Sorbonne Université
Année universitaire 2023-2024, master 1, *Théorie des nombres 1.* Corrigé de certains exercices de la feuille de TD numéro 1.

Exercice 1

Question (a). Dans l'anneau principal $\mathbb{Z}$, l'idéal $a\mathbb{Z}\cap b\mathbb{Z}$ admet un générateur m (uniquement déterminé à un inversible près, c'est-à-dire ici au signe près). Si x est un élément de $\mathbb{Z}$ on a donc par définition

$$m|x \iff (a|x \text{ et } b|x),$$

ce qui fait de m le PPCM de a et b, par définition du PPCM dans un anneau intègre général.

Remarque. Ce fait s'étend en fait sans aucune difficulté à une famille quelconque d'entiers, même infinie : si $(a_i)_{i\in I}$ est une famille d'entiers, et si m désigne un générateur de $\bigcap_i a_i\mathbb{Z}$, alors m est un PPCM de $(a_i)_{i\in I}$: les multiples de m sont exactement les multiples de tous les a_i. Exemple à méditer : si on prend pour (a_i) la famille de tous les nombres premiers, son PPCM est.... 0, qui est le seul entier qui soit multiple de tous les nombres premiers. C'est une petite bizarrerie de 0 : pour l'ordre usuel, c'est le plus petit élément de $\mathbb{N}$, mais pour la divisibilité c'est le plus grand ! On retrouve ce genre de blague à propos du cardinal de $\mathbb{Z}/n\mathbb{Z}$, qui vaut n sauf quand n est nul, car $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$ est infini.

Question (b). Commençons par traiter le cas où m et n sont strictement positifs. Soit d leur PGCD. Il est alors $\geqslant 1$, et > 1 s'ils ne sont pas premiers entre eux. Plaçons-nous dans ce cas. Écrivons $m = \mu d$ et $n = \nu d$. On a $\mu < m$ et $\nu < n$, et $\mu\nu d = m\nu = n\mu$ est un multiple commun strictement positif de m et n, qui est strictement inférieur à mn (exercice : montrez que c'est précisément le PPCM de m et n). C'est donc un élément non nul modulo nm, mais nul modulo n et m ; sa classe modulo mn est en conséquence un élément non trivial du noyau de $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, qui n'est dès lors pas injectif, et n'est *a fortiori* pas un isomorphisme.

Plaçons-nous maintenant dans le cas où m ou n est nul ; quitte à les échanger, supposons $n = 0$. Le PGCD de m et n vaut alors m. Supposons que m et n ne sont pas premiers, c'est-à-dire que $m \neq 1$.

On a alors $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/nm\mathbb{Z} \simeq \mathbb{Z}$, et le morphisme canonique de $\mathbb{Z}/nm\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ s'identifie au morphisme $x \mapsto (x, \overline{x})$ de $\mathbb{Z}$ vers $\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Or comme $m \neq 1$, l'élément $\overline{1}$ de $\mathbb{Z}/m\mathbb{Z}$ n'est pas nul, si bien que l'élément $(0, \overline{1})$ n'est pas de la forme $(x, \overline{x})$. Par conséquent $\mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ n'est pas surjectif, et n'est *a fortiori* pas un isomorphisme.

Question (c). Soient r et s deux éléments de $\mathbb{Q}^\times$ tels que $\mathrm{ord}_p(r) < \mathrm{ord}_p(s)$. Posons $n = \mathrm{ord}_p(r)$ et $m = \mathrm{ord}_p(s)$. Écrivons

$$r = p^n \frac{a}{b} \text{ et } s = p^m \frac{c}{d},$$

où a, b, c sont des entiers relatifs premiers à p. On a alors

$$r + s = p^n \frac{a}{b} + p^m \frac{c}{d} = p^n \left(\frac{a}{b} + p^{m-n} \frac{c}{d} =\right) = p^n \left(\frac{ad + p^{m-n}bc}{bd}\right).$$

Comme a et b sont premiers à p et comme $m > n$ par hypothèse , la somme $ad + p^{m-n}bc$ est première à p. Et comme b et d sont premiers à p, le produit bd est encore premiers à p. Il vient

$$\mathrm{ord}_p(r+s) = \mathrm{ord}_p\left(p^n \cdot \frac{\overbrace{ad + p^{m-n}bc}^{\text{premier à } p}}{\underbrace{bd}_{\text{premier à } p}}\right) = n = \mathrm{ord}_p(r) = \min(\mathrm{ord}_p(r), \mathrm{ord}_p(s)).$$

Question (d). Soit $(r_1, \ldots, r_n)$ une famille finie d'éléments de $\mathbb{Q}^\times$. Soit G le sous-groupe de $\mathbb{Q}^\times$ engendré par les r_i. Nous allons montrer que $G \neq \mathbb{Q}^\times$, ce qui prouvera que ce dernier n'est pas de type fini. Soit $\mathscr{P}$ l'ensemble des nombres premiers intervenant dans la décomposition des r_i (en produits de puissances entières relatives de nombres premiers).

Tout élément de G est de la forme $\prod r_i^{n_i}$ où les n_i appartiennent à $\mathbb{Z}$. Par conséquent, la décomposition d'un élément de G en produits de puissances entières relatives de nombres premiers ne fait intervenir que des éléments de $\mathscr{P}$. Choisissons un nombre premier p n'appartenant pas à $\mathscr{P}$ (ce qui est possible car il y a une infinité de nombres premiers) ; par ce qui précède, $p \notin G$.

Exercice 2

L'idée est la suivante : puisqu'on cherche à fabriquer des contre-exemples à quelques lemmes dans un groupe non abélien, nous allons tenter notre chance avec le premier groupe non abélien, à savoir $\mathfrak{S}_3$. Ce dernier a six éléments : l'identité qui est d'ordre 1, les trois transpositions $(12), (23)$ et (13) qui sont d'ordre 2, et les deux 3-cycles (123) et (132) qui sont d'ordre 3.

Premier contre-exemple. Les éléments (12) et (123) sont d'ordres finis premiers entre eux (à savoir 2 et 3). Mais l'ordre de leur produit $(12)(123)$ ne peut pas être égale à $2 \cdot 3 = 6$ car il n'y a pas d'élément d'ordre 6 dans S_3. (On peut faire le calcul si on le souhaite : $(12)(123) = (23)$, qui est d'ordre 2).

Second contre-exemple. Le PPCM des ordres des éléments de $\{(12), (123)\}$ est 6 et $\mathfrak{S}_3$ n'a pas d'éléments d'ordre 6.

Troisième contre-exemple. Le maximum des ordres des éléments de $\mathfrak{S}_3$ est 3, mais $(12)^3 = (12) \neq \mathrm{Id}$.

Exercice 3

Question (a). On a $97 - 1 = 96 = 32 \cdot 3 = 2^5 \cdot 3$. On cherche à construire un élément de $\mathbb{Z}/97\mathbb{Z})^\times$ d'ordre 96. On va pour ce faire exhiber un élément x d'ordre 3 et un élément y d'ordre 32 ; comme 3 et 32 sont premiers entre eux (et comme on travaille dans un groupe abélien), on n'aura plus qu'à poser $z = xy$. Dans ce qui suit, les calculs sont implicitement modulo 97, et pour alléger les notations nous ne mettrons pas de «barres de modulo»

Si a est un élément quelconque de $(\mathbb{Z}/97\mathbb{Z})^\times$ on a $a^{96} = 1$ et donc $(a^{32})^3 = 1$; ainsi, si a^{32} n'est pas lui-même égal à 1, il est forcément d'ordre 3. Tentons notre chance avec $a = 2$. Pour faciliter les calculs, on remarque que $100 = 3$ modulo 97.

