = 1$. Dans ce cas, la question 3 donne une unique solution modulo N.

L'algorithme d'Euclide donne

$$\begin{aligned} 101 &= 2 \times 37 + 27, \\ 37 &= 27 + 10, \\ 27 &= 2 \times 10 + 7, \\ 10 &= 7 + 3, \\ 7 &= 2 \times 3 + 1. \end{aligned}$$

En remontant,

$$1 = 11 \times 101 - 30 \times 37.$$

Ainsi -30 est un inverse de 37 modulo 101, soit

$$37^{-1} \equiv 71 \pmod{101}.$$

Puis

$$x \equiv 71 \times 23 \equiv 17 \pmod{101}.$$

II Les classes modulo N

5

(a) La relation est réflexive puisque $N \mid a - a$, symétrique puisque $N \mid a - b$ implique $N \mid b - a$, et transitive puisque $N \mid a - b$ et $N \mid b - c$ impliquent $N \mid a - c$. C'est donc une relation d'équivalence.

(b) Pour tout $a \in \mathbb{Z}$, la division euclidienne donne $a = qN + r$ avec $0 \leqslant r < N$. Donc $a \equiv r \pmod{N}$ et $\overline{a} = \overline{r}$.

Si $\overline{r} = \overline{s}$ avec $0 \leqslant r, s < N$, alors $N \mid r - s$. Comme $|r - s| < N$, on a $r = s$. Il y a donc exactement N classes.

6

(a) Si $a \equiv a' \pmod{N}$ et $b \equiv b' \pmod{N}$, alors

$$(a + b) - (a' + b') = (a - a') + (b - b')$$

est divisible par N, donc $\overline{a + b} = \overline{a' + b'}$. De plus

$$ab - a'b' = a(b - b') + b'(a - a')$$

est divisible par N, donc $\overline{ab} = \overline{a'b'}$. Les deux classes sont donc indépendantes des représentants choisis, et les deux lois sont bien définies sur $\mathbb{Z}/N\mathbb{Z}$.

(b) Les propriétés d'associativité, de commutativité et de distributivité sont héritées de celles des entiers. Les éléments neutres sont $\overline{0}$ et $\overline{1}$, et l'opposé de $\overline{a}$ est $\overline{-a}$. Ainsi $\mathbb{Z}/N\mathbb{Z}$ est un anneau commutatif unitaire.

7

(a) Si $a' = a + kN$, les diviseurs communs de a' et N sont exactement les diviseurs communs de a et N. Donc $\mathrm{PGCD}(a', N) = \mathrm{PGCD}(a, N)$.

(b) La classe $\overline{a}$ est inversible si et seulement s'il existe b tel que $ab \equiv 1 \pmod{N}$. Par la question 4,

$$\boxed{\overline{a} \in (\mathbb{Z}/N\mathbb{Z})^\times \iff \mathrm{PGCD}(a, N) = 1.}$$

(c) $\overline{1}$ est inversible. Si u et v sont inversibles, alors uv l'est, d'inverse $v^{-1}u^{-1}$. L'inverse d'un élément inversible est lui-même inversible et l'associativité est héritée de l'anneau. Ainsi $(\mathbb{Z}/N\mathbb{Z})^\times$ est un groupe multiplicatif.

8

(a) Soit $\overline{a} \neq \overline{0}$ et $d = \mathrm{PGCD}(a, N) > 1$. Comme $N \nmid a$, on a $d < N$. La classe de $b = N/d$ est donc non nulle et

$$ab = a\frac{N}{d} = \frac{a}{d}\,N,$$

donc $\overline{a}\,\overline{b} = 0$. Ainsi $\overline{a}$ est un diviseur de zéro.

