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 $\mathbb{Z}/n\mathbb{Z}$.

a. Trouver deux entiers $u, v \in \mathbb{Z}$ tels que $15u + 26v = 1$.

b. 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 $um + vn = 1$.

c. Montrer que $\mathbb{Z}/n\mathbb{Z}^\times$ est un groupe.

Exercice 2. ▽ Le but de cet exercice est de montrer le théorème des restes chinois suivant : Soient m, n deux entiers, et $\phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 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.

a. Montrer que ϕ est un homomorphisme d'anneaux.

b. 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 $(\mathbb{Z}/mn\mathbb{Z})^\times \to (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.

c. Soient $u, v \in \mathbb{Z}$ satisfont $um + vn = 1$ et soient $a, b \in \mathbb{Z}$ des entiers arbitraires. Calculer l'image de $aum + bvn$ dans $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

d. Trouver un entier x qui vérifie les conditions suivantes :

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

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

a. ▼ Soit G un groupe abélien de type fini. Montrer qu'il existe une unique suite des entiers positifs $d_1, d_2, \ldots$ telle que d_i divise d_{i+1} pour tout i et

$$G = \prod_i \mathbb{Z}/d_i\mathbb{Z}.$$

b. Soit $n \in \mathbb{Z}_{\geqslant 1}$ avec la factorisation primaire $n = p_1^{a_1} \cdots p_k^{a_k}$, où $a_i \in \mathbb{Z}_{\geqslant 1}$ et p_i sont des nombres premiers avec $p_i \neq p_j$ si $i \neq j$. Calculer l'ordre du groupe $(\mathbb{Z}/n\mathbb{Z})^\times$.

c. 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 ? Trouver les nombres d_i correspondants.

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

Exercice 4. (Lemme de Hensel) Soit $Q(x) \in \mathbb{Z}[x]$ un polynôme et $x_0 \in \mathbb{Z}/p\mathbb{Z}$ tel que $Q(x_0) \equiv 0 \mod p$ et $Q'(x_0) \not\equiv 0 \mod p$. Montrer qu'il existe une unique suite $x_0, x_1, \ldots$ telle que $x_0 \in \mathbb{Z}/p\mathbb{Z}$, $x_{e+1} \equiv x_e \mod p^e$ et $Q(x_e) \equiv 0 \mod p^{e+1}$.

Exercice 5. ▽ Soient $p \geqslant 3$ un nombre premier, et $e \geqslant 1$ 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 $a \equiv b \mod p^e$. Montrer que $a^p \equiv b^p \mod p^{e+1}$.

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

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 6* Soit $e \geqslant 2$ un entier. On pose $H = \{x \in (\mathbb{Z}/2^e\mathbb{Z})^\times | x \equiv 1 \mod 4\}$.

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

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 7* Soit G un groupe fini. Une *représentation* de G est un homomorphisme $\rho : G \to \mathrm{Aut}(V)$, 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 8. ▽ Expliciter tous les caractères pour les groupes

a. $(\mathbb{Z}/12\mathbb{Z})^\times$

b. $(\mathbb{Z}/9\mathbb{Z})^\times$.

c. Expliciter tous les caractères d'ordre 2 pour le groupe $(\mathbb{Z}/p^n\mathbb{Z})^\times$.

Exercice 9. 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 $\{\chi \in \hat{G} | \chi(x) = 1 \text{ pour tout } x \in H\}$. 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 $\widehat{fg} = \hat{f} * \hat{g}$ et $\widehat{f * g} = |G|\hat{f}\hat{g}$. Ici $f * g(x) = \sum_{y,z|y+z=x} f(y)g(z)$ et la convolution des fonctions f et g.

Exercice 10. ▽

a. Montrer que

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

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

c. ▼ Caractériser les nombres premiers p modulo lesquels 2 est un carré.

Exercice 11. ▽ Exprimer la condition que a premier avec $p > 2$ est un carré modulo p^k, en termes du symbole de Legendre.

Exercice 12. *Sommes de Gauss.*▽ Soit p un nombre premier. On pose ζ une racine primitive p-ème de l'unité, par exemple $\zeta = \exp(2\pi i/p)$. Soit $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ 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

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

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 $(a, \chi) \neq (0, \varepsilon)$ où ε est le caractère trivial.

b. Calculer $\tau(\chi_1)\tau(\chi_2)/\tau(\chi_1\chi_2)$ pour tout (χ_1, χ_2) tels que $\chi_1\chi_2 \neq \varepsilon$.

c. Calculer $\tau(\chi)\tau(\bar{\chi})$ pour tout $\chi \neq \varepsilon$.

d. Calculer $|\tau(\chi)|$ pour tout $\chi \neq \varepsilon$.