On a alors modulo 97 :

- $2^2 = 4$;
- $2^4 = 4^2 = 16$;
- $2^8 = 16^2 = 256 = 200 + 56 = 2 \cdot 3 + 56 = 62 = -35$;
- $2^16 = (-35)^2 = 900 + 300 + 25 = 12 \cdot 3 + 25 = 61 = -36$;
- $2^32 = (-36)^2 = 900 + 360 + 36 = 1296 = 12 \cdot 3 - 1 = 35$.

Puisque $35 \neq 1$ (modulo 97, toujours), $x := 35 = 2^{32}$ est d'ordre 3 dans $(\mathbb{Z}/96\mathbb{Z})^\times$.

Si a est un élément quelconque de $(\mathbb{Z}/97\mathbb{Z})^\times$ on a $a^{96} = 1$ et donc $(a^3)^{32} = 1$; ainsi, a^3 est d'ordre divisant $32 = 2^5$, donc de la forme 2^n avec $n \leqslant 5$; si $(a^3)^{16} \neq 1$ alors 2^n ne divise pas 2^4, ce qui veut dire que $n = 5$ et que (a^3) est d'ordre 2^{32}.

À nouveau, tentons notre chance avec $a = 2$. On a alors $a^3 = 8$, puis :

- $8^2 = 64 = -33$;
- $8^4 = (-33)^2 = 900 + 180 + 9 = 1089 = 10 \cdot 3 - 8 = 22$;
- $8^8 = 22^2 = 400 + 80 + 4 = 4 \cdot 3 - 13 = -1$;
- $8^{16} = (-1)^2 = 1$.

C'est donc un échec. Rejouons avec $a = 3$. O a $a^3 = 27$, puis :

- $27^2 = 400 + 280 + 49 = 729 = 7 \cdot 3 + 29 = 50$;
- $27^4 = 50^2 = 2500 = 25 \cdot 3 = 75 = -22$.
- $27^8 = (-22)^2 = 484 = 4 \cdot 3 - 13 = (-1)$;
- $27^{16} = (-1)^2 = 1$.

C'est donc encore un échec. Il est inutile de faire l'essai avec 4 : on a vu que $(2^3)^{16} = 2^{48} = 1$, ce sera *a fortiori* le cas de $(4^3)^{16} = 4^{48} = (2^{48})^2$. Retentons notre chance avec $a = 5$. On a $a^3 = 125 = 3 + 25 = 28$, puis :

- $28^2 = 400 + 320 + 64 = 784 = 7 \cdot 3 - 13 = 8$.
- On peut directement écrire, pour exploiter les calculs précédents : $(28)^{16} = 8^8 = (-1) \neq 1$.

Par conséquent $y = 5^3 = 28$ est bien d'ordre 32, et

$$xy = 35 \cdot 28 = 700 + 240 + 40 = 980 = 970 + 10 = 10$$

est donc un générateur de $(\mathbb{Z}/97\mathbb{Z})^\times$.

Question (b). Pour montrer que 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$, il faut s'assurer que son ordre multiplicatif est $p - 1 = 4\ell$. On raisonne par l'absurde. On suppose donc que l'ordre de 2 est un diviseur strict de 4ℓ. Comme ℓ est premier, ceci implique que l'ordre de 2 divise 4 ou 2ℓ, donc que $2^4 = 1$ ou que $2^{2\ell} = 1$. Nous allons montrer que chacune de ces deux hypothèses conduit à une contradiction.

Supposons tout d'abord que $2^4 = 1$. On travaille modulo p, donc cela signifie que p divise $2^4 - 1 = 15$. En conséquence $p = 3$ ou 5 mais aucun de ces deux nombres premiers ne s'écrit $4\ell + 1$ avec ℓ premier (on a $5 = 4 \cdot 1 + 1$ mais 1 n'est pas premier !).

Supposons maintenant que $2^{2\ell} = 1$. Cela peut se récrire $2^{(p-1)/2} = 1$ et signifie donc exactement que le symbole de Legendre $\left(\frac{2}{p}\right)$ est égal à 1, c'est-à-dire que 2 est un carré modulo p. Mais d'après le cours cela équivaut à demander que p vaille 1 ou (-1) modulo 8. Or $p - 1 = 4\ell$ qui est non nul modulo 8 car le nombre premier ℓ est impair (si on avait $\ell = 2$ on aurait $p = 9$ ce qui est absurde) ; et $p + 1 = 4\ell + 2 = 2(2\ell + 1)$ qui n'est pas non plus multiple de 8. On aboutit ainsi encore à une contradiction.

Exercice 4

Question (a). Nous allons montrer successivement les deux égalités. Commençons par la première. Pour tout j, posons

$$N_j = \left\lfloor \frac{n}{p^j} \right\rfloor ;$$

on peut également caractériser N_j comme le nombre d'entiers entre 1 et n multiples de p^j, c'est-à-dire encore le nombre d'entiers entre 1 et n dont la valuation p-adique vaut au moins j.

Le but est de montrer que $\mathrm{ord}_p(n!) = \sum_{j=0}^{+\infty} N_j$. Pour cela il va être commode d'introduire pour tout entier m la fonction $\mathbf{1}_{\leqslant m}$ de $\mathbf{N}$ dans lui-même qui vaut 1 sur les entiers $\leqslant m$ et 0 ailleurs (autrement dit c'est l'indicatrice de $\{0, \ldots, m\}$).

On a alors

$$\begin{aligned}
\mathrm{ord}_p(n!) &= \mathrm{ord}_p\left(\prod_{i=1}^{n} i\right) \\
&= \sum_{i=1}^{n} \mathrm{ord}_p(i) \\
&= \sum_{i=1}^{n} \sum_{j=1}^{\mathrm{ord}_p(i)} 1 \\
&= \sum_{i=1}^{n} \sum_{j=1}^{+\infty} \mathbf{1}_{\leqslant \mathrm{ord}_p(i)}(j) \\
&= \sum_{j=1}^{+\infty} \sum_{i=1}^{n} \mathbf{1}_{\leqslant \mathrm{ord}_p(i)}(j) \\
&= \sum_{j=1}^{+\infty} \#\{i, 1 \leqslant i \leqslant n, \mathrm{ord}_p(i) \geqslant j\} \\
&= \sum_{j=1}^{+\infty} N_j .
\end{aligned}$$

(Le symbole # désigne le cardinal).

Montrons maintenant la seconde égalité. Celle-ci ne fera pas intervenir le fait que p est premier, ce qui suit étant valable pour tout entier $p \geqslant 2$ (il faut que la notion même de développement en base p ait un sens). On écrit $n = \sum_{i=0}^{r} a_i p^i$ (dans cet exercice, lorsqu'on considèrera ce type d'écriture, il sera sous-entendu que c'est le développement en base p et donc que les a_i sont des entiers compris entre 0 et $p-1$). Pour tout $j \geqslant 1$ la partie entière $\left\lfloor \frac{n}{p^j} \right\rfloor$ est alors égale à $\sum_{j \leqslant i \leqslant r} a_i p^{i-j}$ si $j \leqslant r$, et à 0 sinon. On a alors

$$\begin{aligned}
\sum_{j \geqslant 1} \left\lfloor \frac{n}{p^j} \right\rfloor &= \sum_{1 \leqslant j} \sum_{j \leqslant i \leqslant r} a_i p^{i-j} \\
&= \sum_{i \leqslant r} \sum_{1 \leqslant j \leqslant i} a_i p^{i-j}
\end{aligned}$$

$$
\begin{aligned}
&= \sum_{0\leqslant i\leqslant r} a_i \sum_{1\leqslant j\leqslant i} p^{i-j} \\
&= \sum_{0\leqslant i\leqslant r} a_i \frac{p^i-1}{p-1} \\
&= \frac{\sum_{0\leqslant i\leqslant r} a_i p^i - \sum_{0\leqslant i\leqslant r} a_i}{p-1} \\
&= \frac{n - \sum_{0\leqslant i\leqslant r} a_i}{p-1}.
\end{aligned}
$$

(Concernant la quatrième égalité, notez que dans le cas extrême $i = 0$ la somme $\sum_{1\leqslant j\leqslant i} p^{i-j}$ est la somme vide et est donc nulle, et que $\frac{p^i-1}{p-1}$ est également nul.)