Réciproquement, si $\overline{a}\,\overline{b} = 0$ avec $\overline{b} \neq 0$ et si $\mathrm{PGCD}(a, N) = 1$, alors $\overline{a}$ est inversible. En multipliant par son inverse, on obtiendrait $\overline{b} = 0$, contradiction. Ainsi

$$\boxed{\overline{a} \neq 0 \Longrightarrow \big(\overline{a} \text{ diviseur de zéro } \iff \mathrm{PGCD}(a, N) > 1\big).}$$

(b) Si N est premier, tout entier $a \in \{1, \dots, N-1\}$ est premier avec N ; toute classe non nulle est donc inversible. Un élément inversible ne pouvant être un diviseur de zéro, il n'existe alors aucun diviseur de zéro non nul.

Si N est composé, écrivons $N = rs$ avec $1 < r, s < N$. Alors $\overline{r}$ et $\overline{s}$ sont non nulles et $\overline{r}\,\overline{s} = \overline{0}$: il existe donc un diviseur de zéro non nul. De plus $\mathrm{PGCD}(r, N) = r > 1$, si bien que $\overline{r}$ n'est pas inversible d'après la question 7. Les trois propriétés proposées sont ainsi équivalentes. En particulier,

$$\boxed{\mathbb{Z}/N\mathbb{Z} \text{ est un corps } \iff N \text{ est premier.}}$$

III Réductions naturelles et idéaux

9

(a) La formule $[x]_r \mapsto [x]_s$ définit une application si $[x]_r = [y]_r$ implique $[x]_s = [y]_s$, c'est-à-dire si $r \mid x - y$ implique $s \mid x - y$ pour tous x, y. C'est vrai lorsque $s \mid r$.

Réciproquement, si l'application est bien définie, $[0]_r = [r]_r$ doit donner $[0]_s = [r]_s$, donc $s \mid r$. Ainsi

$$\boxed{\rho_{r,s} \text{ est bien définie } \iff s \mid r.}$$

(b) Lorsque $s \mid r$, pour toutes classes $[x]_r, [y]_r$,

$$\rho_{r,s}([x]_r + [y]_r) = [x + y]_s = [x]_s + [y]_s,$$
$$\rho_{r,s}([x]_r[y]_r) = [xy]_s = [x]_s[y]_s.$$

De plus $\rho_{r,s}([0]_r) = [0]_s$ et $\rho_{r,s}([1]_r) = [1]_s$. Ainsi $\rho_{r,s}$ est un morphisme d'anneaux. Enfin, toute classe $[y]_s$ est l'image de $[y]_r$: le morphisme est surjectif.

(c) On a

$$[x]_r \in \ker \rho_{r,s} \iff [x]_s = 0 \iff s \mid x.$$

Si $r = qs$, le noyau est

$$\{[0]_r, [s]_r, \dots, [(q-1)s]_r\}.$$

Ces q classes sont distinctes : si $[is]_r = [js]_r$ avec $0 \leqslant i, j < q$, alors $qs \mid (i - j)s$, donc $q \mid i - j$, ce qui impose $i = j$. D'où

$$\boxed{|\ker \rho_{r,s}| = \frac{r}{s}.}$$

10

Fixons $N \geqslant 2$.

(a) Pour un morphisme $f : A \to B$, on a $f(0) = 0$. Si $x, y \in \ker f$, alors $f(x-y) = f(x) - f(y) = 0$. Enfin, pour $a \in A$ et $x \in \ker f$, $f(ax) = f(a)f(x) = 0$. Le noyau est donc un idéal.

(b) Comme $d \mid N$, $\rho_{N,d}$ est définie et

$$\ker \rho_{N,d} = \{[x]_N \mid d \mid x\} = I_d.$$

(c) Soit I un idéal. Si $I = \{0\}$, alors $I = I_N$. Supposons $I \neq \{0\}$ et choisissons le plus petit entier $d \in \{1, \dots, N-1\}$ tel que $[d]_N \in I$.

Écrivons $N = qd + r$ avec $0 \leqslant r < d$. Dans $\mathbb{Z}/N\mathbb{Z}$,

$$[r]_N = [N]_N - q[d]_N = -q[d]_N \in I.$$

La minimalité de d impose $r = 0$, donc $d \mid N$.

Si $[a]_N \in I$ avec $0 \leqslant a < N$, écrivons $a = qd + r$ avec $0 \leqslant r < d$. Alors $[r]_N = [a]_N - q[d]_N \in I$, donc $r = 0$. Ainsi $d \mid a$ et $I \subset I_d$.

