TD 11 : Séries de Dirichlet, courbes elliptiques et formes modulaires

Olivier de Gaay Fortman · 16 - 20 mai 2022

1 Séries de Dirichlet

Exercice 1

Montrer les égalités suivantes, où chaque fois $s = \sigma + it$ avec $\sigma > 1$:

1.
$$\zeta(s) = s \int_1^\infty \frac{\lfloor x \rfloor}{x^{s+1}} dx;$$

2.
$$\sum_p \frac{1}{p^s} = s \int_1^\infty \frac{\pi(x)}{x^{s+1}} dx, \quad \pi(x) = \sum_{p \leq x} 1;$$

3.
$$\frac{1}{\zeta(s)} = s \int_1^\infty \frac{M(x)}{x^{s+1}} dx, \quad M(x) = \sum_{n \leq x} \mu(n), \quad \mu(n) = \begin{cases} 1 & \text{si} \quad n = 1 \\ (-1)^k & \text{si} \quad n = \prod_{i=1}^k p_i \mid p_i \neq p_j \\ 0 & \text{sinon.} \end{cases}$$

4.
$$-\frac{\zeta'(s)}{\zeta(s)} = s \int_1^\infty \frac{\psi(x)}{x^{s+1}} dx, \quad \psi(x) = \sum_{n \leq x} \Lambda(n);$$

5.
$$L(s, \chi) = s \int_1^\infty \frac{A(x)}{x^{s+1}} dx, \quad A(x) = \sum_{n \leq x} \chi(n), \quad \Lambda(n) = \begin{cases} \log(p) & \text{si} \quad n = p^m \mid m \ \geq 1 \\ 0 & \text{sinon.} \end{cases}$$

†Exercice 2

Supposons que la série $\sum_{n=1}^\infty f(n)$ converge vers $A \in \mathbb{C}$, et soit $A(x) = \sum_{n \leq x} f(n)$.

1. Montrer que les séries de Dirichlet $F(s) = \sum_{n=1}^\infty f(n) n^{-s}$ convergent, pour tout s avec $\sigma > 0$, et que
$$\sum_{n=1}^\infty \frac{f(n)}{n^s} = A - s \int_1^\infty \frac{R(x)}{x^{s+1}} dx, \quad R(x) = A - A(x).$$

2. En déduire que $F(\sigma) \to A$ quand $\sigma \to 0^+$.
3. Soit $\sigma > 0$ et $N \geq 1$ et un entier. Monter que

$$F(s) = \sum_{n=1}^{N} \frac{f(n)}{n^s} - \frac{A(N)}{N^s} + s \int_N^\infty \frac{A(y)}{y^{s+1}} dy.$$

4. Écrivons $s = \sigma + it$, prenons $N = 1 + [|t|]$ dans la partie 3. Montrer que

$$|F(\sigma + it)| = O(|t|^{1-\sigma}), \quad 0 < \sigma < 1.$$

Exercice 3

On définit $\xi(s) = \frac{s(s-1)}{2} \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s)$. On rappelle que ξ est entière et vérifie l'équation fonctionnelle $\xi(s) = \xi(1-s)$.

1. Montrer que pour tout s tel que $\Re s > 0$ et $s \neq 1$, on a

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{+\infty} \frac{\{x\}}{x^{s+1}} \mathrm{d}x$$

où $\{x\}$ désigne la partie fractionnaire de x.

2. En déduire que pour tout $\epsilon > 0$, il existe des constantes $A, B > 0$ telles que pour tout $s \in \mathbb{C}$ on ait

$$|\xi(s)| \leq A \exp\left(B |s|^{1+\epsilon}\right).$$

Montrer que l'on ne peut pas prendre ici $\epsilon = 0$.

