

Exercice 1. Soit $n \in \mathbb{Z}$. Considérons l'anneau $\mathbb{Z}/n\mathbb{Z}$, et notons $\mathbb{Z}/n\mathbb{Z}^\times$ le sous-ensemble des éléments inversibles pour la loi de la multiplication sur $\mathbb{Z}/n\mathbb{Z}$.

- Montrer que $\mathbb{Z}/n\mathbb{Z}^\times$ est un groupe.
- Soit $m \in \mathbb{Z}$ un autre entier. Montrer que $\gcd(m, n) = 1$ si et seulement s'il existe deux entiers $u, v \in \mathbb{Z}$ tels que $um + vn = 1$ et en déduire que la classe $\bar{m} \in \mathbb{Z}/n\mathbb{Z}$ appartient à $\mathbb{Z}/n\mathbb{Z}^\times$ si et seulement si $\gcd(m, n) = 1$.

Exercice 2. Le but de cet exercice est de montrer le théorème des restes chinois suivant : Soient m, n deux entiers, et $\phi : \mathbb{Z}/mn\mathbb{Z}^\times \rightarrow \mathbb{Z}/m\mathbb{Z}^\times \times \mathbb{Z}/n\mathbb{Z}^\times$ le morphisme de réduction défini par $\phi : x + mn\mathbb{Z} \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$. Si $(m, n) = 1$, alors ϕ est un isomorphisme d'anneaux.

- Montrer que ϕ est un homomorphisme d'anneaux.
- Supposons que $(m, n) = 1$. Montrer que ϕ est injectif, et en déduire que ϕ est un isomorphisme d'anneaux, et qu'il induit donc un isomorphisme de groupes $(\mathbb{Z}/mn\mathbb{Z}^\times) \rightarrow (\mathbb{Z}/m\mathbb{Z}^\times) \times (\mathbb{Z}/n\mathbb{Z}^\times)$.
- Pour $a, b \in \mathbb{Z}$, écrire explicitement un entier $x \in \mathbb{Z}$ tel que $x \equiv a \pmod{m}$ et $x \equiv b \pmod{n}$.
- Trouver un entier x qui vérifie les conditions suivantes :

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

Exercice 3. Dans cet exercice, on donne des applications du théorème des restes chinois.

- Soit $n \in \mathbb{Z}_{\geq 1}$ avec la factorisation primaire $n = p_1^{a_1} \cdots p_k^{a_k}$, où $a_i \in \mathbb{Z}_{\geq 1}$ et p_i sont des nombres premiers avec $p_i \neq p_j$ si $i \neq j$. Montrer qu'on a un isomorphisme d'anneaux

$$\mathbb{Z}/n\mathbb{Z} = \prod_i \mathbb{Z}/p_i^{a_i}\mathbb{Z}.$$

- Calculer l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.
- Montrer que tout groupe abélien d'ordre 24 est isomorphe à l'un des trois groupes suivants :

$$\mathbb{Z}/24\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^3 \times \mathbb{Z}/3\mathbb{Z}.$$

Pourquoi ces trois groupes ne sont-ils pas isomorphes ?

- Combien y-a-il de classes d'isomorphisme des groupes abéliens d'ordre 10^4 ?

Exercice 4. Expliciter tous les caractères pour les groupes a. $(\mathbb{Z}/12\mathbb{Z})^\times$ et b. $(\mathbb{Z}/9\mathbb{Z})^\times$.

Exercice 5. Soient G un groupe abélien fini et \hat{G} son groupe de caractères. Notons \mathbb{C}^G l'espace des fonctions complexes sur G . Pour $f \in \mathbb{C}^G$, on définit sa transformée de Fourier $\hat{f} \in \mathbb{C}^{\hat{G}}$ par

$$\hat{f}(\chi) = \frac{1}{|G|} \sum_{x \in G} \overline{\chi(x)} f(x).$$

a. Montrer que pour toute $f \in \mathbb{C}^G$, on a

$$f(x) = \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi(x).$$

b. Montrer qu'on a une égalité

$$\sum_{x \in G} |f(x)|^2 = |G| \sum_{\chi \in \hat{G}} |\hat{f}(\chi)|^2$$

c. Soit $H \in G$ un sous-groupe de G et $H^\perp \subset \hat{G}$ est défini comme $\{\chi \in \hat{G} \mid \chi(x) = 1 \text{ pour tout } x \in H\}$. Montrer que pour tout $f \in \mathbb{C}^G$