Réciproquement, $[d]_N \in I$ et la stabilité par multiplication donne $[kd]_N \in I$ pour tout k, donc $I_d \subset I$. Finalement

$$\boxed{\{\text{idéaux de } \mathbb{Z}/N\mathbb{Z}\} = \{I_d : d \mid N,\ d > 0\}.}$$

L'unicité de d découle du choix du plus petit représentant positif, avec le cas $I_N = \{0\}$ séparé.

IV Deux congruences à la fois

11

(a) Si $[x]_{mn} = [y]_{mn}$, alors $mn \mid x - y$. En particulier $m \mid x - y$ et $n \mid x - y$, donc

$$[x]_m = [y]_m, \qquad [x]_n = [y]_n.$$

La valeur de $\Phi_{m,n}([x]_{mn})$ ne dépend donc pas du représentant choisi.

Vérifions ensuite les opérations. Pour $x, y \in \mathbb{Z}$,

$$\begin{aligned}\Phi_{m,n}([x]_{mn} + [y]_{mn}) &= \Phi_{m,n}([x+y]_{mn}) \\ &= ([x+y]_m, [x+y]_n) \\ &= ([x]_m + [y]_m, [x]_n + [y]_n) \\ &= \Phi_{m,n}([x]_{mn}) + \Phi_{m,n}([y]_{mn}),\end{aligned}$$

et

$$\begin{aligned}\Phi_{m,n}([x]_{mn}[y]_{mn}) &= \Phi_{m,n}([xy]_{mn}) \\ &= ([xy]_m, [xy]_n) \\ &= ([x]_m[y]_m, [x]_n[y]_n) \\ &= \Phi_{m,n}([x]_{mn})\Phi_{m,n}([y]_{mn}).\end{aligned}$$

Enfin $\Phi_{m,n}(0) = (0,0)$ et $\Phi_{m,n}(1) = (1,1)$. Ainsi $\Phi_{m,n}$ est un morphisme d'anneaux.

(b) Posons $\ell = \mathrm{PPCM}(m,n)$. On a

$$[x]_{mn} \in \ker \Phi_{m,n} \iff m \mid x \text{ et } n \mid x \iff \ell \mid x.$$

Le noyau est donc constitué exactement des classes $[k\ell]_{mn}$, avec $k \in \mathbb{Z}$. Il y a mn/ℓ telles classes distinctes. La relation classique

$$\mathrm{PGCD}(m,n)\,\mathrm{PPCM}(m,n) = mn$$

donne donc

$$\boxed{|\ker \Phi_{m,n}| = \mathrm{PGCD}(m,n).}$$

(c) Pour un morphisme d'anneaux f, l'égalité $f(x) = f(y)$ équivaut à $f(x-y) = 0$. Ainsi f est injectif si et seulement si $\ker f = \{0\}$. D'après (b),

$$\boxed{\Phi_{m,n} \text{ injective} \iff \mathrm{PGCD}(m,n) = 1.}$$

12

(a) Comme $\mathrm{PGCD}(m,n) = 1$, le théorème de Bézout assure l'existence de $u, v \in \mathbb{Z}$ tels que

$$um + vn = 1.$$

Fixons désormais un tel couple et les éléments $e_m = [vn]_{mn}$ et $e_n = [um]_{mn}$.

(b) L'identité de Bézout donne $vn \equiv 1 \pmod{m}$ et $vn \equiv 0 \pmod{n}$, donc

$$\Phi_{m,n}(e_m) = (1,0).$$

De même,

$$\Phi_{m,n}(e_n) = (0,1).$$

(c) Pour tous $a, b \in \mathbb{Z}$, on identifie dans $\mathbb{Z}/mn\mathbb{Z}$ l'entier a à sa classe $[a]_{mn}$, et de même pour b. Le caractère multiplicatif et additif de $\Phi_{m,n}$ donne alors

$$\begin{aligned}\Phi_{m,n}([a]_{mn}e_m + [b]_{mn}e_n) &= ([a]_m,[a]_n)\Phi_{m,n}(e_m) + ([b]_m,[b]_n)\Phi_{m,n}(e_n)\\ &= ([a]_m,[a]_n)(1,0) + ([b]_m,[b]_n)(0,1)\\ &= ([a]_m,0) + (0,[b]_n)\\ &= ([a]_m,[b]_n).\end{aligned}$$