Remarque. Ce calcul montre en particulier que $n - \sum a_i$ est multiple de $p-1$, mais c'était évident *a priori* : comme $p = 1$ modulo $p-1$, on a $n = \sum a_i p^i = \sum a_i$ modulo $p-1$. Notez qu'on a aussi $n = \sum a_i p^i = \sum a_i(-1)^i$ modulo $p+1$. En faisant $p = 10$ on retrouve ainsi les critères classiques (ou qui devraient l'être) de divisibilité par 9 et 11.

Question (b). On a

$$\binom{2n}{n} = \frac{(2n!)}{(n!)^2}.$$

Comme $p \leqslant 2n$, il divise $(2n)!$. Et comme $p > n$, il ne divise pas $n!$ ni $(n!)^2$. Par conséquent p divise $\binom{2n}{n}$.

Question (d). On écrit $a = \sum_{i=0}^r a_i p^i$, $b = \sum_{i=0}^r b_i p^i$ et $a_i + b_i = \sum_{i=0}^{r+1} c_i p^i$ (on choisit un même entier r convenant à a et b, si bien qu'on ne suppose pas que a_r et b_r sont non nuls). La valuation p-adique de $\binom{a+b}{a} = \frac{(a+b)!}{a!b!}$ est égale à $\mathrm{ord}_p((a+b)!) - \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$ c'est-dire, en vertu de la question précédente, à

$$\frac{(a+b) - \sum_i c_i - a + \sum_i a_i - b + \sum_i b_i}{p-1} = \frac{\sum_i (a_i+b_i)) \sum_i c_i}{p-1}.$$

Il s'agit donc démontrer que $\frac{\sum_i (a_i+b_i) - \sum_i c_i}{p-1}$ est le nombre de retenues dans le calcul de $a+b$ en base p. On procède par réurrence sur r.

Initialisation. On traite le cas $r = 0$. On a alors $a = a_0$ et $b = b_0$. On distingue deux cas.

- ⋄ Supposons $a_0 + b_0 < p$. Il n'y a alors pas de retenue, on a $c_0 = a_0 + b_0$ et $c_1 = 0$, si bien que $\frac{(a_0+b_0-c_0)}{(p-1)} = 0$, ce qui est l'égalité cherchée.
- ⋄ Supposons que $a_0 + b_0 \geqslant p$. Il y a alors une retenue, on a $c_0 = a_0 + b_0 - p$ et $c_1 = 1$, si bien que $\frac{(a_0+b_0-c_0-c_1)}{(p-1)} = 1$, ce qui est l'égalité cherchée.

Le passage de $r-1$ à r. On suppose $r \geqslant 1$ et le résultat vrai au rang $r-1$. Posons $\alpha = \sum_{i=0}^{r-1} a_i p^i$ et $\beta = \sum_{i=0}^{r-1} a_i p^i$. Posons $\gamma = \alpha + \beta$ et écrivons $\gamma = \sum_{i=0}^r d_i p^i$ (notons que $d_r = 0$ si le dernier cran du calcul de $\alpha + \beta$ ne donne pas lieu à une retenue, et 1 sinon.) Notons k le nombre de retenues dans le calcul de $\alpha + \beta$, et ℓ le nombre de retenues dans le calcul de $a + b$. L'hypothèse de récurrence assure que

$$k = \frac{\sum_{i=0}^{r-1}(a_i+b_i) - \sum_{i=0}^r d_i}{p-1}.$$

Par l'algorithme de l'addition on a $c = \sum_{i=0}^{r+1} c_i p^i$ où $c_i = d_i$ pour tout $i \leqslant r-1$, et où l'on est dans l'un des deux cas suivants :

(1) $a_r + b_r + c_r < p$; on a alors $c_r = a_r + b_r + d_r$ et $c_{r+1} = 0$;

(2) $a_r + b_r + c_r \geqslant p$; on a alors $c_r = a_r + b_r + d_r - p$ et $c_{r+1} = 1$.

L'expression

$$\frac{\sum_{i=0}^{r}(a_i + b_i) - \sum_{i=0}^{r+1} c_i}{p-1}$$

peut se récrire

$$\frac{\sum_{i=0}^{r}(a_i + b_i) - c_{r+1} - c_r - \sum_{i=0}^{r-1} c_i}{p-1},$$

c'est-à-dire encore

$$\frac{\sum_{i=0}^{r}(a_i + b_i) - c_{r+1} - c_r - \sum_{i=0}^{r-1} d_i}{p-1}$$

(car $c_i = d_i$ pour tout $i \leqslant r-1$). Ceci est égal à

$$\frac{a_r + b_r - c_{r+1} - c_r + d_r + \sum_{i=0}^{r-1}(a_i + b_i) - \sum_{i=0}^{r} d_i}{p-1},$$

c'est-à-dire finalement à

$$\frac{a_r + b_r - c_{r+1} - c_r + d_r}{p-1} + k$$

d'après l'expression de k donnée plus haut.

- ◇ Traitons d'abord le cas (1). C'est celui où la dernière étape du calcul de $a + b$ ne comporte pas de retenue, donc le cas où $\ell = k$. Et on a par ailleurs dans ce cas $c_{r+1} = 0$ et $c_r = a_r + b_r + d_r$, si bien que

$$\frac{a_r + b_r - c_{r+1} - c_r + d_r}{p-1} + k = k.$$

  On a donc

$$\frac{\sum_{i=0}^{r}(a_i + b_i) - \sum_{i=0}^{r+1} c_i}{p-1} = k = \ell,$$

  ce qui termine la preuve dans le cas (1).

- ◇ Traitons maintenant le cas (2). C'est celui où la dernière étape du calcul de $a + b$ comporte une retenue, donc le cas où $\ell = k + 1$. Et on a par ailleurs dans ce cas $c_{r+1} = 1$ et $c_r = a_r + b_r + d_r - p$, si bien que

$$\frac{a_r + b_r - c_{r+1} - c_r + d_r}{p-1} + k = 1 + k.$$

  On a donc

$$\frac{\sum_{i=0}^{r}(a_i + b_i) - \sum_{i=0}^{r+1} c_i}{p-1} = 1 + k = \ell,$$

  ce qui termine la preuve dans le cas (2).

Question (e). On a

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}.$$

Le nombre premier p divise $p!$, mais ne divise pas $i!$ ni $(p-i)!$ car i et $p-i$ sont tous deux strictement compris entre 0 et p. Par conséquent p divise $\binom{p}{i}$.

Soit A un anneau commutatif dans lequel p est nul (ce qui est un abus pour dire que $p \cdot 1_A = 0$). On a alors pour tout $(a, b) \in A^2$

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

car $\binom{p}{i} a^i b^{p-i} = 0$ pour tout i tel que $0 < i < p$ puisqu'on a vu que pour un tel i le coefficient binomial $\binom{p}{i}$ est multiple de p et donc nul dans A. Comme il est par ailleurs clair que $1^p = a$et $(ab)^p = a^p b^p$, l'élévation à la puissance p est un endomorphisme de A.