$$\sum_{x \in H} f(x) = |H| \sum_{\chi \in H^\perp} \hat{f}(\chi)$$

d. Montrer que $\widehat{f \hat{g}} = \hat{f} * \hat{g}$ et $\widehat{f * g} = |G| \hat{f} \hat{g}$. Ici $f * g(x) = \sum_{y, z \mid y+z=x} f(y)g(z)$ et la convolution des fonctions f et g .

Exercice 6. Soient $p \geq 3$ un nombre premier, et $e \geq 1$ un entier. Le but de cet exercice est de montrer que le groupe $G = (\mathbb{Z}/p^e\mathbb{Z})^\times$ est cyclique d'ordre $(p-1)p^{e-1}$.

a. Soit $a \equiv b \pmod{[p^e]}$. Montrer que $a^p \equiv b^p \pmod{[p^{e+1}]}$.

b. Montrer que $(1 + ap)^{p^{e-2}} \equiv 1 + ap^{e-1} \pmod{p^e}$.

c. On fixe un $a \in \mathbb{Z}$ tel que $p \nmid a$. Trouver l'ordre de $1 + ap$ dans le groupe $(\mathbb{Z}/p^e\mathbb{Z})^\times$.

d. On notera par $H \in G$ le sous-groupe cyclique engendré par $1 + ap$. Montrer qu'on a un isomorphisme de groupes $G/H \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

e. Soit $x \in G$ tel que son image dans $(\mathbb{Z}/p\mathbb{Z})^\times$ soit un générateur. Montrer que $x(1 + ap)$ est un générateur de G .

Exercice 7. Soit $e \geq 2$ un entier. On pose $H = \{\chi \in (\mathbb{Z}/2^e\mathbb{Z})^\times \mid \chi \equiv 1 \pmod{4}\}$.

a. Montrer que $5^{2^{e-3}} \equiv 1 + 2^{e-1} \pmod{[2^e]}$.

b. Montrer que H est un groupe cyclique d'ordre 2^{e-2} et $5 \in H$ est un générateur de H .

c. Montrer que on a $(\mathbb{Z}/2^e\mathbb{Z})^\times = H \times \mathbb{Z}/2\mathbb{Z}$.

Exercice 8* Soit G un groupe fini. Une *représentation* de G est un homomorphisme $\rho : G \rightarrow \text{Aut}(V)$, où V un espace vectoriel sur \mathbb{C} de dimension finie.

On dit qu'un sous-espace $W \subset V$ est invariant si il est invariant par rapport à tout les applications $\rho(g)$ où $g \in G$.

a. Montrer que pour tout espace invariant W il existe un sous-espace invariant supplémentaire W' .

b. Montrer que si G est abélien il existe un sous-espace de V invariant de dimension 1.

c. Montrer que tout représentation de G est isomorphe à une somme de représentations de dimension 1.

Exercice 9.

a. Caractériser les nombres premiers p modulo lesquels -1 est un carré.

b* Caractériser les nombres premiers p modulo lesquels 2 est un carré.

Exercice 10. Exprimer la condition que a est un carré modulo n pour $n = 2^e p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, où p_1, \dots, p_k sont des nombres premiers impairs distinctes, en termes des symboles de Legendre.

Exercice 11. (Sommes de Gauss). Soit p un nombre premier. On pose ζ une racine primitive p -ème de l'unité, par exemple $\zeta = \exp(\frac{2\pi i}{p})$. Soit $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ un caractère. On étend χ en une fonction sur $\mathbb{Z}/p\mathbb{Z}$ en posant $\chi(0) = 0$. Pour $a \in \mathbb{Z}/p\mathbb{Z}$, on pose

$$\tau_a(\chi) = \sum_{x \in (\mathbb{Z}/p\mathbb{Z})^\times} \chi(x) \zeta^{ax}$$

et $\tau(\chi) = \tau_1(\chi)$. On appelle les $\tau_a(\chi)$ des *sommes de Gauss* de χ .