Or

$$[a]_{mn}e_m + [b]_{mn}e_n = [avn + bum]_{mn}.$$

Ainsi la classe $[avn+bum]_{mn}$ a bien pour image $([a]_m,[b]_n)$.

(d) La question (c) montre que $\Phi_{m,n}$ est surjective. Comme $\mathrm{PGCD}(m,n) = 1$, la question 11 donne son injectivité. Donc

$$\boxed{\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.}$$

(e) On a d'abord

$$e_m + e_n = [vn + um]_{mn} = 1, \qquad e_m e_n = [uvmn]_{mn} = 0.$$

Puis $1 - e_m = e_n$, donc $e_m(1 - e_m) = e_m e_n = 0$ et ainsi $e_m^2 = e_m$. De même, $e_n^2 = e_n$.

Si $\Phi_{m,n}(x) = (x_m, x_n)$, alors

$$\Phi_{m,n}(xe_m) = \Phi_{m,n}(x)\Phi_{m,n}(e_m) = (x_m, x_n)(1, 0) = (x_m, 0),$$

et de même

$$\Phi_{m,n}(xe_n) = (x_m, x_n)(0, 1) = (0, x_n).$$

Les deux idempotents isolent donc les deux composantes de x.

13

Posons $d = \mathrm{PGCD}(m, n)$ et $\ell = \mathrm{PPCM}(m, n)$.

(a) S'il existe x tel que $x \equiv a \pmod m$ et $x \equiv b \pmod n$, alors, puisque d divise m et n, on a $a \equiv b \pmod d$.

Réciproquement, supposons $d \mid b - a$ et écrivons $m = dm'$, $n = dn'$, avec $\mathrm{PGCD}(m', n') = 1$. Cherchons $x = a + mt$. La seconde congruence devient

$$m't \equiv \frac{b - a}{d} \pmod{n'}.$$

Comme $\mathrm{PGCD}(m', n') = 1$, la question 7 montre que $[m']_{n'}$ est inversible. Si c est un inverse de m' modulo n', on peut prendre par exemple

$$t \equiv c\,\frac{b - a}{d} \pmod{n'}.$$

Il existe donc bien un entier t satisfaisant la congruence, et $x = a + mt$ fournit une solution du système. Ainsi

$$\boxed{([a]_m, [b]_n) \in \mathrm{Im}\,\Phi_{m,n} \iff a \equiv b \pmod d.}$$

Cette condition est bien indépendante des représentants : si l'on remplace a par $a + km$, alors $d \mid m$ donne $a + km \equiv a \pmod d$; de même $b + qn \equiv b \pmod d$ puisque $d \mid n$.

(b) Si x et y sont deux solutions, m et n divisent $x - y$, donc $\ell = \mathrm{PPCM}(m, n)$ divise $x - y$. Réciproquement, si x_0 est une solution, alors $x_0 + k\ell$ reste congru à x_0 modulo m et modulo n pour tout $k \in \mathbb{Z}$. Les solutions sont donc exactement les entiers

$$x \equiv x_0 \pmod{\ell}.$$

Modulo mn, les classes de solutions sont

$$[x_0]_{mn},\ [x_0 + \ell]_{mn}, \ldots, [x_0 + (d - 1)\ell]_{mn},$$

puisque $mn = d\ell$. Elles sont distinctes et la suivante, obtenue pour $k = d$, revient à $[x_0]_{mn}$. Il y a donc exactement d classes de solutions modulo mn.