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

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

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

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

g. Calculer $\left(\frac{79}{101}\right)$ et $\left(\frac{1877}{3323}\right)$.

Exercice 13. *(Somme de Gauss quartique).* Soit p un nombre premier avec $p \equiv 1 \mod 4$, et soit $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$ 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 $p \equiv 1 \mod 4$ est une somme de deux carrées.

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

Exercice 14.

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 15. ▽ *(Séries d'Eisenstein).* Soient $\tau \in \mathbb{C}$ avec $\Im m\ \tau > 0$, 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 $\tau \in \mathbb{H} = \{z \in \mathbb{C} | \Im m\ \tau > 0\}$

c. Soit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z})$ 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 16*. ▽ *(Fonction $\wp$ de Weierstrass).* Considérons la fonction

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

a. Montrer que la série est convergente et que $\wp$ est une fonction holomorphe en dehors de l'ensemble $\{m + n\tau | m, n \in \mathbb{Z}\}$.

b. Calculer $\wp(z + m + n\tau)$.

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

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

convolution multiplicative de f et g.

On dit qu'une fonction $f \in C$ est *multiplicative* (respectivement *strictement multiplicative*) si $f(mn) = f(m)f(n)$ pour tous $m, n \in \mathbb{N}^*$ tels que $\text{pgcd}(m, n) = 1$ (respectivement pour tous $m, n \in \mathbb{N}^*$)

a. Montrer que la convolution est commutative et associative.

b. Trouver une fonction $\varepsilon \in C$ telle que $f \star \varepsilon = f$.

c. Décrire toutes fonctions $f \in C$ inversibles par rapport à la convolution.

d. Monter que l'espace de fonctions multiplicatives est stable par rapport à la convolution. Est-ce que l'espace de fonctions strictement multiplicatives en est aussi ?

e. 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.

f. Soit $g \in C$. Trouver la fonction $f \in C$ telle que $g(n) = \sum_{d|n} f(d)$.

g. Soit $\varphi \in C$ la fonction définie par $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$. On appelle φ *l'indicatrice d'Euler*. Calculer $\sum_{d|n} \varphi(d)$.

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 $n \to \infty$. On notera par $C' \subset C$ l'espace de fonctions de croissance polynomiale.

Pour $f \in C'$ on pose

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

a. Montrer que C' est fermé par rapport à la convolution.

b. Montrer que $L(s, f)$ est une fonction holomorphe pour $\Re e(s)$ assez grand.

c. Exprimer $L(s, f \star g)$ en termes de $L(s, f)$ et $L(s, g)$.

d. Calculer $L(s, \mu)$ et $L(s, \varphi)$ en termes de $\zeta(s) = L(s, 1)$, ou φ est l'indicatrice d'Euler et μ - la fonction de Möbius.

e. Soit $f \in C'$ une fonction multiplicative. Exprimer $L(s, f)$ comme un produit infini. La même question pour une fonction strictement multiplicative.

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

a. Calculer $\sum_{d|n} \lambda(d)$.

b. 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

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

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

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

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 $(n_1,\dots,n_k,n)=1$.

a. Exprimer $J_k(n)$ en termes de diviseurs premiers de n.

b. Calculer $\sum_{d|n} J_k(n)$.

c. Calculer la série de Dirichlet $L(s,J_k)$.

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. ▽ *Formule de Perron.* Calculer les intégrales

a. $\dfrac{1}{2\pi i}\displaystyle\int_{c-i\infty}^{c+i\infty} L(s,f)x^s\frac{ds}{s}$,

b* $\dfrac{1}{2\pi i}\displaystyle\int_{c-i\infty}^{c+i\infty} \frac{\zeta'(s)}{\zeta(s)}x^s\frac{ds}{s}$.

pour $x\in\mathbb{R}_{>0}$ et c assez grand afin que l'intégrale converge.

Exercice 25* ▽ Les *nombres de Bernoulli* B_k sont défini par le développement

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

a. Calculer B_0, B_1 B_2, B_4 et B_k pour $k>1$ impaires.

b. Trouver le développement en série de Taylor de la fonction.