a. Montrer que $\tau_a(\chi) = \bar{\chi}(a) \tau(\chi)$ pour tout $a \in \mathbb{Z}/p\mathbb{Z}$.

b. Calculer $\tau(\chi) \overline{\tau(\chi)}$ et en déduire la valeur absolue $|\tau(\chi)|$.

c. Montrer que si $\chi(x) = \left(\frac{x}{p}\right)$ est le symbole de Legendre, alors on a $\tau(\chi)^2 = \chi(-1)p$ et en déduire que

$$\tau(\chi) = \pm \begin{cases} \sqrt{p} & \text{si } p \equiv 1 \pmod{4}, \\ i\sqrt{p} & \text{si } p \equiv 3 \pmod{4}. \end{cases}$$

d. Soit q un nombre premier différent de p . Calculer $\tau(\chi)^q \pmod{q}$ avec la formule de binôme. En déduire la loi de réciprocité :

$$(-1)^{\frac{p-1}{2} \frac{q-1}{2}} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = 1$$

e. Calculer $\left(\frac{79}{101}\right)$.

Exercice 12. (Somme de Gauss quartique). Soit p un nombre premier avec $p \equiv 1 \pmod{4}$, et soit $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ un caractère d'ordre 4. On pose

$$J = \sum_{t=1}^{p-2} \left(\frac{1+t}{p}\right) \chi(t).$$

a. Montrer que

$$\tau(\chi)^2 = J \tau(\chi^2)$$

b. Montrer que J prend valeurs dans les nombres Gaussien $\mathbb{Z}[i]$ et que $J\bar{J} = p$. En déduire que tout nombre premier p avec $p \equiv 1 \pmod{4}$ est une somme de deux carrés.

c. Montrer que tout nombre premier p avec $p \equiv 3 \pmod{4}$ n'est pas une somme de deux carrés.

Exercice 13.

a. Montrer que pour tout $k \in \mathbb{N}$, la série

$$\sum_{n=1}^{\infty} \frac{(\ln n)^k}{n^s}$$

converge pour tout $s \in \mathbb{R}_{>1}$.

b. Montrer que pour tout $x > 0$ on a

$$\sum_{n=1}^{\infty} \frac{1}{n^2 + x^2} < \frac{\pi}{2x}$$

c. Montrer que

$$\sum_{n=1}^{\infty} \sum_{m=1}^{\infty} \frac{1}{n^2 + m^4} < \frac{\pi^3}{12}$$

Exercice 14. (Séries d'Eisenstein). Soient $\tau \in \mathbb{C}$ avec $\Im \tau > 0$, et $s \in \mathbb{R}_{>0}$.

a. Montrer que la série d'Eisenstein

$$E(s, \tau) = \sum_{(m,n) \neq (0,0)} \frac{1}{|m + n\tau|^{2s}}$$

converge absolument lorsque $s > 1$.

b. Montrer que pour tout $k \in \mathbb{N}$ la série d'Eisenstein

$$E_{2k}(\tau) = \sum_{(m,n) \neq (0,0)} \frac{1}{(m + n\tau)^{2k}}$$

définit bien une fonction holomorphe sur le demi-plan supérieur $\tau \in \mathbb{H} = \{z \in \mathbb{C} | \Im z > 0\}$

c. Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z})$ une matrice aux éléments entiers et déterminant 1. Calculer $E\left(s, \frac{a\tau + b}{c\tau + d}\right)$ et $E_{2k}\left(\frac{a\tau + b}{c\tau + d}\right)$.

Exercice 15. Considérons la fonction

$$f(z) = \frac{\pi^2}{\sin^2 \pi z} - \sum_{n=-\infty}^{\infty} \frac{1}{(z - n)^2}$$

a. Montrer que f est holomorphe sur \mathbb{C} .

b. Montrer que f est bornée.

c. Calculer $\lim_{\Im z \rightarrow \infty} f(z)$.

d. En déduire que $f = 0$.

e. Montrer que

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2}$$

f. Montrer que

$$\sin \pi z = \pi z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2}\right)$$

Exercice 16. Considérons la fonction

$$\wp(z) = \frac{1}{z^2} + \sum_{(m,n) \neq (0,0)} \frac{1}{(z + m + n\tau)^2} - \frac{1}{(m + n\tau)^2}$$

- Montrer que la série est convergente et que \wp est une fonction holomorphe en dehors de l'ensemble $\{m + n\tau \mid m, n \in \mathbb{Z}\}$.
- Calculer $f(z + m + n\tau)$.