(c) Si $d = 1$, toute paire est compatible et la solution est unique modulo mn : $\Phi_{m,n}$ est un isomorphisme. Si $d > 1$, le couple $([0]_m, [1]_n)$ n'est pas compatible modulo d, donc $\Phi_{m,n}$ n'est pas surjective. Ainsi

$$\boxed{\Phi_{m,n} \text{ est un isomorphisme } \iff \mathrm{PGCD}(m,n) = 1.}$$

(d) Pour $m = 4$ et $n = 6$, $d = 2$. Le système $x \equiv 0 \pmod 4$, $x \equiv 1 \pmod 6$ imposerait à la fois $x \equiv 0 \pmod 2$ et $x \equiv 1 \pmod 2$: il est impossible.

Pour

$$x \equiv 1 \pmod 4, \qquad x \equiv 3 \pmod 6,$$

les deux restes sont congrus modulo 2. On vérifie que $x = 9$ convient. Les solutions vérifient $x \equiv 9 \pmod{12}$. Modulo 24, on obtient exactement

$$\boxed{[9]_{24} \quad \text{et} \quad [21]_{24}.}$$

V Lire des propriétés dans la décomposition

14

Fixons $N \geqslant 2$.

(a) Si (a,b) est inversible dans $A \times B$, il existe (c,d) tel que

$$(a,b)(c,d) = (ac, bd) = (1_A, 1_B).$$

Ainsi $ac = 1_A$ et $bd = 1_B$: a et b sont inversibles. Réciproquement, si a^{-1} et b^{-1} existent, alors

$$(a,b)(a^{-1}, b^{-1}) = (1_A, 1_B),$$

donc (a,b) est inversible, d'inverse (a^{-1}, b^{-1}).

(b) Supposons $\mathrm{PGCD}(m,n) = 1$. D'après la question 12, $\Phi_{m,n}$ est un isomorphisme. Si x est inversible dans $\mathbb{Z}/mn\mathbb{Z}$, avec inverse y, alors

$$\Phi_{m,n}(x)\,\Phi_{m,n}(y) = \Phi_{m,n}(xy) = \Phi_{m,n}(1) = (1,1),$$

donc $\Phi_{m,n}(x)$ est inversible dans le produit. Réciproquement, si $\Phi_{m,n}(x)$ est inversible, son inverse possède un unique antécédent y par la bijectivité de $\Phi_{m,n}$; alors

$$\Phi_{m,n}(xy) = \Phi_{m,n}(x)\Phi_{m,n}(y) = (1,1) = \Phi_{m,n}(1).$$

L'injectivité de $\Phi_{m,n}$ donne $xy = 1$, donc x est inversible.

La question 14(a) identifie les unités du produit aux couples d'unités. La restriction de $\Phi_{m,n}$ donne donc une bijection compatible avec la multiplication

$$(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times.$$

En prenant les cardinaux,

$$\boxed{\varphi(mn) = \varphi(m)\varphi(n).}$$

(c) Dans $\mathbb{Z}/p^\alpha\mathbb{Z}$, les classes non inversibles sont exactement celles représentées par un multiple de p. Parmi $0, 1, \ldots, p^\alpha - 1$, il y en a $p^{\alpha-1}$. Ainsi

$$\boxed{\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.}$$

(d) Si $N = \prod_{i=1}^r p_i^{\alpha_i}$ est sa décomposition en facteurs premiers, les facteurs $p_i^{\alpha_i}$ sont deux à deux premiers entre eux. Par multiplicativité,

$$\varphi(N) = \prod_{i=1}^r \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) = N \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

Donc

$$\boxed{\varphi(N) = N \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).}$$

15

(a) Le cas de deux facteurs est la question 12. Si le résultat est établi pour $r-1$ facteurs, alors $n_1 \cdots n_{r-1}$ est premier avec n_r, et le théorème des restes chinois donne

$$\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z} \simeq \mathbb{Z}/(n_1 \cdots n_{r-1})\mathbb{Z} \times \mathbb{Z}/n_r\mathbb{Z}.$$

Par l'hypothèse de récurrence,

$$\mathbb{Z}/(n_1 \cdots n_{r-1})\mathbb{Z} \simeq \prod_{i=1}^{r-1} \mathbb{Z}/n_i\mathbb{Z}.$$