Une récurrence immédiate montre qu'on a pour tout entier $n \geqslant 0$ et tout n-uplet $(a_1, \ldots, a_n)$ d'éléments de A l'égalité $(a_1 + \ldots + a_n)^p = a_1^p + \ldots + a_n^p$. En l'appliquant avec $a_1 = a_2 = \ldots = a_n = 1$ on voit que $n^p = n$ dans A. C'est en particulier le cas lorsque $A = \mathbb{Z}/p\mathbb{Z}$. On a donc $n^p = n$ dans $\mathbb{Z}/p\mathbb{Z}$ pour tout entier $n \geqslant 0$, et en fait pour tout entier n car pour tout n dans $\mathbb{Z}$ il existe $m \geqslant 0$ tel que $n = m$ modulo p.

Exercice 5

Question (a). Tout nombre premier impair est égal à 1 ou à (-1) modulo 4. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers égaux à (-1) modulo 4, disons $p_1, \ldots, p_r$. Posons $N = 4p_1 p_2 \ldots p_r - 1$. Alors $N > 1$ et N vaut (-1) modulo 4. Si p est un diviseur de N il ne peut diviser $4p_1 \ldots p_r$, et n'est donc ni égal à 2 ni à l'un des p_i ; par conséquent il est égal à 1 modulo 4. En considérant l'écriture de N comme produit de nombres premiers on voit alors que $N = 1$ modulo 4, ce qui est absurde (notez que 1 et (-1) diffèrent modulo 4).

Question (b). Tout nombre premier est égal à $0, 1, (-1), 2$ ou (-2) modulo 5. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers égaux à (-1) modulo 5, disons $p_1, \ldots, p_r$. Posons $N = 5(p_1 p_2 \ldots p_r)^2 - 1$. Alors $N > 1$ et $N = (-1)$ modulo 5. Si p est un diviseur de N il ne peut diviser $5p_1 \ldots p_r$, et n'est donc ni égal à 5 ni à l'un des p_i ; par conséquent il est égal à 1, 2 ou (-2) modulo 5.

On a par ailleurs pour un tel p l'égalité $5(p_1 p_2 \ldots p_r)^2 - 1 = 0$ modulo p ; il vient

$$5 = \left(\frac{1}{p_1 \ldots, p_r}\right)^2$$

dans $\mathbb{Z}/p\mathbb{Z}$ (notez que comme p n'est pas égal à l'un des p_i, le produit $p_1 \ldots p_r$ est bien inversible dans $\mathbb{Z}/p\mathbb{Z}$). Par conséquent 5 est un carré modulo p. On a alors

$$\left(\frac{p}{5}\right) = (-1)^{\frac{(p-1)}{2} \cdot \frac{(5-1)}{2}} \left(\frac{5}{p}\right) = \left(\frac{5}{p}\right) = 1.$$

Ainsi p est un carré modulo 5. Par inspection directe, on voit que ceci force p à valoir 1 ou (-1) modulo 5. Comme on savait déjà que p vaut $1, 2$ ou (-2) modulo 5, la seule possibilité est que p vaille 1 modulo 5.

En considérant l'écriture de N comme produit de nombres premiers on voit alors que $N = 1$ modulo 5, ce qui est absurde (notez que 1 et (-1) diffèrent modulo 5).

Question (c). Tout nombre premier est égal à $2, 3$ 1 ou (-1) modulo 6. Supposons qu'il n'y ait qu'un nombre fini de nombres premiers égaux à (-1) modulo 6, disons $p_1, \ldots, p_r$. Posons $N = 6p_1p_2 \ldots p_r - 1$. Alors $N > 1$ et $N = (-1)$ modulo 6. Si p est un diviseur de N il ne peut diviser $6p_1 \ldots p_r$, et n'est donc ni égal à 2 ni à 3 ni à l'un des p_i ; par conséquent il est égal à 1 modulo 6. En considérant l'écriture de N comme produit de nombres premiers on voit alors que $N = 1$ modulo 6, ce qui est absurde (notez que 1 et (-1) diffèrent modulo 6).

Exercice 6

Question (a). Comme f est un polynôme non constant, $|f(n)|$ tend vers l'infini quand n tend vers l'infini. En particulier il existe N tel que $|f(N)| > 1$. Dans ce cas $f(N)$ possède un diviseur premier p. On a donc $f(\overline{N}) = \overline{0}$ dans $\mathbb{Z}/p\mathbb{Z}$, si bien que pour tout k on a encore $f(N + kp) = 0$ modulo p. Comme $|f(N+kp)|$ tend vers l'infini lorsque k tend vers l'infini, il existe k_0 tel que pour tout $k \geqslant k_0$ $|f(N + kp)| > p$. Mais alors dès que $k \geqslant n$ l'entier $|f(N + kp)|$ est divisible par p et strictement supérieur à p, donc n'est pas premier.

Question (b). *Remarque : pour que la question ait vraiment un intérêt, il faut préciser qu'on s'intéresse aux entiers* non nuls *de la forme $f(n)$, car si $f(n) = 0$ alors tout nombre premier divise $f(n)$.*

Écrivons $f = \sum_{0 \leqslant i \leqslant r} a_i T^i$, avec $r > 0$ et $a_r \neq 0$. Supposons tout d'abord que $a_0 = 0$. Dans ce cas T divise f et donc n divise $f(n)$ pour tout n. En particulier p divise $f(p)$ pour tout nombre premier p, et $f(p)$ est par ailleurs non nul dès que p est assez grand. Le résultat voulu est donc vrai dans ce cas.

Supposons maintenant que a_0 est non nul, et que les diviseurs premiers des entiers non nuls de la forme $f(n)$ appartiennent tous à un ensemble fini $\{p_1, \ldots, p_r\}$. Soit m le produit des p_i. Pour tout entier k on a

$$f(ka_0m) = \sum_{0 \leqslant i \leqslant r} a_i a_0^i k^i m^i = a_0(1 + \sum_{1 \leqslant i \leqslant r} a_0^{i-1} a_i k^i m^i).$$

L'expression $g(k) := 1 + \sum_{1 \leqslant i \leqslant r} a_0^{i-1} k^i a_i m^i$ est polynomiale de degré $r > 0$ en k et tend donc vers l'infini en valeur absolue avec k. En particulier il existe k tel que $|g(k)| > 1$ (on a alors $g(k) \neq 0$ si bien que $f(ka_0m) = a_0 g(k)$ est lui-même non nul). L'entier $g(k)$ possède alors un diviseur premier p. Celui-ci ne peut diviser m puisque $g(k) = 1$ modulo m, et p n'est donc pas l'un des p_i ; mais c'est par construction un diviseur de l'entier non nul $f(ka_0m) = a_0 g(k)$, ce qui est contradictoire.

Exercice 7

Question (a). Écrivons $f = \sum_{i=0}^{r} \lambda_i T^i$. Dans ce qui suit, les barres désignent les classes modulo $m - n$.

On a

$$\overline{\sum \lambda_i n^i} = \sum \overline{\lambda}_i \overline{n}^i = \sum \overline{\lambda}_i \overline{m}^i = \overline{\sum \lambda_i m^i}$$

(où la troisième égalité provient du fait que $\overline{n} = \overline{m}$ dans $\mathbb{Z}/(m-n)\mathbb{Z}$). Par conséquent $f(n)$ et $f(m)$ sont égaux modulo $n - m$, ce qu'il fallait démontrer.