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

c. Exprimer $\zeta(2k)$, $k=1,2,\dots$ en termes de nombres de Bernoulli.

d. Utilisant l'équation fonctionnelle $\zeta^*(s)=\zeta^*(1-s)$ où

$$\zeta^*(s)=\pi^{-s/2}\Gamma(s/2)\zeta(s)=\zeta(s)\int_{-\infty}^{\infty}e^{-\pi t^2}|t|^{s-1}dt$$

exprimer $\zeta(-k)$, $k=1,2,\dots$ en termes de nombres de Bernoulli. En particulier calculer $\zeta(-1)$.

e. Exprimer $S_m(n)=\sum_{i=0}^{n} i^m$ en termes de nombres de Bernoulli. *Indication :* Utiliser la formule d'Euler-Maclaurin :

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

où $f^{(-1)}(z):=\int_0^z f(t)dt$.

Exercice 26. ▽

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 27⁑ ▽ 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 28. ▽ Trouver le résidu $\operatorname*{Res}_{s=1} L(s,\chi)ds$, où χ est un caractère de Dirichlet

a. non-trivial

b. ▼ trivial

modulo N.

Exercice 29. ▽ Trouver les limites

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

où φ est l'indicatrice d'Euler.

Exercice 30⁑ ▽▼ 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

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

Exercice 31⁑ ▽ Trouver le produit infini

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

Reponses :

2. c : (a,b) ; 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, (24), $(2,12)$, $(2,2,6)$; d : 25.
5. c : p^{e-1}.
8. 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 $\zeta = \exp \pi i/3$, c : $\chi(x) = (-1)^{\frac{x-1}{2}}$ si $p \neq 2$, $\chi_1(x) = (-1)^{\frac{x-1}{2}}$, $\chi_2(x) = (-1)^{\frac{x^2-1}{8}}$, $\chi_3 = \chi_1\chi_2$ si $p = 2$.
10. b : $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 \text{ if } p = 1 \mod 4 \\ -1 \text{ sinon} \end{cases}$, c : $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 \text{ if } p = \pm 1 \mod 8 \\ -1 \text{ sinon} \end{cases}$
11. $\left(\frac{a}{p}\right) = 1$ si $p \neq 2$; $a = 1 \mod 4$ si $p = 2$, $k = 2$; $a = 1 \mod 8$ si $p = 2$, $k > 2$.
12. b : $\sum_x \chi_1(x)\chi_2(1-x)$; c : $\chi(-1)p$; d : $\sqrt{p}$; g :1,-1.
15. c : $(c\tau + d)^{-2s}E(s,\tau)$, $(c\tau + d)^{-2k}E_{2k}(\tau)$.
16. b : $\wp(z)$.
17. b : $\begin{cases} 1 & n = 1 \\ 0 & \text{sinon} \end{cases}$; c : $f(1) \neq 0$; e : ε, 1 ; f : n, g : $g = \mu \star f$.
18. c : $L(s,f)L(s,g)$, d : $\zeta(s)^{-1}$, $\zeta(s-1)/\zeta(s)$.
19. a : $\begin{cases} 1 & n = m^2 \\ 0 & \text{sinon} \end{cases}$, b : $\dfrac{\zeta(2s)}{\zeta(s)} = \prod_p \dfrac{1}{1+p^{-s}}$.
20. $\zeta(s-k)\zeta(s)$.
21. a : $\zeta(2)^2/\zeta(4) = 5/2$, b : $\zeta(s_1)\cdots\zeta(s_r)/\zeta(s_1+\cdots+s_r)$.
22. a : $n^k\prod_{p|n}(1-p^{-k})$, b : n^k, d : $\zeta(s-k)/\zeta(s)$.
24. a : $\sum_{n<x} f_n$; b : $x - \sum_{\rho|\zeta(\rho)=0}\frac{x^\rho}{\rho} - \ln(2\pi) - \ln(1-x^{-2})$.
25. a :1, $-1/2$, $1/6$, $-1/30$, 0, b : $1 - \pi i z + \sum_{k=1}^{\infty}(-1)^k\frac{(2\pi)^{2k}}{(2k)!}z^{2k}$, c : $\zeta(2k) = (-1)^{k+1}\frac{(2\pi)^{2k}}{2(2k)!}B_{2k}$, d : $\zeta(-k) = \frac{(-1)^k}{k+1}B_{k+1}$, e : $\frac{1}{m+1}\left((n+1)^{m+1} + \sum_{l=1}^{m+1}B_l\binom{m+1}{l}(n+1)^{m+1-l}\right)$.
26. a : $\Re e(s) > 0$, b : $(1-2^{1-s})\zeta(s)$, c : 1
27. $2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$.
28. a : 0, b : $\frac{\varphi(N)}{N}$.
29. 1,0.
30. $1-\gamma$.
31. e^z.