Exercice 17. Soit C l'ensemble des fonctions complexes définies sur \mathbb{N}^* . Pour $f, g \in C$ on pose

$$f \star g(n) = \sum_{d \mid n} f(d)g(n/d) = \sum_{d_1, d_2 \mid d_1 d_2 = n} f(d_1)g(d_2)$$

convolution multiplicative de f et g .

- Montrer que la convolution est commutative et associative.
- Trouver une fonction $\varepsilon \in C$ telle que $f \star \varepsilon = f$.
- Décrire toutes fonctions $f \in C$ inversibles par rapport à la convolution.
- Montrer que l'espace de fonctions multiplicatives est fermé par rapport à la convolution.
- Soit $\mu \in C$ la fonction telle que $\mu(n) = (-1)^r$ si $n = p_1 \cdots p_r$ est un produit de r nombres premiers distincts, et $\mu(n) = 0$ sinon. On appelle μ la *fonction de Möbius*. Calculer $\mu \star 1$. En déduire l'inverse de la fonction μ par rapport à la convolution.
- Soit $\varphi \in C$ la fonction définie par $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. On appelle φ l'*indicatrice d'Euler*. Calculer $\sum_{d \mid n} \varphi(d)$.
- Let $g \in C$. Trouver la fonction $f \in C$ telle que $g(n) = \sum_{d \mid n} f(d)$.

Exercice 18. On dit que $f \in C$ est à *croissance polynomiale*, s'il existe un entier k tel que $f(n) = O(n^k)$ lorsque $n \rightarrow \infty$. On notera par $C' \subset C$ l'espace de fonctions de croissance polynomiale.

Pour $f \in C'$ on pose

$$L(s, f) = \sum_n \frac{f(n)}{n^s}.$$

- Montrer que C' est fermé par rapport à la convolution.
- Montrer que $L(s, f)$ est une fonction holomorphe pour $\Re(s)$ assez grand.
- Exprimer $L(s, f \star g)$ en termes de $L(s, f)$ et $L(s, g)$.
- Calculer $L(s, \mu)$ et $L(s, \varphi)$ en termes de $\zeta(s) = L(s, 1)$, où φ est l'indicatrice d'Euler et μ - la fonction de Möbius.

Exercice 19. La *fonction de Liouville* $\lambda \in C'$ est une fonction strictement multiplicative définie par $\lambda(p) = -1$ pour tout p premiers.

- Calculer $\sum_{d \mid n} \lambda(d)$.
- Exprimer $L(s, \lambda)$ en termes de la fonction zêta et comme un produit infini.

Exercice 20. Soit $k \in \mathbb{N}$ un nombre naturel et soit $\sigma_k(n)$ la somme de k -èmes puissances de diviseurs de n

$$\sigma_k(n) = \sum_{d \mid n} d^k.$$

Exprimer la série de Dirichlet $L(s, \sigma_k)$ en termes de la fonction zêta.

Exercice 21.

a. Exprimer la somme

$$\sum_{\substack{m,n \in \mathbb{N}^2 \\ (m,n)=1}} \frac{1}{m^2 n^2}$$

en termes de la fonction zêta.

b. La même question pour la somme

$$\sum_{\substack{m_1, \dots, m_k \in \mathbb{N}^k \\ (m_1, \dots, m_k)=1}} \frac{1}{m_1^{s_1} \dots m_r^{s_r}}$$

Exercice 22.

Soit $J_k(n)$ est le nombre de k -tuplets d'entiers positifs n_1, \dots, n_k inférieurs à n tels que $(n_1, \dots, n_k, n) = 1$.

- Exprimer $J_k(n)$ en termes de diviseurs premiers de n .
- Calculer $\sum_{d|n} J_k(n)$.
- Montrer que $J_k(n)$ est multiplicative.
- Calculer la série de Dirichlet $L(s, \sigma_k)$.

