L'anneau $\mathbf{Z}$

Solution de l'exercice (??)

On note $a_n = 2^n + 3^n$ et soit $\delta := a_n \wedge a_{n+1}$ le pgcd de a_n et a_{n+1}. On a alors $\delta = a_n \wedge (a_{n+1} - 2a_n) = a_n \wedge 3^n = (a_n - 3^n) \wedge 3^n = 2^n \wedge 3^n = 1$.

Solution de l'exercice (??)

On rappelle que les sous-groupes de $\mathbf{Z}$ sont de la forme $n\mathbf{Z}$; l'inclusion $48\mathbf{Z} \subset n\mathbf{Z}$ se traduit par n divise 48 soit $n = 1, 2, 3, 4, 6, 8, 12, 16, 18, 24, 48$ avec les inclusions :

$$\begin{array}{ccccccccc}
(16) & \subset & (8) & \subset & (4) & \subset & (2) & \subset & (1) = \mathbf{Z} \\
\cup & & \cup & & \cup & & \cup & & \cup \\
(48) & \subset & (24) & \subset & (12) & \subset & (6) & \subset & (3)
\end{array}$$

Solution de l'exercice (??)

(a) Tout nombre divisant ac et b est premier avec a par hypothèse et donc divise c par le lemme de Gauss. Les diviseurs communs à ac et b sont donc les mêmes que ceux communs à c et b.
(b) On décompose a en facteurs premiers :

$$a = \prod_{p \in \mathcal{P}} p^{\nu_p(a)}$$

où $\mathcal{P}$ est l'ensemble des nombres premiers et où la famille $\nu_p(a)$ est nulle sauf pour un nombre fini de nombres premiers. On introduit de même les multiplicités $\nu_p(b)$ et $\nu_p(c)$. On a alors

$$(ab) \wedge c = \prod_{p \in \mathcal{P}} p^{\nu_p}$$

avec $\nu_p := \min(\nu_p(a) + \nu_p(b), \nu_p(c))$. L'hypothèse $a \wedge b = 1$ s'interprète par $\nu_p(a)\nu_p(b) = 0$, *i.e.* $\nu_p(a)$ et $\nu_p(b)$ ne sont jamais tous deux non nuls. On en déduit alors que $\nu_p = \min(\nu_p(a), \nu_p(c)) + \min(\nu_p(b), \nu_p(c))$ soit donc $(ab) \wedge c = (a \wedge b)(b \wedge c)$.

Dans le cas où l'on ne suppose plus $a \wedge b = 1$, la deuxième égalité est fausse comme le montre le cas $a = b = c = 2$: $4 \wedge 2 \neq (2 \wedge 2)(2 \wedge 2)$. En ce qui concerne la première égalité, on peut choisir $a = b = 2$ et $c = 3$ ce qui donne $6 \wedge 2 \neq 3 \wedge 2$.

Solution de l'exercice (??)

(a) D'après l'exercice précédent (**??**), on a $(a \wedge 6) = (a \wedge 2)(a \wedge 3)$ pour tout entier $a > 0$. On calcule alors $(n^2 + 2n - 2) \wedge 2 = n^2 \wedge 2 = n \wedge 2$. De même on a $n^2 + 2n - 2 \equiv 0 \mod 3$ si et seulement si $n \equiv 2 \mod 3$ (il suffit de tester $n = 0, 1, 2$ modulo 3). Ainsi le pgcd en question est égal ± 1 (resp. 2, resp. 3, resp. 6) si et seulement si $n \equiv 1 \mod 2$ et $n \not\equiv 2 \mod 3$ (resp. $n \equiv 0 \mod 2$ et $n \not\equiv 2 \mod 3$, resp. $n \equiv 1 \mod 2$ et $n \equiv 2 \mod 3$, resp. $n \equiv 0 \mod 2$ et $n \equiv 2 \mod 3$) soit $n \equiv 1, 3 \mod 5$ (resp. $n \equiv 0, 4 \mod 6$, resp. $n \equiv 5 \mod 6$, resp. $n \equiv 2 \mod 6$).
(b) Le but est de faire des combinaisons pour faire descendre le degré en utilisant des égalités du genre $a \wedge b = (a - b) \wedge b$. Concrètement appelons $\delta(n)$ ce pgcd. On a $n^3 + n^2 + 1 = (n^2 + 2n - 1)(n - 1) - (n + 1)$ de sorte que $\delta(n) = (n^2 + 2n - 1) \wedge (n + 1)$. De même $n^2 + 2n - 1 = (n + 1)^2 - 2$ et donc $\delta(n) = (n + 1) \wedge 2$ soit $\delta(n) = 2$ si $n \equiv 1 \mod 2$ et $(n) = 1$ si $n \equiv 0 \mod 2$.

Solution de l'exercice (??)