3. En déduire que la fonction ζ a une infinité de zéro dans la bande $\{s \in \mathbb{C} : 0 \leq \Re s \leq 1\}$.

2 Formes modulaires

Exercice 4

Soit f une forme modulaire de poids $2k$, $k \geq 2$. Utilisons le théorème suivant :

Théorème (Hecke)**.** *Si f est parabolique, alors $a_n = O(n^k)$.*

Prouver que, si f n'est pas parabolique, l'ordre de grandeur de a_n est n^{2k-1}.

Exercice 5

Soit $f = \sum_{n \geq 0} a_n q^n$ une forme modulaire de poids $2k$, $k > 0$. Définissons ses séries de Dirichlet associées :

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \quad s \in \mathbb{C}. \tag{1}$$

Montrer que $L(f, s)$ converge absolument pour $\Re(s) > 2k$.

3 Courbes Elliptiques

Définition 6

Une *courbe elliptique* E est une équation de la forme

$$E\colon \{F = Y^2Z - X^3 + aXZ^2 + bZ^3 = 0\}, \quad a, b \in \mathbb{C} \mid 4a^3 + 27b^2 \neq 0. \tag{2}$$

Le *discriminant* de E est la valeur $\Delta = 4a^3 + 27b^2 \in \mathbb{C}^*$.

Exercice 7

On rappelle que le plan projectif complexe $\mathbb{P}^2(\mathbb{C})$ est le quotient de $\mathbb{C}^3 - \{(0,0,0)\}$ par l'action des homothéties $\mathbb{C}$-linéaires de $\mathbb{C}^3$. Écrivons $[x : y : z] \in \mathbb{P}^2(\mathbb{C})$ pour la classe de $\mathbb{C}^*$-équivalence du point $(x, y, z) \in \mathbb{C}^3 - \{(0,0,0)\}$.

Montrer que, pour une courbe elliptique E, bien que l'application $F : \mathbb{C}^3 \to \mathbb{C}$ ne descend pas en une application $F\colon \mathbb{P}^2(\mathbb{C}) \to \mathbb{C}$, le lieu de zéros suivant est bien défini :

$$E(\mathbb{C}) \coloneqq \{[x : y : z] \in \mathbb{P}^2(\mathbb{C}) \mid F(x, y, z) = 0\} \subset \mathbb{P}^2(\mathbb{C}).$$

Montrer que le groupe $\mathrm{PGL}_3(\mathbb{C}) = \mathrm{GL}_3(\mathbb{C})/\mathbb{C}^*$ agit sur $\mathbb{P}^2(\mathbb{C})$. On dit que deux courbes elliptiques E_i $(i = 1, 2)$ sont *isomorphes* s'il existe $\gamma \in \mathrm{PGL}_3(\mathbb{C})$ tel que $\gamma E_1(\mathbb{C}) = E_2(\mathbb{C})$.

Exercice 8

On se donne $\tau \in \mathbb{H}$. Définissons une équation E_τ comme

$$E_\tau\colon Y^2Z = 4X^3 - g_2(\tau)XZ^2 - g_3(\tau)Z^3.$$

1. Montrer qu'après un changement de variables, E_τ définit une courbe elliptique.
2. Montrer que E_τ s'identifie avec l'ensemble des solutions $(x, y) \in \mathbb{C}^2$ de l'équation

   $$y^2 = 4x^3 - g_2(\tau)x - g_3(\tau)$$

   auxquelles on a ajouté un point à l'infini que l'on identifiera.
3. Notons $\wp$ la fonction de Weierstrass associée au réseau Λ_τ. Montrer que, sous l'identification de la partie 2, l'application $z \mapsto (\wp(z), \wp'(z))$ induit une bijection

   $$\mathbb{C}/\Lambda_\tau \xrightarrow{\sim} E_\tau$$

   avec la convention que 0 est envoyé sur le point à l'infini.
4. Par la question précédente, E_τ hérite une structure de groupe abélien de celui de $\mathbb{C}/\Lambda_\tau$. Montrer que pour $y \in \mathbb{C} \setminus \Lambda_\tau$, la fonction suivante est identiquement nulle :

   $$z \mapsto \begin{vmatrix} \wp(z) & \wp'(z) & 1 \\ \wp(y) & \wp'(y) & 1 \\ \wp(z+y) & -\wp'(z+y) & 1 \end{vmatrix}.$$

Remarque. Rappelons que $\mathcal{L}$ était défini comme l'ensemble des réseaux Λ dans $\mathbb{C}$. Ci-dessus, on a défini une fonction $\mathbb{C}^* \setminus \mathcal{L} \to \{\text{courbes elliptiques}\} / \cong$. Il se trouve que cette fonction est *bijective*.