En remplaçant le premier facteur par ce produit dans l'isomorphisme précédent, on obtient

$$\mathbb{Z}/(n_1 \cdots n_r)\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}.$$

(b) Soit $e = [a]_{p^\alpha}$ idempotent. L'égalité $e^2 = e$ s'écrit

$$e(e-1) = 0.$$

Si $p \nmid a$, alors $\mathrm{PGCD}(a, p^\alpha) = 1$; la question 7 montre que e est inversible. En multipliant $e(e-1) = 0$ par e^{-1}, on obtient $e - 1 = 0$, donc $e = 1$.

Si $p \mid a$, alors $p \nmid a - 1$, donc $\mathrm{PGCD}(a-1, p^\alpha) = 1$ et $e - 1$ est inversible. En multipliant cette fois $e(e-1) = 0$ par $(e-1)^{-1}$, on obtient $e = 0$. Les seuls idempotents sont donc 0 et 1.

(c) Dans la décomposition

$$\mathbb{Z}/N\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z},$$

un élément est idempotent si et seulement si chaque composante l'est. Chacune offre deux choix, 0 ou 1. Il y a donc

$$\boxed{2^r}$$

idempotents.

(d) Comme $60 = 4 \times 3 \times 5$,

$$\mathbb{Z}/60\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}.$$

Cherchons les trois idempotents qui sélectionnent une seule coordonnée. On vérifie directement

$$\begin{aligned} &45 \equiv 1 \pmod 4, \quad 45 \equiv 0 \pmod 3, \quad 45 \equiv 0 \pmod 5,\\ &40 \equiv 0 \pmod 4, \quad 40 \equiv 1 \pmod 3, \quad 40 \equiv 0 \pmod 5,\\ &36 \equiv 0 \pmod 4, \quad 36 \equiv 0 \pmod 3, \quad 36 \equiv 1 \pmod 5. \end{aligned}$$

Les classes $[45]_{60}$, $[40]_{60}$ et $[36]_{60}$ correspondent donc respectivement à $(1,0,0)$, $(0,1,0)$ et $(0,0,1)$.

Dans le produit, un idempotent est un triplet dont chaque coordonnée vaut 0 ou 1. Il s'obtient donc en additionnant une sous-famille de ces trois sélecteurs. Les huit sommes, réduites modulo 60, sont

$$\boxed{0, 1, 16, 21, 25, 36, 40, 45 \pmod{60}.}$$

16

(a) Écrivons

$$P(X) = a_0 + a_1 X + \cdots + a_r X^r, \qquad a_0, \ldots, a_r \in \mathbb{Z}.$$

Soit $x \in \mathbb{Z}/mn\mathbb{Z}$ et supposons

$$\Phi_{m,n}(x) = (x_m, x_n).$$

Dans $\mathbb{Z}/mn\mathbb{Z}$, la définition donnée dans l'énoncé s'écrit

$$P(x) = [a_0]_{mn} + [a_1]_{mn} x + \cdots + [a_r]_{mn} x^r.$$

Comme $\Phi_{m,n}$ est un morphisme d'anneaux, il préserve les sommes et les produits. Par récurrence sur k,

$$\Phi_{m,n}(x^k) = \Phi_{m,n}(x)^k = (x_m^k, x_n^k).$$

De plus, pour tout entier a, la classe de a dans $\mathbb{Z}/mn\mathbb{Z}$ est envoyée sur $([a]_m, [a]_n)$. Par conséquent

$$\begin{aligned} \Phi_{m,n}(P(x)) &= \Phi_{m,n}([a_0]_{mn} + [a_1]_{mn} x + \cdots + [a_r]_{mn} x^r)\\ &= ([a_0]_m, [a_0]_n) + ([a_1]_m, [a_1]_n)(x_m, x_n) + \cdots\\ &\qquad + ([a_r]_m, [a_r]_n)(x_m^r, x_n^r)\\ &= \left(\sum_{k=0}^{r} [a_k]_m x_m^k,\ \sum_{k=0}^{r} [a_k]_n x_n^k \right)\\ &= (P(x_m), P(x_n)). \end{aligned}$$