On suppose a et b positifs et on décompose a et b en facteurs premiers :

$$a = \prod_{p \in \mathcal{P}} p^{\nu_p(a)} \qquad b = \prod_{p \in \mathcal{P}} p^{\nu_p(b)}$$

où $\mathcal{P}$ est l'ensemble des nombres premiers > 0 et où les familles d'entiers $(\nu_p(a))_{p \in \mathcal{P}}$ et $(\nu_p(b))_{p \in \mathcal{P}}$ sont nulles sauf pour un ensemble fini de nombres premiers. Soit alors $u \in \mathbf{N}$ tel que $ab = u^k$. On écrit de même $u = \prod_{p \in \mathcal{P}} p^{\nu_p(u)}$ avec pour tout $p \in \mathcal{P}$

$$\nu_p(a) + \nu_p(b) = k\nu_p(u).$$

L'hypothèse a et b premiers entre eux signifie que pour tout $p \in \mathcal{P}$, $\nu_p(a)$ et $\nu_p(b)$ ne sont pas tous deux non nuls. On en déduit donc que pour tout $p \in \mathcal{P}$, $\nu_p(a)$ et $\nu_p(b)$ sont divisibles par k : $\nu_p(a) = ka_p$ et $\nu_p(b) = kb_p$ avec à nouveau a_p et b_p non tous deux non nuls. En posant $\alpha = \prod_{p \in \mathcal{P}} p^{a_p}$ et $\beta = \prod_{p \in \mathcal{P}} p^{b_p}$, on en déduit $a = \alpha^k$ et $b = \beta^k$.

Solution de l'exercice (??)

(a) On remarque tout d'abord que $650 = 2 \times 325$ et $66 = 2 \times 33$. On va appliquer l'algorithme d'Euclide à 325 et 33 puis on multipliera par deux.

$$\begin{aligned}
325 &= 33 \times 9 + 28 \\
33 &= 28 + 5 \\
28 &= 5 \times 5 + 3 \\
5 &= 3 + 2 \\
3 &= 2 + 1
\end{aligned}$$

On remonte alors les calculs :

$$\begin{aligned}1 &= 3-2\\ 1 &= 3-(5-3) = 23-5\\ 1 &= 2(28-5\times 5)-5 = 2\times 28 - 11\times 5\\ 1 &= 2\times 28 - 11(33-28) = 13\times 28 - 11\times 33\\ 1 &= 13(325-9\times 33) - 11\times 33 = 13\times 325 - 128\times 33\end{aligned}$$

Finalement la relation de Bézout est $2 = 13 \times 650 - 128 \times 66$ et c'est la plus "simple" ; on rappelle que les autres sont données par :

$$2 = (13 + k \times 66)650 - (128 - k \times 650)66$$

pour $k \in \mathbf{Z}$.
(b) (i) Les sommes qui peuvent être payées sont celles qui s'écrivent sous la forme $ua + vb$. Si on utilise le rendu de monnaie, u ou v peuvent être négatifs de sorte que dans ce cas l'ensemble des sommes payables est le groupe engendré par a et b soit d'après Bezout le groupe engendré par $a \wedge b$ qui est donc égal à $\mathbf{Z}$.

(ii) Dans le cas où l'on n'autorise pas le rendu de monnaie, on impose à u et v d'être positifs. On écrit alors $x = au + bv$ de manière unique en imposant $0 \leq u \leq b-1$; si en effet on écrit $x = au + bv$, toute autre écriture est de la forme $x = a(u - bt) + b(v + at)$. Si donc $x > ab - a - b$ et $0 \leq u \leq b-1$, on a $bv = x - au > ab - a - b - a(b-1) = -b$, soit $v > -1$ et donc $v \geq 0$.

(iii) On écrit $48x+20y+15z = 3(16x+5z)+20y$. D'après ce qui précède tout nombre de la forme $60+t$ avec $t \geq 0$ peut s'écrire sous la forme $16x+5z$ avec $x \geq 0$, $z \geq 0$. De même tout nombre de la forme $38+s$ avec $s \geq 0$ peut s'écrire sous la forme $3t + 20y$ avec $t \geq 0$, $y \geq 0$. Finalement toute somme supérieure ou égale à $218 = 3 \times 60 + 38$ est payable.

L'anneau $\mathbf{Z}/n\mathbf{Z}$, congruences

Solution de l'exercice (??)

L'ordre de 2 dans $(\mathbf{Z}/7\mathbf{Z})^*$ est 3 comme on le constate immédiatement. Si n est pair, on a $2^n \equiv 1 \bmod 3$ et donc $2^{2^n} \equiv 2 \bmod 7$; si n est impair, $2^n \equiv 2 \bmod 3$ et donc $2^{2^n} \equiv 4 \bmod 7$. Le même raisonnement pour 4 (aussi d'ordre 3 dans $(\mathbf{Z}/7\mathbf{Z})^*$) donne $2^{2^n} \equiv 4 \bmod 7$ si n est pair et $2^{2^n} \equiv 2 \bmod 7$ si n est impair, d'où le résultat.

Solution de l'exercice (??) Lorsqu'il n'y a pas d'ambiguïté possible, on note de la même manière un nombre entier et sa classe modulo n.
On rappelle que les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont indexés par les diviseurs d de n ; concrètement l'application $d|n \mapsto (\frac{n}{d})$ qui à un diviseur d de n associe le sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ engendré par $\frac{n}{d}$ est une bijection. Pour $n = 24$, les sous-groupes sont ceux engendrés par les classes de $1, 2, 3, 4, 6, 8, 12, 0$ avec les relations d'inclusion :

$$\begin{array}{ccccccc} (8) & \subset & (4) & \subset & (2) & \subset & (1) \\ \cup & & \cup & & \cup & & \cup \\ (0) & \subset & (12) & \subset & (6) & \subset & (3) \end{array}$$

En outre on rappelle que le groupe engendré par k dans $\mathbf{Z}/n\mathbf{Z}$ est le même que celui engendré par $k \wedge n$ (remarque **??**). On a ainsi $(16) = (8)$ et $(18) = (6)$.

