FEUILLE DE TD 1

Exercice 1 (Quelques petits compléments au cours 1)**.**

(a) Soient a et b des entiers. Démontrer l'égalité

$$a\mathbb{Z} \cap b\mathbb{Z} = \mathrm{ppcm}(a, b)\mathbb{Z},$$

où $\mathrm{ppcm}(a, b)$ désigne le plus petit common multiple de a et b.

(b) Démontrer que l'application $\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ n'est pas un isomorphisme si m et n ne sont pas premiers entre eux.

(c) Soit p un nombre premier et soient $x, y \in \mathbb{Q}$ tels que $\mathrm{ord}_p(x) \neq \mathrm{ord}_p(y)$. Montrer l'égalité

$$\mathrm{ord}_p(x + y) = \min(\mathrm{ord}_p(x), \mathrm{ord}_p(y)).$$

(d) Démontrer que le groupe multiplicatif $\mathbb{Q}^\times$ n'est pas finiment engendré.

Exercice 2 (Nécessité de l'hypothèse abélien dans les lemmes de théorie des groupes du cours 2)**.** Soit G un groupe abélien fini. On a vu en cours que les trois propriétés suivantes sont vraies :

— Soient $g, h \in \mathrm{G}$ des éléments d'ordre m et n respectivement. Si m et n sont premiers entre eux, alors gh est d'ordre mn.

— Étant donnée une partie $\mathrm{S} \subset \mathrm{G}$, il existe un élément de G d'ordre le ppcm de tous les éléments de S.

— Soit N le maximum des ordres des éléments de G. Alors $g^{\mathrm{N}} = 1$ pour tout $g \in \mathrm{G}$.

Montrer par des exemples que ces trois énoncés peuvent tomber en défaut si G n'est *pas* abélien.

Exercice 3 (Générateurs des groupes cycliques $(\mathbb{Z}/p\mathbb{Z})^\times$)**.**

(a) Trouver un générateur du groupe cyclique $(\mathbb{Z}/97\mathbb{Z})^\times$.

(b) Soit p un nombre premier de la forme $4\ell + 1$, où ℓ est un nombre premier. Démontrer que 2 est un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$.

Exercice 4 (Valuation p-adique des factorielles)**.** Soit p un nombre premier. Écrivons n en base p, c'est-à-dire

$$n = a_0 + a_1 p + \cdots + a_r p^r \quad \text{avec } a_i \in \{0, \ldots, p-1\} \text{ et } a_r \neq 0.$$

(a) Démontrer que la valuation p-adique de $n!$ est donnée par

$$\mathrm{ord}_p(n!) = \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor = \frac{n - (a_0 + \cdots - +a_n)}{p-1},$$

où $\lfloor x \rfloor$ désigne la partie entière d'un nombre réel x.

(b) Soit $n \geq 1$ un entier. Démontrer que tout nombre premier p satisfaisant à $n < p \leq 2n$ divise le coefficient binomial $\binom{2n}{n}$.

(c) Démontrer que le quotient de factorielles

$$\frac{n!(30n)!}{(6n)!(10n)!(15n)!}$$

est un nombre entier pour tout $n \geq 1$.

(d) Soient $a, b \geq 1$ des entiers. Démontrer que $\mathrm{ord}_p(\binom{a+b}{a})$ est le nombre de retenus dans l'addition de a et b en base p.

(e) Soit p un nombre premier. Démontrer que $\binom{p}{i}$ est divisible par p pour tout $1 \leq i \leq p-1$. En déduire que $n^p - n$ est divisible par p pour tout entier n et que l'application $x \mapsto x^p$ induit un morphisme d'anneaux $\mathrm{A} \to \mathrm{A}$ pour tout anneau A dans lequel p est nul.

Exercice 5 (Cas élémentaires du théorème de Dirichlet)**.**

(a) En considérant $(n!)^2 - 1$, démontrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 4.