Corrections :

3a.

Tous les groupes dans ce texte sont supposés abéliens.

Définition : Un *groupe libre* est un groupe isomorphe à $\mathbb{Z}^k$ pour un certain $k \in \mathbb{Z}_{\geq 0}$. Le nombre k s'appelle le *rang* du groupe libre.

Lemme 1. Tout sous-groupe d'un groupe abélien libre est libre.

Démonstration : Tous les sous-groupes de $\mathbb{Z}$ sont de la forme $N\mathbb{Z}$ et sont donc libres. Supposons le lemme démontré pour tous les groupes de rang $\leqslant k$. Montrons que tout sous-groupe G de $\mathbb{Z}^{k+1}$ est libre.

Soit p la projection $\mathbb{Z}^{k+1} \to \mathbb{Z}$ sur la première coordonnée. Alors $p(G)$ est un sous-groupe de $\mathbb{Z}$, donc de la forme $N\mathbb{Z}$.

Si $N = 0$, alors $G \subset \ker p = \mathbb{Z}^k$ et donc G est libre par hypothèse de récurrence.

Si $N \neq 0$, soit $x \in G$ tel que $p(x) = N$. Tout élément $g \in G$ s'écrit $g = x\dfrac{p(g)}{N} + y$, où $y \in \ker p \cap G$.

Le groupe $\ker p \cap G$ est libre par hypothèse. Donc G est somme directe de deux groupes libres, et est donc libre.

—

Définition : Soit $\mathcal{A} : G_1 \to G_2$ un homomorphisme de groupes abéliens. Le *conoyau* de $\mathcal{A}$ (notation $\operatorname{coker}\mathcal{A}$) est le quotient $G_2/\operatorname{Im}(\mathcal{A})$.

Observation : Tout groupe fini est l'image homomorphe d'un groupe libre. Donc tout groupe fini G est isomorphe au conoyau d'une application $A : \mathbb{Z}^k \to \mathbb{Z}^n$.

Observation : Tout homomorphisme $A : \mathbb{Z}^k \to \mathbb{Z}^n$ est donné par $(n_1, \ldots, n_k)^\intercal \mapsto A(n_1, \ldots, n_k)^\intercal$, où A est une matrice $n \times k$ à coefficients entiers.

—

Lemme 2 : Soient $X : \mathbb{Z}^k \to \mathbb{Z}^k$ et $Y : \mathbb{Z}^n \to \mathbb{Z}^n$ deux automorphismes (c'est-à-dire des homomorphismes inversibles, donc donnés par des matrices inversibles à coefficients entiers). Alors $\operatorname{coker}(XAY)$ est isomorphe à $\operatorname{coker} A$.

Démonstration : $\operatorname{coker}(XAY) = \mathbb{Z}^n/XAY(\mathbb{Z}^k) = \mathbb{Z}^n/XA(\mathbb{Z}^k) = X(\mathbb{Z}^n)/XA(\mathbb{Z}^k) = \mathbb{Z}^n/A(\mathbb{Z}^k) = \operatorname{coker} A$.

—

Définition : On dit que deux matrices rectangulaires à coefficients entiers A et B sont *équivalentes* s'il existe deux matrices carrées à coefficients entiers inversibles X et Y telles que $B = XAY$.

Définition : Une matrice rectangulaire à coefficients entiers $D = (d_i^j)$ est une *matrice de Smith* si d_i^i divise d_{i+1}^{i+1} pour tout i et $d_i^j = 0$ pour tout $i \neq j$. On notera les éléments d_j^i juste par d_i.

Théorème : Pour toute matrice A à coefficients entiers, il existe deux matrices carrées inversibles X et Y, également à coefficients entiers, telles que $D = XAY$ soit une matrice de Smith.

—

Lemme 3 : Soit $A = \begin{pmatrix} a_1^1 & \cdots & a_1^n \\ \vdots & \ddots & \vdots \\ a_k^1 & \cdots & a_k^n \end{pmatrix}$ et $c_1 = \operatorname{pgcd}(a_i^j)$. Alors A est équivalente à une matrice

$B = \begin{pmatrix} c_1 & 0 & \cdots & 0 \\ 0 & b_2^2 & \cdots & b_2^n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & b_k^2 & \cdots & b_k^n \end{pmatrix}$ où c_1 divise tous les b_i^j. En itérant cette construction, on voit que toute matrice est équivalente à une matrice de Smith.