Solution de l'exercice (??)

D'après le théorème chinois, il suffit de donner la congruence de $a = 2005^{2005}$ modulo 2 et 7. On a d'abord de manière immédiate $a \equiv 1 \mod 2$. D'autre part, on a $2005 \equiv 0 \mod 7$ et donc $a \equiv 0 \mod 7$. On en déduit alors que $a \equiv 7 \mod 14$, par exemple parceque $a = 7\alpha$ avec α impair.

Solution de l'exercice (??)

Comme précédemment on cherche la congruence de $a = 10^{100}$ modulo 13 et 19. On a $10 \equiv -3 \mod 13$ et d'après le petit théorème de Fermat (cf. (**??**)) on a $(-3)^{12} \equiv 1 \mod 13$. Comme $100 \equiv 4 \mod 12$, on obtient $a \equiv (-3)^4 \mod 13$ soit $a \equiv 3 \mod 13$.

De la même façon, on a $10 \equiv -9 \mod 19$ avec $(-9)^{18} \equiv 1 \mod 19$. Comme $100 \equiv 10 \mod 18$, on obtient $a \equiv (-9)^{10} \mod 18$. Or on a $9^2 \equiv 5 \mod 19$, $9^4 \equiv 5^2 \equiv 6 \mod 19$ et $9^8 \equiv 6^2 \equiv -2 \mod 19$ et donc $9^{10} = 9^2 9^8 \equiv -10 \mod 19$.

On a alors $a \equiv -10 \mod 13$ et $a \equiv -10 \mod 19$ soit $a \equiv -10 \mod 247$. De manière générale on rappelle que pour trouver la congruence de a modulo 247 , on cherche une relation de Bézout. Pour cela on effectue l'algorithme d'Euclide, soit $19 - 13 = 6$ et $13 - 2.6 = 1$ ce qui donne $1 = 13 - 2(19 - 13) = 3.13 - 2.19$. On a alors $a \equiv 9.3.13 - 3.2.19 \mod 247$ soit $a \equiv 237 \mod 247$ (*cf.* l'exemple **??**).

Solution de l'exercice (??)

On a $1035125 \equiv 12 \mod 17$. D'après le petit théorème de Fermat on a $12^{16} \equiv 1 \mod 17$. Or $5642 \equiv 10 \mod 16$ de sorte que $1035125^{5642} \equiv 12^{10}$

mod 17. Or $12 \equiv -5 \mod 17$ et $12^2 \equiv 8 \mod 17$ soit $12^4 \equiv -4$ soit $12^8 \equiv -1$ de sorte que l'ordre de $12^{10} = 12^2 12^8 = -12^2 = -8 = 9 \mod 17$.

Solution de l'exercice (??)

On a $1823 \equiv 5 \mod 18$; or $5 \in (\mathbf{Z}/18\mathbf{Z})^*$; on peut donc utiliser le petit théorème de Fermat avec $\varphi(18) = \varphi(2)\varphi(9) = 1.6 = 6$ soit $5^6 \equiv 1 \mod 18$. Or on a $242 \equiv 2 \mod 6$ soit $1823^{242} \equiv 5^2 \equiv 7 \mod 18$.

De même $2222 \equiv 2 \mod 20$ avec $2 \notin (\mathbf{Z}/20\mathbf{Z})^*$; on ne peut donc pas utiliser le petit théorème de Fermat (2^8 est pair et ne peut donc pas être congru à 1 modulo 20). On utilise l'isomorphisme du lemme chinois : on a $2222 \equiv 2 \mod 4$ de sorte que $2222^n \equiv 0 \mod 4$ dès que $n \geq 2$. On a aussi $2222 \equiv 2 \mod 5$ et $321 \equiv 1 \mod 4$ et donc d'après le petit théorème de Fermat $2222^{321} \equiv 2 \mod 5$ d'où $2222^{321} \equiv 5 \times 0 - 4 \times 2 \equiv 12 \mod 20$.

Solution de l'exercice (??)

On a $42 = 2 \times 3 \times 7$, il suffit alors de vérifier la congruence modulo 2, 3 et 7 (corollaire **??**). Pour 2 et 3, on a clairement $n^7 \equiv n$ et pour 7 le résultat découle du petit théorème de Fermat.

Solution de l'exercice (??)

On rappelle que 700 n'étant pas premier, 429 est inversible dans $\mathbf{Z}/700\mathbf{Z}$ si et seulement s'il est premier avec 700 et son inverse est donné par la relation de Bézout, *i.e.* si $1 = 700a + 429b$ alors l'inverse cherché est la classe de b. Il suffit donc d'appliquer l'algorithme d'Euclide :

$$\begin{aligned}
700 &= 429 + 271 \\
429 &= 271 + 158 \\
271 &= 158 + 113 \\
158 &= 113 + 45 \\
113 &= 2 \times 45 + 23 \\
45 &= 23 + 22 \\
23 &= 22 + 1
\end{aligned}$$

On remonte alors les calculs et on obtient la relation de Bézout : $1 = 19 \times 700 - 31 \times 429$ de sorte que l'inverse de 429 dans $\mathbf{Z}/700\mathbf{Z}$ est $\overline{-31} = \overline{669}$.

Solution de l'exercice (??)