Ainsi

$$\boxed{\Phi_{m,n}(P(x)) = (P(x_m), P(x_n)).}$$

Supposons maintenant $\mathrm{PGCD}(m,n) = 1$. Comme $\Phi_{m,n}$ est alors bijective,

$$P(x) = 0 \iff \Phi_{m,n}(P(x)) = (0,0) \iff P(x_m) = 0 \text{ et } P(x_n) = 0.$$

À toute racine x modulo mn correspond donc un couple de racines (x_m, x_n). Réciproquement, tout couple de racines possède, par le théorème des restes chinois, un unique antécédent x modulo mn, et l'égalité précédente impose alors $P(x) = 0$. On obtient bien une bijection entre les deux ensembles de racines.

(b) Posons $N = n_1 \cdots n_r$ et considérons

$$\Psi : \mathbb{Z}/N\mathbb{Z} \longrightarrow \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}, \qquad \Psi([x]_N) = ([x]_{n_1}, \ldots, [x]_{n_r}).$$

La question 15(a) affirme que Ψ est un isomorphisme lorsque les n_i sont deux à deux premiers entre eux. Le même calcul qu'en (a), effectué composante par composante, donne

$$\Psi(P(x)) = (P(x_1), \ldots, P(x_r))$$

dès que $\Psi(x) = (x_1, \ldots, x_r)$. Par bijectivité de Ψ,

$$P(x) = 0 \iff P(x_i) = 0 \quad \text{pour tout } i \in \{1, \ldots, r\}.$$

Ainsi

$$\boxed{\{x \in \mathbb{Z}/N\mathbb{Z} : P(x) = 0\} \simeq \prod_{i=1}^{r} \{x_i \in \mathbb{Z}/n_i\mathbb{Z} : P(x_i) = 0\}.}$$

(c) Comme $105 = 3 \times 5 \times 7$, la question (b) permet de résoudre séparément l'équation modulo 3, 5 et 7. Dans chacun des trois corps $\mathbb{Z}/p\mathbb{Z}$,

$$x^2 = 1 \iff x^2 - 1 = 0 \iff (x-1)(x+1) = 0.$$

Un corps n'ayant pas de diviseur de zéro, on obtient nécessairement $x = 1$ ou $x = -1$. Il y a donc $2 \times 2 \times 2 = 8$ triplets de solutions, donc huit solutions modulo 105.

Pour reconstruire explicitement ces huit classes, cherchons les sélecteurs des trois coordonnées. On vérifie

$$\begin{aligned} &70 \equiv 1 \pmod 3, \quad 70 \equiv 0 \pmod 5, \quad 70 \equiv 0 \pmod 7, \\ &21 \equiv 0 \pmod 3, \quad 21 \equiv 1 \pmod 5, \quad 21 \equiv 0 \pmod 7, \\ &15 \equiv 0 \pmod 3, \quad 15 \equiv 0 \pmod 5, \quad 15 \equiv 1 \pmod 7. \end{aligned}$$

Ainsi le triplet $(\varepsilon_3, \varepsilon_5, \varepsilon_7)$, avec chaque $\varepsilon_p \in \{-1, 1\}$, correspond à la classe

$$x \equiv 70\varepsilon_3 + 21\varepsilon_5 + 15\varepsilon_7 \pmod{105}.$$

En évaluant les huit choix de signes puis en réduisant modulo 105, on obtient

$$\boxed{x \equiv 1, 29, 34, 41, 64, 71, 76, 104 \pmod{105}.}$$

La décomposition fournie par le théorème des restes chinois ne sert pas seulement à résoudre simultanément plusieurs congruences : elle transporte les opérations et donc les équations polynomiales vers un produit d'anneaux plus simples. Lorsque les facteurs sont premiers, ces anneaux sont des corps $\mathbb{Z}/p\mathbb{Z}$, ce qui ouvre naturellement l'étude des phénomènes polynomiaux propres à la caractéristique p.