Question (b). Si n est un entier relatif, n ou $(n-1)$ est pair si bien que $n(n-1)/2$ est entier. Le polynôme $f = T(T-1)/2 = T^2/2 - T/2$, qui est à coefficients rationnels, est donc tel que $f(n) \in \mathbb{Z}$ pour tout $n \in \mathbb{Z}$. Mais on a $f(0) = 0$ et $f(2) = 1$; par conséquent, $f(2) - f(0)$ n'est pas divisible par $2-0 = 2$, et la propriété prouvée au (a) pour les polynômes à coefficients entiers est donc ici prise en défaut ; elle est ainsi fausse en générale pour les polynômes à coefficients rationnels à valeurs entières sur $\mathbb{Z}$.

Question (c). On a pour tout entier n l'égalité

$$en! = \underbrace{\frac{n!}{0!} + \frac{n!}{1!} + \frac{n!}{2!} + \ldots + \frac{n!}{(n-1)!} + \frac{n!}{n!}}_{b_n} + \frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \ldots$$

Supposons $n \geqslant 1$. Pour montrer que $b_n = \lfloor en! \rfloor$, il suffit de montrer que le reste

$$r_n := \frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \ldots = \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \ldots = \sum_{i \geqslant 1} \frac{1}{(n+1)\ldots(n+i)}$$

est strictement inférieur à 1. Or on a

$$r_n = \sum_{i \geqslant 1} \frac{1}{(n+1)\ldots(n+i)} < \sum_{i \geqslant 1} \frac{1}{(n+1)^i} = \frac{1}{n+1} \cdot \frac{1}{1 - \frac{1}{n+1}} = \frac{1}{n} \leqslant 1.$$

Par conséquent $r_n < 1$, ce qu'on souhaitait établir.

Remarque. L'égalité $b_n = \lfloor en! \rfloor$ est fausse pour $n = 0$, car $b_0 = \frac{0!}{0!} = 1$ alors que $\lfloor e0! \rfloor = \lfloor e \rfloor = 2$.

(Question (d). On a pour tout $n \geqslant 1$ l'égalité $b_n = \lfloor en! \rfloor$, ce qui entraîne que $2n! \leqslant b_n \leqslant 3n!$. Des encadrements $2n! \leqslant b_n \leqslant 3n!$ et $2(n+1)! \leqslant b_{n+1} \leqslant 3(n+1)!$ on déduit alors que $\frac{b_{n+1}}{b_n} \geqslant \frac{2(n+1)!}{3n!} = \frac{2n}{3}$. En particulier b_{n+1}/b_n tend vers l'infini quand n tend vers l'infini, ce qui montre que b_n n'est pas un polynôme en n (si c'était le cas b_{n+1}/b_n tendrait vers 1).

(Question (e). Fixons $m > n \geqslant 0$. On a

$$b_m = \sum_{k=0}^{m} \frac{m!}{k!} = \sum_{k=m}^{0} \frac{m!}{k!} = \sum_{k=m}^{m-n} \frac{m!}{k!} + \sum_{k=m-n-1}^{0} \frac{m!}{k!}.$$

Le premier terme du membre de droite s'écrit

$$1 + m + m(m-1) + \ldots + m(m-1)\ldots(m-n+1)$$

et le second

$$m(m-1)\dots(m-n+1)(m-n)+m(m-1)\dots(m-n+1)(m-n)(m-n-1)+\dots+m!,$$

et l'on observe qu'il est somme de termes tous multiples de $(m-n)$ et est donc lui-même multiple de $m-n$.

On a par ailleurs $b_n = \sum_{k=0}^{n} \frac{n!}{k!} = \sum_{k=n}^{0} \frac{n!}{k!}$, soit encore

$$b_n = 1 + n + n(n-1) + \dots + n(n-1)\dots(n-n+1).$$

Soit f le polynôme

$$1 + T + T(T-1) + T(T-1)(T-2) + \dots + T(T-1)(T-2)\dots(T-n+1).$$

Par ce qui précède b_n est égale à $f(n)$, et b_m est égal à $f(m)$ modulo $m-n$. Il s'ensuit que $b_m - b_n$ est égal à $f(m) - f(n)$ modulo $m-n$, et donc à 0 modulo $m-n$ d'après la question (a), ce qu'il fallait démontrer.

Exercice 10.

Pour tout n, notons $\mathscr{P}_{\leqslant n}$ l'ensemble des nombres premiers inférieurs ou égaux à n, et $\pi(n)$ son cardinal. Le théorème des nombres premiers affirme que $\frac{\pi(n)\log n}{n}$ tend vers 1 quand n tend vers l'infini.

Posons $f(n) = \log(\mathrm{ppcm}(1,\dots,n))$ (par log nous désignerons toujours le logarithme *népérien*).

Question (a). Les diviseurs premiers de $\mathrm{ppcm}(1,\dots,n)$ sont les éléments de $\mathscr{P}_{\leqslant n}$, et si $p \in \mathscr{P}_{\leqslant n}$ la valuation p-adique de $\mathrm{ppcm}(1,\dots,n)$ est le plus grand entier r tel que p^r divise l'un des éléments de $\{1,\dots,n\}$; c'est donc le plus grand entier r tel que $p^r \leqslant n$, qui n'est autre que $\left\lfloor \frac{\log n}{\log p} \right\rfloor$. Par conséquent

$$f(n) = \sum_{p \in \mathscr{P}_n} \log p \left\lfloor \frac{\log n}{\log p} \right\rfloor.$$

Nous nous proposons de montrer que le théorème des nombres premiers vaut si et seulement si $\frac{f(n)}{n}$ tend vers 1 quand n tend vers l'infini.

Pour ce faire, on commence par observer que

$$\left\lfloor \frac{\log n}{\log p} \right\rfloor \leqslant \frac{\log n}{\log p},$$

d'où une majoration

$$f(n) \leqslant \sum_{p \in \mathscr{P}_n} \log p \cdot \frac{\log n}{\log p} = \sum_{p \in \mathscr{P}_n} \log n = \pi(n) \log n.$$

Pour minorer $f(n)$ nous allons introduire un réel ε strictement compris entre 0 et 1. On a

$$f(n) = \sum_{p \in \mathscr{P}_n} \log p \left\lfloor \frac{\log n}{\log p} \right\rfloor \geqslant \sum_{p \in \mathscr{P}_n, p \geqslant n^{1-\varepsilon}} \log p \left\lfloor \frac{\log n}{\log p} \right\rfloor \geqslant \sum_{p \in \mathscr{P}_n, p \geqslant n^{1-\varepsilon}} \log p.$$

Or quand $p \geqslant n^{1-\varepsilon}$ on a $\frac{\log n}{\log p} \geqslant 1-\varepsilon$, si bien que

$$f(n) \geqslant (1-\varepsilon)\log n \cdot \sharp\{p \in \mathscr{P}_n, p \geqslant n^{1-\varepsilon}\}.$$

La différence entre $\sharp\{p \in \mathscr{P}_n, p \geqslant n^{1-\varepsilon}\}$ et $\pi(n)$ est le cardinal de l'ensemble $\{p \in \mathscr{P}_n, p < n^{1-\varepsilon}\}$, que l'on se contente de majorer (très grossièrement !) par $n^{1-\varepsilon}$. On peut ainsi écrire $\sharp\{p \in \mathscr{P}_n, p \geqslant n^{1-\varepsilon}\} = \pi(n)+O(n^{1-\varepsilon})$, et finalement

$$(1-\varepsilon)\log n(\pi(n)+O(n^{1-\varepsilon})) \leqslant f(n) \leqslant \pi(n)\log n.$$