(b) En considérant $5(n!)^2 - 1$, démontrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 5.

(c) En adaptant la preuve d'Euclide, démontrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 6.

(d) Montrer que si p est un nombre premier congru à 3 modulo 4, alors il n'existe pas d'entier $a \in \mathbb{Z}$ tel que a^2+1 soit multiple de p. (*Indication* : que vaut a^{p-1} modulo p ?). En déduire qu'il existe une infinité de nombres premiers congrus à 1 modulo 4.

(e) Soit $n \geq 2$ un entier. Démontrer qu'il existe une infinité de nombres premiers qui ne sont *pas* congrus à 1 modulo n.

Exercice 6. Soit $f \in \mathbb{Z}[\mathrm{T}]$ un polynôme non constant.

(a) Montrer qu'il existe des entiers n arbitrairement grands tels que $f(n)$ ne soit pas un nombre premier.

(b) Montrer que l'ensemble des nombres premiers qui divisent l'une des valeurs $f(n)$, pour $n \geq 1$, est infini.

Exercice 7 (Pseudopolynômes)**.**

(a) Soit $f \in \mathbb{Z}[\mathrm{T}]$ un polynôme. Posons $a_n = f(n)$ pour $n \geq 0$. Démontrer que

$$m - n \text{ divise } a_m - a_n \text{ pour tout } m > n \geq 0.$$

(b) Soit $f \in \mathbb{Q}[\mathrm{T}]$ tel que $f(n) \in \mathbb{Z}$ pour tout n. La propriété ci-dessus reste-elle vraie ?

(c) Soit $b_n = \sum_{k=0}^{n} \frac{n!}{k!}$. Démontrer l'égalité $b_n = \lfloor en! \rfloor$ pour tout $n \geq 1$, où $e = \sum_{k=0}^{\infty} \frac{1}{k!}$.

(d) Démontrer qu'il n'existe pas de polynôme $f \in \mathbb{Z}[\mathrm{T}]$ tel que $f(n) = b_n$ pour tout $n \geq 0$.

(e) Démonter que $m - n$ divise $b_m - b_n$ pour tout $m > n \geq 0$. Les suites d'entiers $(b_n)_{n\geq 0}$ ayant cette propriété s'appellent des *pseudopolynômes*.

Exercice 8 (Fonction indicatrice d'Euler)**.** Soit $n \geq 1$ un entier.

(a) Démontrer l'égalité

$$\varphi(n) = n \prod_{p|n} \frac{p-1}{p},$$

où le produit décrit l'ensemble des nombres premiers divisant n.

(b) Soit a un nombre entier tel que a et n sont premiers entre eux. Démontrer que l'ordre de a mod n dans $\mathbb{Z}/n\mathbb{Z}$ est égal à n.

(c) En général, démontrer que l'ordre de a mod n dans $\mathbb{Z}/n\mathbb{Z}$ est égal à $n/\mathrm{pgcd}(a, n)$.

(d) Démontrer l'égalité

$$\sum_{d|n} \varphi(d) = n,$$

où la somme décrit l'ensemble des entiers $1 \leq d \leq n$ divisant n.

Exercice 9 (Équation diophantienne $y^2 = x^3 + 7$)**.** Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation

$$y^2 = x^3 + 7.$$

(a) Démontrer que x est impair et que y est pair.

(b) À l'aide de la factorisation $x^3 + 8 = (x + 2)(x^2 - 2x + 4)$, démontrer que $x^3 + 8$ possède un facteur premier congru à 3 modulo 4.

(c) Démontrer que chaque facteur premier de $y^2 + 1$ est congru à 1 modulo 4.

(d) Conclure que $y^2 = x^3 + 7$ n'a pas de solution entière.