Exercice 9

Soit E une courbe elliptique, défini par un polynome $F \in \mathbb{Q}[X, Y, Z]$. Montrer qu'il existe $c \in \mathbb{Q}$ telle que le changement de variables $X \mapsto X/c^2$, $Y \mapsto Y/c^3$ donne une courbe elliptique $Y^2Z = X^3 + aXZ^2 + bZ^3$ avec $a, b \in \mathbb{Z}$. Montrer qu'on peut choisir $c \in \mathbb{Q}$ tel que $|\Delta|$ est minimal – on dit que l'équation est *minimale*.

Pour une telle équation minimale, et un nombre premier p, on obtient une équation $\bar{E} : Y^2Z = X^3 + \bar{a}XZ^2 + \bar{b}Z^3$; soit $\#\bar{E}(\mathbb{F}_p)$ le nombre de solutions de $\bar{E}$ dans $\mathbb{P}^2(\mathbb{F}_p)$.

Exercice 10

Continuous avec la notation de la question précédente. Soit p un nombre premier. Définissons $a_p = p + 1 - \#\bar{E}(\mathbb{F}_p)$. On admet le résultat suivant :

Théorème (Hasse)**.** *Les entiers a_p satisfont $|a_p| \leq 2\sqrt{p}$.*

Définissons

$$\epsilon(p) = \begin{cases} 1 & \text{if } p \not| N, \\ 0 & \text{if } p \,|N; \end{cases} \qquad \text{et ensuite} \quad L(E, s) = \prod_{p \text{ premier}} \frac{1}{1 - a_p p^{-s} + \epsilon(p) p^{1-2s}}.$$

Montrer que $L(E, s)$ définit une fonction holomorphe sur $\{s \in \mathbb{C} \mid \Re(s) > 3/2\}$.

Remarque. Les séries de Dirichlet forment le lien entre les courbes elliptiques et les formes modulaires. Ce lien est montré par Wiles afin de prouver le dernier théoréme de Fermat. Pour être plus précis : plus généralement que ce que l'on a fait dans le cours, on peut définir, pour n'importe quel sous-groupe d'indice fini $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, une *forme modulaire de poids $2k$ pour Γ* comme une fonction holomorphe $f : \mathbb{H} \to \mathbb{C}$ telle que

1. pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, on a $f(\gamma z) = (cz + d)^{2k} f(z)$;
2. la fonction $f \circ \gamma$ est holomorphe à l'infini, pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Pour un entier $N \geq 0$, le groupe

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod N \right\}$$

est d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$ et il se trouve que le résultat de l'Exercice 5 se généralise : les séries $L(f, s)$ de Dirichlet, associées à f comme dans l'Exercice 5, convergent pour $\Re(s) > k + 1$. On se demande si l'on obtient des séries de Dirichlet différentes en utilisant soit des courbes elliptiques sur $\mathbb{Q}$ (c.f. Exercice 10), soit des formes modulaires pour des groupes $\Gamma_0(N)$, $N \in \mathbb{N}$. La réponse à cette question est le fameux théorème de modularité :

Théorème (Modularité)**.** *Soit E une courbe elliptique sur $\mathbb{Q}$. Alors il existe $N \in \mathbb{Z}_{\geq 0}$ et une forme modulaire f de poids 2 pour $\Gamma_0(N)$ telle que $L(f, s) = L(E, s)$.*