(i) 3 étant premier avec 7, il est inversible dans $\mathbf{Z}/7\mathbf{Z}$; on calcule rapidement que $3 \times 5 \equiv 1 \mod 7$, *i.e.* $5 = 1/3$ dans $\mathbf{Z}/7\mathbf{Z}$ de sorte que l'équation s'écrit $x \equiv 20 \mod 7$ soit $x \equiv 6 \mod 7$;

(ii) d'après le corollaire **??** il suffit de vérifier l'équation modulo 3 et 7. L'équation s'écrit $0.x \equiv 0 \mod 3$ et est donc toujours vérifiée. D'autre part l'équation s'écrit $2x \equiv -2 \mod 7$; l'inverse de 2 dans $\mathbf{Z}/7\mathbf{Z}$ est -3, soit donc $x \equiv 6 \mod 7$. Le résultat final est donc $x \equiv 6 \mod 7$;

(iii) on calcule rapidement $676 = 2^2 \times 13^2$; par le théorème chinois (cf. le corollaire **??**) on est donc ramené à résoudre $-x \equiv 0 \mod 4$ et $103x \equiv 105 \mod 169$. L'algorithme d'Euclide fournit $64 \times 103 - 39 \times 169 = 1$ soit donc $x \equiv 64 \times 105 \mod 69$ soit $x \equiv -40 \mod 169$ et donc $x \equiv -40 \mod 676$.

Solution de l'exercice (??)

(a) On commence par regarder la congruence de a^4 modulo 16. On remarque tout d'abord que si a est pair, celle-ci est nulle. Ensuite si a est impair, sa classe modulo $16 = 2^4$ appartient à $(\mathbf{Z}/16\mathbf{Z})^*$ qui est de cardinal $\varphi(2^4) = 4$ de sorte que $a^4 \equiv 1 \mod 16$. On en déduit alors que si a et b sont premiers entre eux et donc ne sont pas tous deux pairs, $a^4 + b^4 \equiv 1, 2 \mod 16$.

(b) Si p divisait a, il diviserait $b^4 = n - a^4$ et donc diviserait b ce qui n'est pas car a et b sont premiers entre eux. On en déduit donc que les classes de a et b dans $\mathbf{Z}/p\mathbf{Z}$ en sont des éléments inversibles.

(c) $\mathbf{Z}/p\mathbf{Z}$ éant un corps, on écrit alors $(\frac{\bar{a}}{\bar{b}})^4 = -1$ dans $\mathbf{Z}/p\mathbf{Z}$. On en déduit donc que $\frac{\bar{a}}{\bar{b}}$ est d'ordre 8 puisque $(\frac{\bar{a}}{\bar{b}})^8 = 1$ et $(\frac{\bar{a}}{\bar{b}})^4 \neq 1$.

(d) Le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est d'ordre $p-1$ et contient un élément d'ordre 8 de sorte que, d'après le théorème de Lagrange, 8 divise $p-1$, soit $p \equiv 1 \mod 8$.

Solution de l'exercice (??)

Si p est premier, le résultat découle du fait que p divise le coefficient binomial $\binom{p}{i}$, pour $0 < i < p$. En effet on a $p\binom{p-1}{i-1} = i\binom{p}{i}$ de sorte que p divise $i\binom{p}{i}$ et comme $p \wedge i = 1$, on en déduit que p divise $\binom{p}{i}$.

Réciproquement supposons p non premier ; soit alors q un facteur premier de $p = q^k m$ avec $q \wedge m = 1$ et $k \geq 1$. On a alors $\binom{p}{q} = q^{k-1}\tilde{m}$ avec $q \wedge \tilde{m} = 1$ et donc q^k ne divise pas $\binom{p}{q}$, de sorte que le coefficient de X^q de $(X-a)^p$, qui est égal à $\binom{p}{q}a^{p-q}$ est non nul modulo p.

Solution de l'exercice (??)

On rappelle que p étant premier, $(\mathbf{Z}/p\mathbf{Z}, +, \times)$ est un corps. Dans $\mathbf{Z}/p\mathbf{Z}$, on a $\bar{a}^2 + \bar{b}^2 = 0$ soit $(\frac{\bar{a}}{\bar{b}})^2 = -1$, car $\bar{b} \neq 0$. Ainsi -1 est un carré dans $\mathbf{Z}/p\mathbf{Z}$: $-1 = x^2$, soit $x^4 = 1$. Le groupe $(\mathbf{Z}/p\mathbf{Z})^*$ est donc un groupe d'ordre $p-1$ qui contient un élément d'ordre 4 de sorte que, d'après le théorème de Lagrange, 4 divise $p-1$.

Solution de l'exercice (??)

(a) D'après le lemme chinois, on a $(\mathbf{Z}/pq\mathbf{Z})^* \simeq (\mathbf{Z}/p\mathbf{Z})^* \times (\mathbf{Z}/q\mathbf{Z})^*$ de sorte que ce dernier est de cardinal $(p-1)(q-1)$. Les éléments x égaux à leur inverse sont ceux qui vérifient $x^2 = 1$, *i.e.* ceux d'ordre divisant 2, ce qui donne 4 éléments, à savoir $(\pm 1, \pm 1)$ soient les classes dans $\mathbf{Z}/pq\mathbf{Z}$ de $1, -1, x_1, x_2$ avec $x_i \equiv (-1)^i \mod p$ et $x_i \equiv (-1)^{i-1} \mod q$, pour $i = 1, 2$.