En divisant par n il vient

$$(1-\varepsilon)\frac{\pi(n)\log n}{n} + \underbrace{(1-\varepsilon)\log n\frac{O(n^{1-\varepsilon})}{n}}_{\text{tend vers zéro quand } n\to\infty} \leqslant \frac{f(n)}{n} \leqslant \frac{\pi(n)\log n}{n},$$

et donc

$$(1) \qquad (1-\varepsilon)\frac{\pi(n)\log n}{n} + o(1) \leqslant \frac{f(n)}{n} \leqslant \frac{\pi(n)\log n}{n},$$

soit encore

$$(2) \qquad \frac{f(n)}{n} \leqslant \frac{\pi(n)\log n}{n} \leqslant \frac{1}{1-\varepsilon}\frac{f(n)}{n} + o(1).$$

Supposons que le théorème des nombres premiers soit valide. Dans l'encadrement (1) de droite tend vers 1 quand n tend vers l'infini, et celui de gauche tend vers $(1-\varepsilon)$. Il vient $\liminf \frac{f(n)}{n} \leqslant 1$ et $\limsup \frac{f(n)}{n} \geqslant 1-\varepsilon$. Cette dernière minoration valant pour tout ε strictement compris entre 0 et 1 on voit en faisant tendre ε vers zéro que $\limsup \frac{f(n)}{n} \geqslant 1$. Comme $\liminf \frac{f(n)}{n} \leqslant 1$ il s'ensuit que $\frac{f(n)}{n}$ tend vers 1 quand n tend vers l'infini.

Réciproquement, supposons que $\frac{f(n)}{n}$ tend vers 1 quand n tend vers l'infini. Dans l'encadrement (2) le terme de gauche tend vers 1 quand n tend vers l'infini, ce qui entraîne que $\liminf \frac{\pi(n)\log n}{n} \geqslant 1$; et le terme de droite tend vers $\frac{1}{1-\varepsilon}$ quand n tend vers l'infini, ce qui entraîne que $\limsup \frac{\pi(n)\log n}{n} \leqslant \frac{1}{1-\varepsilon}$. Cette dernière majoration valant pour tout ε strictement compris entre 0 et 1 on voit en faisant tendre ε vers zéro que $\limsup \frac{\pi(n)\log n}{n} \leqslant 1$. Comme $\liminf \frac{\pi(n)\log n}{n} \geqslant 1$ il s'ensuit que $\frac{\pi(n)\log n}{n}$ tend vers 1 quand n tend vers l'infini.

Question (b). Il suffit au vu de la question (a) de montrer que $\psi(n) = f(n)$ pour tout n. Soit n un entier. On a alors

$$\psi(n) = \sum_{m\leqslant n} \Lambda(m) = \sum_{p\in\mathscr{P}_n} \log p \cdot \sharp\{r \geqslant 1, p^r \leqslant n\}.$$

Mais pour tout $p \in \mathscr{P}_n$ l'ensemble des entiers r tels que $r \geqslant 1$ et $p^r \leqslant n$ est précisément l'ensemble des entiers compris entre 1 et $\left\lfloor \frac{\log n}{\log p} \right\rfloor$, qui est de cardinal $\left\lfloor \frac{\log n}{\log p} \right\rfloor$.

En conséquence

$$\psi(n) = \sum_{p\in\mathscr{P}_n} \log p \left\lfloor \frac{\log n}{\log p} \right\rfloor = f(n).$$

Question (c). On a vu que $\psi(n)$ est égal pour tout n à $f(n)$, c'est-à-dire à $\log(\mathrm{ppcm}(1,\dots,n))$. Pour montrer que $\psi(2n) \geqslant n\log 2$ il suffit donc de montrer que $\mathrm{ppcm}(1,\dots,n) \geqslant 2^n$. Nous allons pour ce faire établir les deux inégalités

$$\mathrm{ppcm}(1,\dots,2n) \geqslant \binom{2n}{n} \text{ et } \binom{2n}{n} \geqslant 2^n.$$

Commençons par la première. Pour la montrer, il suffit de s'assurer que $\binom{2n}{n}$ divise $\mathrm{ppcm}(1,\dots,2n)$, donc que $\mathrm{ord}_p(\binom{2n}{n}) \leqslant \mathrm{ord}_p(\mathrm{ppcm}(1,\dots,2n))$ pour tout nombre premier p. Soit donc p un nombre premier. On a vu à la question (d) de l'exercice 4 que $\mathrm{ord}_p(\binom{2n}{n})$ est le nombre N de retenues apparaissant lors de l'addition $n+n$ en base p. Écrivons $n = \sum_{p=0}^{r} a_i p^i$, où les a_i sont compris entre 0 et $p-1$ et où $a_r \neq 0$. Le nombre N est alors au plus égal à $r+1$. Par ailleurs le développement en base p de $2n = n+n$ est de la forme $\sum_{i=0}^{s} b_i p^i$ avec $b_s \neq 0$, où s est ou bien égal à r (s'il n'y a pas de retenue lors de la dernière étape de l'addition) ou bien $r+1$ (s'il y a une retenue lors de la dernière étape) ; et la valuation p-adique de $\mathrm{ppcm}(1,\dots,2n)$ est égale à $\left\lfloor \frac{\log(2n)}{\log p} \right\rfloor = s$. Il s'agit donc de démontrer que $N \leqslant s$. Si $N \leqslant r$ cette inégalité est bien vérifiée puisque s est égal à r ou $r+1$. Et si $N = r+1$ l'addition $n+n$ comporte $r+1$ retenues, et il y a en particulier une retenue à la dernière étape, si bien que $s = r+1$ et $N = s$.

Venons-en maintenant à la seconde inégalité. Soit $\mathscr{Q}$ l'ensemble des parties de $\{1,\dots,2n\}$ a exactement n éléments. Le coefficient binomial $\binom{2n}{n}$ est égal au cardinal de $\mathscr{Q}$, et 2^n est égal à celui de $\mathscr{P}(\{1,\dots,n\})$. Il suffit donc pour conclure de construire une injection de $\mathscr{P}(\{1,\dots,n\})$ dans $\mathscr{Q}$. On peut par exemple considérer l'application Φ qui envoie une partie E de $\{1,\dots,n\}$ sur la partie $E \cup \{n+i\}_{1\leqslant i\leqslant n, i\notin E}$ de $\{1,\dots,2n\}$ (l'application Φ est injective car on peut retrouver E à partir de $\Phi(E)$, puisque $E = \Phi(E) \cap \{1,\dots,n\}$ par construction).

Alternativement, on peut prouver l'inégalité requise de manière calculatoire (c'est celle que j'avais en tête au début mais je la trouve moins élégante que la preuve combinatoire ci-dessus, proposée par l'un d'entre vous), en procédant comme suit. On remarque que $\binom{2n}{n}$ est égal à

$$\frac{(2n)(2n-1)\dots(2n-n+1)}{n!} = \frac{2n\cdot(2n-1)\cdot(2n-n+1)}{n(n-1)\cdot(n-n+1)},$$

c'est-à-dire à

$$\prod_{i=0}^{n-1} \frac{2n-i}{n-i} = \prod_{i=0}^{n-1} \left(2 + \frac{i}{n-i}\right) \geqslant \prod_{i=0}^{n-1} 2 = 2^n.$$

Exercice 11

Question (a). (Dans cette question, on supposait implicitement les entiers n et m non nuls). Si n et m sont premiers entre eux, le lemme chinois fournit un isomorphisme entre $\mathbb{Z}/nm\mathbb{Z}$ et $(\mathbb{Z}/n\mathbb{Z}) \times (Z/m\mathbb{Z})$, si bien que ce dernier groupe est cyclique. Supposons maintenant que n et m ne sont pas premiers entre eux. Soit d leur PGCD, qui est alors > 1. Écrivons $m = \mu d$ et $n = \nu d$. Le produit $\mu\nu d = (\mu d)\nu = (\nu d)\mu$ est multiple de m et n, et est non nul et strictement

inférieur à mn car $mn = (\mu d)(\nu d) = (\mu\nu d)d$ et $d > 1$. Comme $\mu\nu d$ est multiple de n et m, tous les éléments de $(\mathbb{Z}/n\mathbb{Z}) \times (Z/m\mathbb{Z})$ sont de $\mu\nu d$-torsion. L'ordre de tout élément de $(\mathbb{Z}/n\mathbb{Z}) \times (Z/m\mathbb{Z})$ est dès lors un diviseur de $\mu\nu d$ et est en particulier strictement inférieur à mn. Le groupe $(\mathbb{Z}/n\mathbb{Z}) \times (Z/m\mathbb{Z})$ (qui est de cardinal mn) n'est en conséquence pas cyclique.