Exercice 23. La fonction Λ de von Mangoldt est définie par

$$\Lambda(n) = \begin{cases} \ln p & \text{si } n = p^a \\ 0 & \text{sinon} \end{cases}$$

Montrer que pour une fonction f strictement multiplicative

$$\frac{L(s, f)'}{L(s, f)} = -L(s, \Lambda f).$$

Exercice 24. Les nombres de Bernoulli B_k sont défini par le développement

$$\frac{z}{e^z - 1} = \sum_{k=0}^{\infty} \frac{B_k}{k!} z^k$$

- Calculer B_0, B_1, B_2, B_4 et B_k pour $k > 1$ impaires.
- Trouver le développement en série de Taylor de la fonction.

$$f(z) = \pi z \cot \pi z.$$

- Exprimer $\zeta(2k)$, $k = 1, 2, \dots$ en termes de nombres de Bernoulli.
- d* Utilisant l'équation fonctionnelle $\zeta^*(s) = \zeta^*(1-s)$ où $\zeta^*(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$ exprimer $\zeta(-k)$, $k = 1, 2, \dots$ en termes de nombres de Bernoulli.
- Exprimer $S_m(n) = \sum_{i=0}^n i^m$ en termes de nombres de Bernoulli. *Indication* : Utiliser la formule d'Euler-Maclaurin :

$$\frac{1}{e^{\frac{a}{\delta x}} - 1} f(z) = \sum_{k=0}^{\infty} \frac{B_k}{k!} f^{(k-1)}(z),$$

où $f^{(-1)}(z) := \int_0^z f(t) dt$.

Exercice 25.

a. Trouver le domaine de divergence simple de la série

$$\eta(s) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}$$

b. Exprimer $\eta(s)$ en termes de la fonction ζ .

c. Trouver le résidu $\operatorname{Res}_{s=1} \zeta(s) ds$.

Exercice 26. Trouver la série de Taylor pour la série d'Eisenstein

$$E_{2k}(q) = \sum_{m,n \neq (0,0)} \frac{1}{(m + n\tau)^{2k}},$$

où $q = e^{2\pi i\tau}$.

Exercice 27. Trouver le résidu $\operatorname{Res}_{s=1} L(s, \chi_0) ds$, où χ_0 est le caractère trivial de Dirichlet modulo N .

Exercice 28. Trouver les limites

$$\limsup_{N \rightarrow \infty} \frac{\varphi(N)}{N} \text{ et } \liminf_{N \rightarrow \infty} \frac{\varphi(N)}{N}$$

où φ est l'indicatrice d'Euler.

Exercice 29. Calculer l'intégrale $\int_1^{\infty} \frac{\{x\}}{x^2} dx$, où $\{x\}$ est la partie fractionnelle de x . Exprimer le résultat en termes de la constante d'Euler-Mascheroni

$$\gamma = \lim_{n \rightarrow \infty} \sum_{k=1}^n \frac{1}{k} - \ln n \approx 0.5772$$

Exercice 30. Trouver les produits infinis

a. $\prod_{n=2}^{\infty} \frac{n^3 - 1}{n^3 + 1}$.

b. $\prod_{n=1}^{\infty} (1 - z^n)^{\mu(n)/n}$.

c. $\prod_{n=1}^{\infty} (1 + z^{2^n})$.

d* $z \prod_{n=1}^{\infty} \left(1 + \frac{z}{n}\right) e^{-z/n}$,

e* Trouver la série de Taylor de $\prod_{n=1}^{\infty} (1 - q^n)$.

Reponses :

2. $c : au + bv$ où $um + vn = 1$; $d : 26$.
3. $b : \phi(n) = n \prod_{p|n} (1 - p^{-1})$, c . Le nombre d'éléments d'ordre 2 est 2,4 et 8 respectivement, $d : 25$.
4. $a : (1,1,1,1), (1,-1,1,-1), (1,1,-1,-1), (1,-1,-1,1)$. $b : (1, \zeta^k, \zeta^{2k}, \zeta^{5k}, \zeta^{4k}, \zeta^{3k})$ où $k = 0, \dots, 5$ et $\zeta = \exp \pi i/3$.
6. $c : p^{e-1}$.
9. $a : p \equiv 1 \pmod{4}$ ou $p = 2$, $b : p \equiv \pm 1 \pmod{8}$.