(b) On considère alors le produit de tous les éléments de $(\mathbf{Z}/pq\mathbf{Z})^*$ *i.e.* le produit des $pq-1$ premiers entiers auxquels il faut enlever tous les multiples de p ainsi que tous les multiples de q. Les multiples de p (resp. q) sont $p, 2p, \cdots, (q-1)p$ (resp. $q, 2q, \cdots, (p-1)q$), de sorte que le produit en question vaut $\frac{(pq-1)!}{(q-1)!p^{q-1}(p-1)!q^{p-1}}$ (modulo pq). Par ailleurs en regroupant les classes distinctes de $1, -1, x_1, x_2$ avec leur inverse ce produit est égal à $a = 1(-1)x_1x_2 = -x_1x_2$. On a donc $a \equiv 1 \mod p$ et $a \equiv 1 \mod q$ de sorte que $a \equiv 1 \mod pq$ (lemme chinois), d'où le résultat.

Morphismes

Solution de l'exercice (??)

(a) On a $\phi(k) = k\phi(1)$ de sorte que ϕ est déterminé par $\phi(1)$. En outre on doit avoir $\phi(a.1) = \phi(0) = 0 = a\phi(1)$ et donc l'ordre de $\phi(1)$ divise a. Réciproquement, si l'ordre de $x \in \mathbf{Z}/b\mathbf{Z}$ divise a, le morphisme $\psi : \mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ tel que $\psi(1) = x$ se factorise par le morphisme canonique $\pi : \mathbf{Z} \to \mathbf{Z}/a\mathbf{Z}$ (proposition **??**) pour donner un diagramme commutatif :

$$\begin{tikzcd} \mathbf{Z} \arrow[d, "\pi"'] \arrow[dr, "\psi"] & \\ \mathbf{Z}/a\mathbf{Z} \arrow[r, "\bar{\psi}"] & \mathbf{Z}/b\mathbf{Z} \end{tikzcd}$$

On pose alors $\phi = \bar{\psi}$.

(b) Si a et b sont premiers entre eux, soit $\phi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$ un morphisme de groupes. L'élément $\phi(1)$ est d'ordre divisant a et b, donc $\phi(1)$ est d'ordre 1 et $\phi(1) = 0$. On obtient alors que ϕ est le morphisme nul. Pour la réciproque, on raisonne par contraposée. Supposons que a et b ne soient pas premiers entre eux et soit ψ le morphisme de $\mathbf{Z}$ dans $\mathbf{Z}/b\mathbf{Z}$ tel que $\psi(1) = b/a \wedge b \bmod b$ et donc $\psi(1) \neq 0 \bmod b$. On a alors $\psi(a) = 0$ (car $\frac{ab}{a \wedge b}$ est divisible par b) et le morphisme ψ se factorise par un morphisme non nul $\phi : \mathbf{Z}/a\mathbf{Z} \to \mathbf{Z}/b\mathbf{Z}$.

Solution de l'exercice (??)

Dans le premier cas comme 3 et 4 sont premiers entre eux, les seuls éléments d'ordre divisant 3 dans $\mathbf{Z}/4\mathbf{Z}$ sont le seul d'ordre 1 à savoir 0 de sorte que tout morphisme $\mathbf{Z}/3\mathbf{Z} \to \mathbf{Z}/4\mathbf{Z}$ est nul.

Dans $\mathbf{Z}/15\mathbf{Z}$ les éléments d'ordre divisant 12 sont donc d'ordre divisant $12 \wedge 15 = 3$ et sont donc $0, 5, 10$, ce qui donne 3 morphismes distincts (dont le morphisme nul).

Solution de l'exercice (??)

(a) D'après l'exercice (**??**), la condition nécessaire et suffisante est que p divise n.

(b) D'après l'exercice (**??**), il faut et il suffit que x soit d'ordre divisant p^a. On rappelle (cf. remarque **??**) que l'ordre de x est égal à $\frac{p^b}{\alpha \wedge p^b}$. Ainsi pour $a \geq b$, tout élément α convient tandis que pour $a \leq b$, il faut et il suffit que $\alpha \wedge p^b$ soit divisible par p^{b-a}.

(c) Le nombre de morphismes distincts est donc, d'après ce qui précède, égal au nombre d'éléments d'ordre divisant p^a dans $\mathbf{Z}/p^b\mathbf{Z}$ qui est donc d'après l'exercice (**??**) égal à p^a si $a \leq b$ (et à p^b si $a \geq b$).

Solution de l'exercice (??) On note $n \vee m$ le PPCM de n et m.
On a évidemment $n \vee m \subset \ker \pi$. Réciproquement, soit $k \in \ker \pi :$ k est alors divisible par n et m donc par $n \vee m$ (par définition du PPCM). On a donc $\ker \pi = (n \vee m)$. Soient maintenant a, b tels que $b - a$ soit divisible par $n \wedge m$. On écrit une relation de Bézout $un + vm = n \wedge m$ et on pose $k = u\frac{n}{(n \wedge m)}b + v\frac{m}{(n \wedge m)}a$. On a alors $k = un\frac{(b-a)}{n \wedge m} + a \equiv a \mod n$; de même on a $k = vm\frac{(a-b)}{n \wedge m} + b \equiv b \mod m$, de sorte que (a, b) est dans l'image de π. Pour la réciproque, si $(\bar{a}, \bar{b}) = \pi(k)$, on a $k = a + \lambda n = b + \mu m$ soit $(b - a) = \lambda n - \mu m$ qui est donc divisible par $n \wedge m$. En particulier lorsque n et m sont premiers entre eux, π induit un isomorphisme $\mathbf{Z}/nm\mathbf{Z} \simeq \mathbf{Z}/n\mathbf{Z} \times \mathbf{Z}/m\mathbf{Z}$ et on retrouve le lemme chinois.