Question (b). Le plus simple semble de procéder par récurrence (la preuve directe fondée sur le calcul des valuations 2-adiques de coefficients binomiaux est un peu pénible).

On veut montrer que $(1 + 4x)^n = 1 + 4nx$ modulo $8n$ pour tout entier n qui est une puissance de 2. On écrit $n = 2^a$ et l'on fait une récurrence sur a. Si $a = 0$ alors $n = 1$ et $(1 + 4x)^n = 1 + 4x = 1 + 4 \cdot 1 \cdot x$, et le résultat est vrai.

Supposons que le résultat est vrai pour $n = 2^a$ et montrons-le pour l'entier $2^{a+1} = 2n$.

On a par hypothèse $(1+4x)^n = 1+4nx+8nk$ pour un certain k. On a alors

$$\begin{aligned}(1 + 4x)^{2n} &= ((1 + 4x)^n)^2 \\ &= (1 + 4nx + 8nk)^2 \\ &= 1 + 16n^2x^2 + 64n^2k^2 + 8nx + 16nk + 64n^2xk \\ &= 1 + 4(2n)x + 8(2n)(nx^2 + 4nk^2 + k + 4nxk)\end{aligned}$$

et le résultat cherché est donc vrai pour $2n$, ce qui termine la démonstration.

Question (c). Ici on supposait implicitement que $a \geqslant 2$. Le cardinal de $(\mathbb{Z}/n\mathbb{Z})^\times$ est $\Phi(2^a) = 2^{a-1}(2 - 1) = 2^{a-1}$. L'ordre de 5 dans ce groupe est donc un diviseur de 2^{a-1} ; pour montrer que c'est 2^{a-2} il suffit de vérifier que dans $\mathbb{Z}/n\mathbb{Z}$ on a $5^{2^{a-2}} = 1$ et $5^{2^{a-3}} \neq 1$ si $a \geqslant 3$ (en effet comme l'ordre de 5 est une puissance de 2 l'ordre de 5 est de la forme 2^ℓ avec $\ell \leqslant a - 2$, et si $\ell < a - 2$ alors $\ell \leqslant a - 3$ et 2^ℓ divise 2^{a-3}, donc $5^{2^{a-3}} = 1$).

En vertu de la question (b) on sait que l'on a pour tout x

$$(1 + 4x)^{2^{a-2}} = 1 + 4 \cdot 2^{a-2}x = 1 + 2^a x \ \text{ modulo} 8 \cdot 2^{a-2}.$$

Mais $8^{2^{a-2}} = 2^{a+1}$, si bien que l'entier $8^{2^{a-2}}$ est nul modulo 2^a. Par conséquent $(1 + 4x)^{2^{a-2}}$ égal à 1 modulo 2^a. En faisant $x = 1$ on voit en particulier que $5^{2^{a-2}}$ est égal à 1 dans $\mathbb{Z}/n\mathbb{Z}$.

On a par ailleurs

$$5^{2^{a-3}}(1 + 4 \cdot 1)^{2^{a-3}=1+4\cdot 2^{a-3}} \cdot 1 = 1 + 2^{a-1} \ \text{ modulo} 8 \cdot 2^{a-3},$$

toujours d'après la question (b). Or $8^{2^{a-3}}$ est égal à 2^a, si bien qu'on a finalement $5^{2^{a-3}} = 1 + 2^{a-1}$ modulo 2^a, qui est différent de 1 modulo 2^a. L'ordre de 5 dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est donc bien exactement 2^{a-2}.

On a vu dans la première partie de la question que $(1 + 4x)^{2^{a-2}}$ vaut 1 modulo 2^a pour tout x. Par conséquent si y est un entier égal à 1 modulo 4 alors $y^{2^{a-2}} = 1$ dans $(\mathbb{Z}/n\mathbb{Z})^\times$. Soit maintenant y un entier égal à (-1) modulo 4. On a alors $-y = 1$ modulo 4, si bien que $y^{2^{a-2}} = (-1)^{2^{a-2}}(-y)^{2^{(a-2)}} = (-1)^{2^{a-2}}$ modulo 2^a. On distingue alors deux cas.

Si $a \geqslant 3$ on a $(-1)^{2^{a-2}} = 1$, et $y^{2^{a-2}}$ est de ce fait égal à 1 modulo n pour tout y inversible modulo n (en effet, les entiers inversibles modulo n sont les entiers impairs, et un entier impair est égal à 1 ou à (-1) modulo 4). Tout élément de $(\mathbb{Z}/n\mathbb{Z})^\times$ est donc d'ordre divisant 2^{a-2} ; comme ce groupe est de cardinal 2^{a-1}, il n'est pas cyclique.

Si $a = 2$ alors $n = 4$ et $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à $\{-1, 1\}$ qui est cyclique.

Question (d). Soit x un entier. Nous allons montrer que $\mathrm{ord}_p(x^p - 1) = 0$ si $\mathrm{ord}_p(x - 1) = 0$, et que $\mathrm{ord}_p(x^p - 1) = \mathrm{ord}_p(x - 1)$ sinon ; ceci entraînera que pour tout $a \geqslant 2$ on a $(\mathrm{ord}_p(x - 1) \geqslant a - 1) \iff (\mathrm{ord}_p(x^p - 1) \geqslant a)$, ce qui est une autre reformulation de la question.

On commence par remarquer si x est un entier on a $x^p - 1 = (x - 1)^p$ modulo p ; puisque $\mathbb{Z}/p\mathbb{Z}$ est un corps et en particulier un anneau intègre on voit que si $x - 1$ est non nul modulo p alors $x^p - 1$ est non nul. Autrement dit, $\mathrm{ord}_p(x^p - 1) = 0$ si $\mathrm{ord}_p(x - 1) = 0$, comme annoncé.

Supposons maintenant que $\mathrm{ord}_p(x - 1) > 0$. Notons b cet ordre. On peut alors écrire $x = 1 + p^b u$ avec u premier à p. Il vient

$$x^p = 1 + p \cdot p^b u + \sum_{k=2}^{p} \binom{p}{k} p^{kb} u^k = 1 + p^{b+1} u + \sum_{k=2}^{p} \binom{p}{k} p^{kb} u^k.$$

On a $\mathrm{ord}_p(p^{b+1}u) = b + 1$ car u est premier à p. Et par ailleurs pour tout $k \geqslant 2$ la valuation p-adique de $\binom{p}{k} p^{kb}$ est strictement supérieure à $b + 1$: c'est en effet clair si $k < p$ car alors $\binom{p}{k}$ est multiple de p et $\mathrm{ord}_p(p^{kb}) = kb \geqslant 2b \geqslant b + 1$; et si $k = p$ on a $\binom{p}{k} = 1$ mais $\mathrm{ord}_p(p^{pb}) = pb \geqslant 3b > b + 1$ (rappelons que $b \geqslant 1$). On en déduit que la valuation p-adique de

$$p^{b+1} u + \sum_{k=2}^{p} \binom{p}{k} p^{kb} u^k$$

vaut exactement $b + 1$; autrement dit, $\mathrm{ord}_p(x^p - 1) = b + 1 = \mathrm{ord}_p(x) + 1$, ce qu'il fallait démontrer.