Démonstration : Considérons l'ensemble des matrices équivalentes à A et choisissons-en une dont l'élément a_1^1 est positif et minimal. Montrons qu'il est égal à $c_1 = \operatorname{pgcd}(a_i^j)$.

(A) Montrons d'abord que c_1 divise tous les éléments de la première ligne. Soit $a_1^j = c_1 s + r$ avec $0 \leqslant r < c_1$. En soustrayant de la j-ième colonne la première colonne multipliée par s, puis en échangeant la première et la j-ième colonne, on obtient r à la place de a_1^1. Donc $r = 0$, sinon a_1^1 ne serait pas minimal positif. Ainsi c_1 divise a_1^j pour tout j.

(B) De même, on montre que c_1 divise a_i^1 pour tout i. En soustrayant des multiples appropriés de la première colonne des autres colonnes et de la première ligne aux autres lignes, on obtient la matrice B.

(C) Si l'on ajoute une ligne de la matrice B à la première, on voit que tous les éléments de cette ligne sont divisibles par c_1, sinon on contredit l'argument (A).

Le lemme et le théorème sont ainsi démontrés.

—

Lemme 4 : Toute matrice A est équivalente à une unique matrice de Smith.
Démonstration : Soit $c_l = \text{pgcd}(\text{mineurs } l \times l \text{ de } A)$. Les nombres c_l sont invariants par équivalence. On a alors $c_l = d_1 d_2 \cdots d_l$, ce qui montre que les d_l sont entièrement déterminés par la matrice A.

—

Conséquence : Tout groupe abélien fini est isomorphe à une somme directe unique $\bigoplus_l \mathbb{Z}/d_l\mathbb{Z}$, où d_l divise d_{l+1} car c'est le conoyau de la matrice de Smith.

—

Remarque : La démonstration peut être généralisée automatiquement aux matrices à coefficients dans l'anneau des polynômes en une variable. Plus généralement à coefficients dans un anneau principal.

10c Soit $\zeta = \frac{1+i}{\sqrt{2}} = e^{\pi i/4}$. Évidemment $\zeta^8 = 1$ et $\zeta + \zeta^{-1} = \sqrt{2}$. Donc

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \mod p \equiv (\zeta + \zeta^{-1})^{p-1} \mod p \Rightarrow$$
$$\Rightarrow \left(\frac{2}{p}\right)(\zeta + \zeta^{-1}) \equiv (\zeta + \zeta^{-1})^p \mod p \equiv (\zeta^p + \zeta^{-p}) \mod p$$

Alors $\left(\frac{2}{p}\right) = 1$ si $p = \pm 1 \mod 8$ et $\left(\frac{2}{p}\right) = -1$ si $p = \pm -1 \mod 8$ car $\zeta^3 = \zeta^4\zeta^{-1} = -\zeta^{-1}$.

28b. Soit $L_n(s) = \sum_{k|(k,n)=1} k^{-s}$. Alors $\zeta(s) = \sum_k k^{-s} = \sum_{d|n} \sum_{k\,|\,(k,n)=d} k^{-s} = \sum_{d|n} \sum_{k|(k,n/d)=1} (kd)^{-s} = \sum_{d|n} d^{-s} L_{n/d}(s) = n^{-s} \sum_{d|n} (n/d)^s L_{n/d}(s)$. Donc $n^s\zeta(s) = \sum_{d|n} d^s L_d(s)$, d'ou
$n^s L_n(s) = \zeta(s) \sum_{d|n} d^s \mu(n/d)$. Donc $\operatorname{Res}_{s=1} L_n(s)ds = n^{-1} \sum_{d|n} d\mu(n/d) \operatorname{Res} \zeta(s)ds = \phi(n)/n$.

30.
$$\int_1^\infty \frac{\{x\}}{x^2}dx = \int_1^\infty \frac{x - \lfloor x \rfloor}{x^2}dx = \lim_{N\to\infty}\left(\int_1^N \frac{dx}{x}dx + \int_1^N \lfloor x \rfloor d\frac{1}{x}\right) = \lim_{N\to\infty}\left(\ln N + \lim_{\varepsilon\to 0}\left(\frac{\lfloor x \rfloor}{x}\Big|_{1-\varepsilon}^{N+\varepsilon} - \int_{1-\varepsilon}^{N+\varepsilon} \frac{1}{x} d\lfloor x \rfloor\right)\right)$$
$$\lim_{N\to\infty} \ln N + 1 - \sum_{k=1}^{N} \frac{1}{N} = 1 - \gamma.$$