Si $k \equiv 3 \mod 6$, on applique ce qui précède avec $n = 6, m = 10$. On a alors $k \equiv a \mod 10$ avec $a - 3$ divisible par $2 = 6 \wedge 10$, soit $a = 1, 3, 5, 7, 9$.

Problèmes

Solution du problème (??)

(a) Si q divise $a^m - 1$, on a $a^m \equiv 1 \mod q$, d'où $a^{mp^{r-1}} \equiv 1 \mod q$ et donc q divise $a^{\frac{n-1}{p}} - 1$ et n ce qui contredit l'hypothèse.

(b) On a $a^{n-1} \equiv 1 \mod n$ par hypothèse, donc à fortiori $a^{n-1} \equiv 1 \mod q$, soit $(a^m)^{p^r} \equiv 1 \mod q$. On en déduit que la classe b de a^m est inversible dans $\mathbf{Z}/q\mathbf{Z}$ et que son ordre (multiplicatif) divise p^r. Ce dernier est donc de la forme p^k avec $0 \leq k \leq r$. Si on avait $k < r$, on aurait aussi $b^{p^{r-1}} = 1$ dans $\mathbf{Z}/q\mathbf{Z}$ ce qui impliquerait que q divise $a^{\frac{n-1}{p}} - 1$ ce qui n'est pas. Ainsi b est d'ordre p^r.

(c) Le groupe $(\mathbf{Z}/q\mathbf{Z})^*$ qui est d'ordre $q-1$ contient un élément d'ordre p^r ce qui impose, d'après le théorème de Lagrange, que p^r divise $q-1$ soit $q \equiv 1 \mod p^r$.

(d) Soit q premier divisant n. Pour p premier divisant u, on écrit u (resp. v) sous la forme $p^r m$ (resp. $p^s m'$) avec p ne divisant pas m (resp. m'). D'après ce qui précède, $q \equiv 1 \mod p^{r+s}$ et donc $q \equiv 1 \mod p^r$. La propriété étant vérifiée pour tout diviseur premier p de u, on en déduit par application du lemme chinois que $q \equiv 1 \mod u$.

(e) Les facteurs premiers de n sont tous de la forme $1 + \alpha u$. Si n n'éait pas premier, il posséderait au moins deux facteurs de la forme précédente et serait donc supérieur ou égal à $(1+u)^2 > 1 + u + 2u = 1 + uv$ d'où la contradiction et donc n est premier.

Solution du problème (??)

1. (i) implique (ii) : Supposons $n = p_1. \cdots .p_s$ les p_i étant distincts deux à deux. Le théorème chinois donne alors $\mathbf{Z}/n\mathbf{Z} \simeq \mathbf{Z}/p_1\mathbf{Z} \times \cdots \times \mathbf{Z}/p_s\mathbf{Z}$ et la congruence $a^n \equiv a \mod n$ est équivalente à $a^n \equiv a \mod p_i$ pour tout i (corollaire **??**). Pour i fixé, si p_i divise a le résultat est clair, sinon la congruence est équivalente à $a^{n-1} \equiv 1 \mod p_i$ (lemme de Gauss). Le petit théorème de Fermat donne alors $a^{p_i-1} \equiv 1 \mod p_i$ soit $a^{n-1} \equiv 1 \mod p_i$ puisque $p_i - 1$ divise $n-1$ par hypothèse.

(ii) implique (iii) : si a et n sont premiers entre eux l'implication est évidente car a est inversible dans $\mathbf{Z}/n\mathbf{Z}$.

(iii) implique (i) : Commençons par montrer que n est sans facteur carré ; supposons par l'absurde que $n = p^r q$ avec $r > 1$, p premier et q non divisible par p. Pour a non divisible par p, on a $a^{n-1} \equiv 1 \mod p^r$. On choisit alors un élément a de $(\mathbf{Z}/p^r\mathbf{Z})^*$ d'ordre p (c'est possible car $r > 1$). On en déduit alors que p divise $p^r q - 1$ ce qui n'est pas. Montrons ensuite la deuxième propriété ; soit p premier divisant n et soit a tel que sa classe modulo p engendre $(\mathbf{Z}/p\mathbf{Z})^*$. La congruence $a^n \equiv a \mod n$ implique $a^n \equiv a \mod p$ soit $a^{n-1} \equiv 1 \mod p$ et donc $p-1$ divise $n-1$ car $p-1$ est l'ordre de a.

2. L'implication $(i) \Rightarrow (ii)$ se prouve exactement comme dans (1), en utilisant que dans $\mathbf{Z}/p\mathbf{Z}$, $x^{p-1} = 1$ de sorte que si $p-1$ divise $(n-1)/2$ alors $x^{(n-1)/2} = 1$. Pour la réciproque, on raisonne comme dans 1. Supposons que $n = p^r q$ avec $r \geq 2$ et soit a un élément de $(\mathbf{Z}/p^r\mathbf{Z})^*$ d'ordre p. L'égalité $a^{(n-1)/2} \equiv 1 \mod p^r$, impliquerait alors que $2p$ diviserait $p^r q - 1$ ce qui n'est

pas. Ainsi n est sans facteur carré. Soit alors p divisant n et a un générateur de $(\mathbf{Z}/p\mathbf{Z})^*$ de sorte que l'égalité $a^{(n-1)/2} \equiv 1 \mod p$ implique que $p-1$ divise $(n-1)/2$, d'où le résultat.