Question (e). (On suppose ici implicitement que $n = p^a$ avec a au moins égal à 2). L'ordre de $(\mathbb{Z}/n\mathbb{Z})^\times$ est alors $\Phi(n) = \Phi(p^a) = p^{a-1}(p - 1)$.

Soit x un entier premier à p dont la classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^\times$, ce qui veut dire que x est d'ordre multiplicatif $p - 1$ modulo p. La valuation p-adique b de $x^{p-1} - 1$ est alors strictement positive. Par une application répétée de ce qui a été vu à la question (d), la valuation p-adique de $x^{(p-1)p^{a-2}} - 1$ est égale à $a - 2 + b$. Supposons que la classe de x engendre $\mathbb{Z}/n\mathbb{Z}^\times$; l'ordre de cette classe est alors $(p - 1)p^{a-1}$, si bien que $x^{p^{a-2}(p-1)}$ est différent de 1 modulo p^a, ce qui veut dire que la valuation p-adique de $x^{p^{a-2}(p-1)} - 1$ est strictement inférieure à a. Autrement dit $a - 2 + b < a$, ce qui entraîne que $b < 2$ et donc que $x^{p-1} - 1$ est non nul modulo p^2. Réciproquement supposons que $x^{p-1} - 1$ est non nul modulo p^2. Dans ce cas $b < 2$ et donc $b = 1$ (puisque b est strictement positif). La valuation p-adique de $x^{(p-1)p^{a-2}} - 1$ est alors égale à $a - 2 + 1 = a - 1$, si bien que $x^{(p-1)p^{a-2}} - 1$ est non nul modulo p^a. Et si ℓ est un diviseur strict de $p - 1$ alors $x^{\ell p^{a-1}}$ est différent de 1 modulo p car x^ℓ est différent de 1 modulo p et car $y^{p^{a-1}} = y$ modulo p pour tout y (on applique cela à $y = x^\ell$) ; à plus

forte raison, $x^{\ell p^{a-1}}$ est différent de 1 modulo p^a. Comme tout diviseur strict de $(p-1)p^{a-1}$ ou bien divise $(p-1)p^{a-2}$ ou bien est de la forme ℓp^{a-1} où ℓ est un diviseur strict de $p-1$, on voit que l'ordre de la classe de x dans $(\mathbb{Z}/n\mathbb{Z})^\times$ vaut nécessairement $(p-1)p^{a-1}$; autrement dit, cette classe engendre $(\mathbb{Z}/n\mathbb{Z})^\times$.

Question (f). (Il fallait lire «si $x^{p-1} = 1$ modulo p^2» ; implicitement, x est toujours un entier premier à p dont la classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^\times$). On suppose donc que x^{p-1} est égal à 1 modulo p^2. On écrit $x^{p-1} = 1 + p^2u$. On a alors

$$(x+p)^{p-1} = x^{p-1} + (p-1)p + \sum_{k\geqslant 2} \binom{(p-1)}{k} p^k = x^{p-1} - p \text{ modulo } p^2.$$

Comme $x^{p-1} = 1$ modulo p^2 on voit finalement que $(x+p)^{p-1} = 1-p$ modulo p^2, qui est différent de 1 modulo p^2 puisque p est non nul modulo p^2. Il résulte alors de la question (e), et du fait que $x+p$ est égal à x modulo p, donc engendre également $(\mathbb{Z}/p\mathbb{Z})^\times$, que ou bien x ou bien $x+p$ est générateur de $\mathbb{Z}/n\mathbb{Z})^\times$.

Question (g). On sait que $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique pour tout p premier. On a vu à la question (c) que $(\mathbb{Z}/4\mathbb{Z})^\times$ est cyclique, mais que $(\mathbb{Z}/2^a\mathbb{Z})^\times$ ne l'est plus dès que $a \geqslant 3$. Et si p est impair, $\mathbb{Z}/p^a\mathbb{Z}$ est cyclique pour tout a. On l'a en effet déjà mentionné si $a = 1$. Et si $a \geqslant 2$ on commence par choisir un entier x premier à p qui engendre $(\mathbb{Z}/p\mathbb{Z})^\times$, ce qui est possible par cyclicité de ce dernier. La question (f) assure alors que $(\mathbb{Z}/p^a\mathbb{Z})^\times$ est cyclique, et qu'au moins l'un des deux entiers x et $x+p$ l'engendre.

Soit maintenant n un entier non nul quelconque. Écrivons $n = \prod p_i^{n_i}$ où les p_i sont des nombres premiers deux à deux distincts et les n_i des entiers > 0. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ s'identifie alors par le lemme chinois à $\prod(\mathbb{Z}/p_i^{n_i}\mathbb{Z})^\times$. Supposons que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. Dans ce cas chacun des $(\mathbb{Z}/p_i^{n_i}\mathbb{Z})^\times$ l'est encore, étant un quotient du précédent (par la projection sur le i-ème facteur). Ceci n'impose aucune condition si p_i est impair ; mais si p_i est égal à 2, ceci oblige n_i à être au plus égale à 2. Autrement dit, si $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique, la valuation 2-adique de n est majorée par 2.

Réciproquement, supposons la valuation 2-adique de n majorée par 2. Dans ce cas $(\mathbb{Z}/n\mathbb{Z})^\times = \prod(\mathbb{Z}/p_i^{n_i}\mathbb{Z})^\times$ est un produit de groupes cycliques. Il résulte alors de la question (a) et d'une récurrence immédiate que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si les cardinaux des $(\mathbb{Z}/p_i^{n_i}\mathbb{Z})^\times$ sont deux à deux premiers entre eux, c'est-à-dire si les $p_i^{n_i-1}(p_i-1)$ sont deux à deux premiers entre eux. Or on observe que si p_i est impair, $p_i - 1$ est pair : les $p_i^{n_i-1}(p_i-1)$ ne peuvent donc jamais être deux à deux premiers entre eux s'il existe deux indices i et j distincts avec p_i et p_j impair, ou s'il existe i avec p_i impair et j avec $p_j = 2$ et $n_j = 2$ (rappelons que si $p_j = 2$ on a $n_j = 1$ ou 2, et $p_j^{n_j-1}(p_j-1)$ est égal à 1 si n_j vaut 1 et à 2 sinon).

On voit donc qu'on est nécessairement dans l'un des cas suivants :

- $\diamond$ $n = 1$;
- $\diamond$ $n = 2$ ou $n = 4$;
- $\diamond$ $n = p^a$ avec p premier impair et $a \geqslant 1$;
- $\diamond$ $n = 2p^a$ avec p premier impair et $a \geqslant 1$.

Réciproquement on vérifie que dans chacun de ces cas $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. Cela a déjà été vu explicitement pour les trois premiers ; pour le dernier cela

résulte du fait que si $n = 2p^a$ alors $(\mathbb{Z}/n\mathbb{Z})^\times = (\mathbb{Z}/2\mathbb{Z})^\times \times (\mathbb{Z}/p^a\mathbb{Z})^\times \simeq (\mathbb{Z}/p^a\mathbb{Z})^\times$ qui est cyclique comme on l'a vu (on a utilisé le fait que $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$).