Sorbonne Université
Année universitaire 2025-2026, 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

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

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

Cet exercice est assez facile, une fois qu'on a remarqué que la fonction φ d'Euler est multiplicative : $\varphi(ab) = \varphi(a)\varphi(b)$ lorsque a et b sont premier entre eux (c'est une conséquence du théorème chinois). Par suite, il suffit de vérifier les identités demandées sur $\varphi(n)$ lorsque n est une puissance pure p^k d'un nombre premier p.

Question (a). Les entiers $1 \leqslant x \leqslant p^k$ pas premiers à p^k sont les multiples de p. Il y en a p^{k-1}, ce qui permet de conclure.

Question (b-c) Lorsque $m \geqslant 1$ vérifie $m.a = 0$ modulo n, alors $ma = kn$. Mais alors $m.(a/pgcd(a,n) = k.(n/pgcd(a,n))$. Les deux termes $(a/pgcd(a,n)$ et $(n/pgcd(a,n)$ étant premiers entre eux, il s'ensuit que m est divisible par $(n/pgcd(a,n)$. Finalement le plus petit m possible est $(n/pgcd(a,n)$.

Question (d). Il suffit de traiter $n = p^k$, et c'est une identité télescopique dans ce cas en utilisant a).

Exercice 3

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 $N = 4p_1p_2 \ldots p_r - 1$. Alors $N > 0$ 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 $N = 10(p_1 p_2 \ldots p_r)^2 - 1$. Alors $N > 0$ et $N = (-1)$ modulo 5. Si p est un diviseur de N il ne peut diviser $10p_1 \ldots p_r$, et n'est donc ni égal à 2, ni 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 (par la loi de réciprocité quadratique LRQ)

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

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 $N = 6p_1 p_2 \ldots p_r - 1$. 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).

Question (d). On utilise le fait (cours) qu'il y a $\frac{p-1}{2}$ carrés non-nuls dans $(\mathbb{Z}/p\mathbb{Z})^{\times}$, et que ces carrés sont les racines du polynôme $x^{\frac{p-1}{2}} - 1$. Il s'ensuit que le symbole d'Euler $(\frac{b}{p}) := b^{\frac{p-1}{2}} \bmod p$ vaut 1 lorsque $b \neq 0$ est un carré modulo p, et -1 si b n'est pas un carré modulo p. S'il existait a tel que $a^2 + 1$ soit multiple de p, on aurait $(-1) = a^2$ modulo p, et, d'après le symbole d'Euler qui caractérise le fait d'être un carré modulo p, $(-1)^{(p-1/)2}$ serait donc égal à 1 modulo p. Cela revient, p étant impair (et donc 1 étant différent de (-1) modulo p) à demander que $(p-1)/2$ soit pair, c'est-à-dire que p soit égal à 1 modulo 4. Or p est par hypothèse égal à -1 modulo 4, ce qui est absurde (notez que 1 et -1 diffèrent modulo 4).

Supposons qu'il n'y ait qu'un nombre fini de nombres premiers égaux à 1 modulo 4, disons $p_1, \ldots, p_n$. L'entier $N = 4p_1^2 \ldots p_r^2 + 1$ est alors non nul et si p divise N alors p ne peut être égal à 2 ni à l'un des p_i. Il vaut donc (-1) modulo 4, mais c'est absurde par la première question.