(3) Si $p = 6m+1$ (resp. $p = 12m+1$, resp. $p = 18m+1$), $n \equiv 1 \mod 6m$ (resp. $n \equiv (1+6m)^2 \equiv 1 \mod 12m$, resp. $n \equiv (1+12m)(1-12m) \equiv 1$ mod $18m$).

Par ailleurs $p-1$ divise $\frac{n-1}{2}$ si et seulement si $2(p-1)$ divise $n-1$. Ainsi pour m impair, si $n-1$ est divisible par 8, étant divisible par $12m$ et $18m$ d'après ce qui précède, on en déduit qu'il sera divisible par $8 \vee (12m) = 24m$ et par $(18m) \vee 8 = 36m$ ($a \vee b$ désigne le PPCM des nombres a et b). Or on a $n \equiv (1-2m)(4m+1)(1+2m) \equiv (1-4m^2)(1+4m) \equiv (1-4m)(1+4m) \equiv 1$ mod 8, d'où le résultat.

Solution du problème (??)

(a) Pour $n > 0$, on a la factorisation

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

car -1 est racine de ce polynôme. On écrit m sous la forme $2^n k$ avec k impair. Si $k > 1$, on a alors l'égalité

$$2^m + 1 = (2^{2^n})^k + 1 = (2^{2^n} + 1)((2^{2^n})^{k-1} - \cdots + 1)$$

On obtient alors un diviseur propre $2^{2^n} + 1$ d'o˘ la contradiction, soit $k = 1$ et m est une puissance de 2.

(b) On trouve $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ et l'on vérifie aisément qu'ils sont tous premiers.

(c) Soit p premier divisant F_5, on a alors $2^{2^5} = -1$ dans $\mathbf{Z}/p\mathbf{Z}$ et 2 est d'ordre (multiplicatif) 2^6 dans $(\mathbf{Z}/p\mathbf{Z})^*$. D'après le petit théorème de Fermat, on a $2^{p-1} \equiv 1 \mod p$ et donc $2^6 = 64$ divise $p-1$, d'où le résultat.

(d) On vérifie que 641 est premier. Dans le corps $\mathbf{Z}/641\mathbf{Z}$, on a $0 = 641 = 1 + 5.2^7$ soit $2^7 = -1/5$. Ainsi $F_5 = 2^{32} + 1 = (2^7)^4.2^4 + 1$ car $32 = 7.4 + 4$. D'où dans $\mathbf{Z}/641\mathbf{Z}$, on a $F_5 = (-1/5)^4.2^4 + 1 = (2^4 + 5^4)/5^4 = 0$.

(e) Supposons $n = m+r$ avec $r > 0$. On a $2^{2^n} = (2^{2^m})^{2^r}$ et dans $\mathbf{Z}/F_m\mathbf{Z}$, on a alors $F_n \equiv (-1)^{2^r} + 1 \mod F_m$. Ainsi le pgcd de F_m et de F_n divise 2 ; or 2 ne divise pas F_n d'où le résultat.

L'ensemble $\mathcal{P}$ des nombres premiers positifs contient la réunion disjointe $\coprod_n \mathcal{F}_n$ où $\mathcal{F}_n$ est le sous-ensemble de $\mathcal{P}$ des diviseurs premiers divisant F_n ; $\mathcal{F}_n$ étant non vide pour tout n car $F_n > 1$, on en déduit que $\mathcal{P}$ est infini.

Solution du problème (??)

(a) Soit I un idéal de A et soit $b \neq 0 \in I$ tel que $v(b)$ soit minimal. Pour $i \in I$, on effectue une division euclidienne de i par b: $i = bq + r$ avec $v(r) < v(b)$ et $r \in I$; d'après la minimalité de $v(b)$, on en déduit $r = 0$ et donc $I = (b)$.

(b) (i) L'application N est clairement multiplicative ; si $z \in A^*$, on a $zz' = 1$ et donc $N(z)N(z') = 1$ soit $N(z) = 1$ et finalement $z = \pm 1, \pm i$. L'égalité $N((a+ib)(c+id)) = N(a+ib)N(c+id)$ donne l'identité remarquable de Lagrange.

(ii) Soit z_1 et z_2 des éléments de A ; on écrit $z_1/z_2 = q + e$ avec $q \in A$ et $e \in \mathbf{C}$ de module strictement plus petit que 1. On a alors $z_1 = qz_2 + r$ avec $r = z_2 e = z_1 - qz_2 \in A$ et $N(r) < N(z_2)$. Le choix de q n'est pas unique en général comme on peut le voir sur la figure.

On calcule alors $\frac{5+6i}{3-2i} = \frac{3+28i}{13}$; on pose donc $5 + 6i = (3 - 2i)(2i) + 1$. Le pgcd est donc égal à 1 et une relation de Bézout est $(5 + 6i) - 2i(3 - 2i) = 1$.

(iii) Le fait que S est une stable par multiplications découle directement de l'identité de Lagrange.