Exercice 10 (Des énoncés équivalents au théorème des nombres premiers)**.**

(a) Montrer que le théorème des nombres premiers $\pi(\mathrm{X}) \sim \mathrm{X}/\log \mathrm{X}$ est équivaut à l'énoncé

$$\mathrm{ppcm}(1, \ldots, n) = e^{n+o(n)},$$

où $o(n)$ désigne une fonction $f(n)$ telle que $f(n)/n$ converge vers 0 lorsque $n \to +\infty$.

(b) Soit Λ la fonction de von Mangoldt, définie comme

$$\Lambda(n) = \begin{cases} \log p & \text{si } n = p^r \text{ avec } r \geq 1, \\ 0 & \text{sinon.} \end{cases}$$

Posons $\psi(\mathrm{X}) = \sum_{n \leq \mathrm{X}} \Lambda(n)$ pour un nombre réel $\mathrm{X} > 0$. Démontrer que le théorème des nombres premiers $\pi(\mathrm{X}) \sim \mathrm{X}/\log \mathrm{X}$ équivaut à l'énoncé $\psi(\mathrm{X}) \sim \mathrm{X}$ lorsque $\mathrm{X} \to +\infty$.

(c) En considérant le coefficient binomial $\binom{2n}{n}$, démontrer l'inégalité $\psi(2n) \geq n \log 2$.

Exercice 11.

(a) Soient m et n des nombres entiers. Démontrer que le groupe $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ est cyclique si et seulement si m et n sont premiers entre eux.

(b) Si n est une puissance de 2, montrer que $(1 + 4x)^n \equiv 1 + 4nx$ modulo $8n$.

(c) Soient a un entier et $n = 2^a$. Démontrer que l'ordre de la classe de 5 dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est égal à 2^{a-2}. Le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est-il cyclique ?

(d) Soient $p \geq 3$ un nombre premier et $a \geq 2$ un entier. Si x est un entier, démontrer que les conditions $x \equiv 1 \bmod p^{a-1}$ et $x^p \equiv 1 \bmod p^a$ sont équivalentes.

(e) Soit x un entier dont la classe modulo p engendre $(\mathbb{Z}/p\mathbb{Z})^\times$. Montrer que la classe de x engendre $(\mathbb{Z}/n\mathbb{Z})^\times$ si et seulement si $x^{p-1} \not\equiv 1 \bmod p^2$.

(f) Si $x^{p-1} \equiv 1 \bmod p$, démontrer que $(x + p)^{p-1} \not\equiv 1 \bmod p^2$. En déduire qu'au moins l'un des deux, x ou $x + p$, est générateur de $(\mathbb{Z}/n\mathbb{Z})^\times$.

(g) Quels sont les nombres entiers pour lesquels le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique ?

Exercice 12 (Nombres de Carmichael)**.** On appelle *nombre de Carmichael* un entier n qui n'est pas un nombre premier tel que : tout entier $1 \leq a < n$ premier à n satisfait à $a^{n-1} \equiv 1 \bmod n$.

(a) Soit $n \geq 2$ un entier sans facteur carré tel que, pour tout diviseur premier p de n, le nombre $p-1$ divise $n-1$. Démontrer que n est soit premier soit un nombre de Carmichael.

(c) En déduire que 561 est le plus petit nombre de Carmichael.

Exercice 13 (Témoins de non-primalité dans le critère de Miller-Rabin)**.**

(1) Démontrer que dans un groupe cyclique G d'ordre pair, l'équation $2x = 0$ possède exactement deux solutions.

(2) Soit $n \geq 3$ un entier impair et soit u le nombre de facteurs premiers distincts de n. Montrer que dans le groupe $(\mathbb{Z}/n\mathbb{Z})^\times$, l'équation $x^2 = 1$ possède exactement 2^u solutions.

(3) On suppose que n n'est pas premier, d'où $u \geq 2$. Démontrer que, parmi les nombres entiers $1 \leq a \leq n$ qui sont premiers à n, les témoins de non-primalité de Miller-Rabin de n sont en proportion au moins égale à $1 - 2^{1-u} \geq 3/4$.