(iv) On rappelle que p est irréductible si et seulement si $A/(p)$ est intègre ; or $A/(p) \simeq \mathbf{Z}/p\mathbf{Z}[X]/(X^2 + 1)$ qui est intègre si et seulement si $X^2 + 1$ n'a pas de racines dans $\mathbf{Z}/p\mathbf{Z}$, soit si et seulement si (-1) n'est pas un carré modulo p et donc si et seulement si $p \equiv 3 \mod 4$.
En outre $n \in S$ si et seulement s'il existe $z \in A$ tel que $n = N(z)$ de sorte que si $p \in S$, on a $p = z\bar{z}$ avec $N(z) = p$ avec $zet\bar{z}$ non inversibles, et donc p non irréductible. Réciproquement si p n'est pas irréductible, on a $p = zz'$ avec $z' = \bar{z}$ et donc $p = N(z) \in S$.

(v) Soit p premier congru à 3 modulo 4 alors p est irréductible dans A. De même si $z = a + ib$ est tel que $N(z)$ soit premier, z est irréductible car $z = xy$ implique $N(x)N(y)$ premier soit $N(x)$ ou $N(y)$ égal à 1, *i.e.* x ou y inversible.
Montrons qu'aux inversibles près, ce sont les seuls ; soit z irréductible et p premier divisant $N(z)$. Si $p \equiv 3 \mod 4$, alors p est irréductible et $p|z\bar{z}$ et donc $p|z$ et $p|\bar{z}$, d'où $z = pu$ avec u inversible. Si $p = 2$ ou $p \equiv 1 \mod 4$, on a $p = a^2 + b^2$ et donc $a + ib$ irréductible et divise p donc z, et $z = u(a + ib)$ avec u inversible, d'où le résultat.

(vi) Soit $n \geq 2$ et supposons que pour tout $p \equiv 3 \mod 4$, $v_p(n)$ soit pair. Pour montrer que $n \in S$, il suffit de montrer que pour tout p, $p^{v_p(n)} \in S$. Le résultat est clair pour $p \equiv 3 \mod 4$ car $v_p(n)$ est pair (le carré d'un nombre entier quelconque appartient à S) ; pour $p = 2$ et $p \equiv 1 \mod 4$, on a $p \in S$ et donc $p^{v_p(n)} \in S$.
Montrons maintenant par récurrence sur $n \geq 2$, l'implication réciproque : le cas $n = 2$ est trivial et pour $n \geq 3$, $n = a^2 + b^2$. Si p est un nombre premier

diviseur de n tel que $p \equiv 3 \mod 4$, alors p divise $(a+ib)(a-ib)$; or p est irréductible dans A de sorte que p divise $a+ib$ et $a-ib$, soit p divise a et b ; ainsi $n = p^2((a/p)^2 + (b/p)^2)$ et $n/p^2 \in S$. Par hypothèse de récurrence $v_p(n/p^2)$ est pair et donc $v_p(n)$ aussi.

bigskip

Solution du problème (??)

(i) L'application N est bien sur multiplicative, *i.e.* $N(zz') = N(z)N(z')$, à valeurs dans $\mathbf{N}$. Si z est inversible, on en déduit qu'il existe z' tel que $zz' = 1$ soit $N(z)N(z') = 1$ ce qui impose $N(z) = 1$. Réciproquement si on a $N(z) = z\bar{z} = 1$ alors $\bar{z}$ est l'inverse de z.

Soit alors z tel que $N(z)$ soit premier ; soit $z_1z_2 = z$ avec z_1 non inversible, il s'agit alors de montrer que z_2 l'est. On a donc $N(z) = N(z_1)N(z_2)$ et donc $N(z_2) = 1$ et $z_2 \in A^*$.

(ii) On va montrer que si z est tel que $N(z) = 9$ alors z est irréductible de sorte que 3, $2 \pm i\sqrt{5}$ sont tous irréductibles, et l'égalité $3 \times 3 = (2+i\sqrt{5})(2-i\sqrt{5})$ correspond à deux factorisations distinctes en produit d'irréductibles. Soit donc $z \in \mathbf{Z}[i\sqrt{5}]$ tel que $N(z) = 9$; on écrit $z = z_1z_2$ avec $N(z_1) \neq 1$. On a donc $N(z) = 9 = N(z_1)N(z_2)$; or les factorisations de 9 dans $\mathbf{Z}$, sont 3×3 et 9×1. On remarque que $N(a + ib\sqrt{5}) = a^2 + 5b^2 = 3$ est impossible, de sorte $N(z_2) = 1$ *i.e.* z_2 inversible.

(ii) De la même façon, si $N(z) = 4$ ou 6, alors z est irréductible de sorte que $2 \times 3 = (1+i\sqrt{5})(1-i\sqrt{5})$ est un autre contre-exemple à l'unicité de la décomposition en produit d'irréductibles. En particulier 2 est irréductible et divise $6 = ab$ et 2 ne divise ni a, ni b. Soit δ un éventuel pgcd de $2a$ et ab ; on a 2 et a qui divisent δ, de sorte que $N(\delta)$ est un multiple de 4 et de 6 et donc un multiple de 12. De la même façon comme d divise 6 et $2a$, on en déduit que $N(\delta)$ divise 36 et 24 et donc leur pgcd qui est 12. Ainsi on obtiendrait $N(\delta) = 12 = a^2 + 5b^2$ qui n'a pas de solutions, d'où la contradiction.