Fonctions elliptiques, séries théta

Soit Λ un réseau de $\mathbb{R}^2$; toute fonction entière Λ-périodique est constante. Donc si nous voulons obtenir des fonctions intéressantes, il faut soit autoriser des pôles soit être moins exigeants sur la périodicité. Nous allons étudier sommairement ces deux possibilités.

1 Fonctions elliptiques et courbes elliptiques

Exercice 1. *Une fonction f est dite* ***elliptique*** *par rapport à un réseau Λ si c'est une fonction méromorphe sur $\mathbb{C}$ qui est Λ-périodique, i.e.*

$$f(z+\omega) = f(z)$$

pour tout $z \in \mathbb{C}$ et tout $\omega \in \Lambda$.

(1) Montrer que f est Λ-périodique si et seulement si $f(z+\omega_1) = f(z) = f(z+\omega_2)$ pour tout $z \in \mathbb{C}$ avec $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Par ailleurs si f n'a pas de poles, montrer que f est constante.

(2) Soit f une fonction elliptique par rapport à Λ et soit P un parallélogramme fondamental.

(i) On suppose que f n'a pas de poles sur le bord ∂P de P. Montrer alors que la somme des résidus de f dans P est égale à 0.

(ii) On suppose que f n'a ni zéros ni poles sur ∂P. On note a_i les zéros et poles de f dans P et on note m_i la multiplicité de f en a_i. Montrer que

$$\sum_i m_i = 0$$

$$\sum_i m_i a_i \equiv 0 \mod \Lambda$$

(3) On considère la fonction $\mathfrak{P}$ de Weierstrass:

$$\mathfrak{P}_\Lambda(x) = x^{-2} + \sum_{\omega \in \Lambda - 0} [(x-\omega)^{-2} - \omega^{-2}]$$

(i) Montrer que pour tout $s > 2$ la somme $\sum_{\omega\in\Lambda-0} \frac{1}{|\omega|^s}$ converge.

(ii) En déduire que la série qui définit $\mathfrak{P}$ converge uniformément sur tout compact de $\mathbb{C}$ ne contenant pas les points du réseau Λ.

(iii) En considérant $\mathfrak{P}'(x) = -2\sum_{x\in\Gamma}(x-\omega)^{-3}$, montrer que $\mathfrak{P}$ est elliptique par rapport à Λ.

(4) L'ensemble des fonctions elliptiques par rapport à Λ est un corps sur $\mathbb{C}$; on veut montrer que celui-ci est engendré par $\mathfrak{P}$ et $\mathfrak{P}'$.

(i) Soit f elliptique paire et soit $u \equiv -u \mod \Lambda$ avec $u \not\equiv 0 \mod \Lambda$. Montrer que $g(z) := \mathfrak{P}(z) - \mathfrak{P}(u)$ a un zéro d'ordre 2. En déduire que f a un zéro d'ordre pair en u. Traitez le cas de $u \equiv 0 \mod \Lambda$ en considérant $g = 1/\mathfrak{P}$.

(ii) Soit $(u_i)_{1\le i\le r}$ un famille de points contenant un représentant de chaque classe $(u, -u) \mod \Lambda$ où f a un pole ou un zéro autre que la classe de Λ. On pose

$$m_i = \mathrm{ord}_{u_i} f \text{ si } 2u_i \not\equiv 0 \mod \Lambda$$

$$m_i = \frac{1}{2}\mathrm{ord}_{u_i} f \text{ si } 2u_i \equiv 0 \mod \Lambda$$

Montrer, en utilisant le théorème de Liouville, que f est égal à une constante fois $\prod_{i=1}^r [\mathfrak{P}(z) - \mathfrak{P}(u_i)]^{m_i}$.

(iii) En déduire que $\mathbb{C}(\mathfrak{P})$ est le corps des fonctions elliptiques paires par rapport à Λ, puis que $\mathbb{C}(\mathfrak{P},\mathfrak{P}')$ est le corps des fonctions elliptiques par rapport à Λ.

(5) On veut montrer que les points $(\mathfrak{P}(z),\mathfrak{P}'(z))$ appartiennent à une cubique d'équation $y^2 = 4x^3 - g_2x - g_3$ avec $\Delta = g_2^3 - 27g_3^2 \neq 0$.

(i) Montrer que

$$\mathfrak{P}(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)s_{2n+2}(\Lambda)z^{2n}$$

avec $s_n(\Lambda) = s_n = \sum_{\omega\neq 0}\frac{1}{\omega^m}$.

(ii) En posant $g_2 = 60s_4$ et $g_3 = 140s_6$, montrer que $(\mathfrak{P}(z),\mathfrak{P}'(z))$ appartiennent à une cubique d'équation $y^2 = 4x^3 - g_2x - g_3$.

(iii) On pose $e_1 = \mathfrak{P}(\omega_1/2)$, $e_2 = \mathfrak{P}(\omega_2)$ et $e_3 = \mathfrak{P}(\frac{\omega_1+\omega_2}{2})$. Montrer que modulo Γ, $\mathfrak{P}'$ a trois racines simples à savoir $\omega_1/2$, $\omega_2/2$ et $(\omega_1+\omega_2)/2$. En déduire que

$$(\mathfrak{P}')^2 = 4(\mathfrak{P}-e_1)(\mathfrak{P}-e_2)(\mathfrak{P}-e_3)$$

avec $\Delta = g_2^3 - 27g_3^2 \neq 0$.

(iv) En déduire que

$$x = \frac{1}{2}\int_{\infty}^{\mathfrak{P}(x)}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy \mod \Gamma$$

avec $\omega_1 = \int_{\infty}^{e_1}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$ et $\omega_2 = \int_{e_1}^{e_2}[(y-e_1)(y-e_2)(y-e_3)]^{-1/2}dy$.

(v) Montrer que l'équation $y^2 = x^3 - x$ correspond au réseau $\mathbb{Z}^2$ en utilisant l'égalité

$$\omega_1 = \int_0^1 (x-x^2)^{-1/2}dx = \int_1^{\infty}(x^3-x)^{-1/2}dx = \omega_2/i$$

que l'on montrer via le changement de variable $x \mapsto 1/x$.

Exercice 2. ***Loi d'addition*** *Etant donné des nombres complexes g_2, g_3 on peut se demander s'il existe un réseau pour lequel ce sont les invariants associés comme dans l'exercice précédent. La réponse est oui. On considère la courbe projective A d'équation*

$$uy^2 = 4x^3 - g_2xu^2 - g_3u^3$$

de point infini $(0,0,1)$ qui est l'image des points de Λ par l'application $z \mapsto (1,\mathfrak{P}(z),\mathfrak{P}'(z))$.

(1) Montrer que l'application ci-dessus induit une bijection $\mathbb{C}/\Lambda - 0 \longrightarrow A_{\mathbb{C}} - \{\infty\}$, où $A_{\mathbb{C}}$ désigne les points complexes de la cubique A.

(2) L'ensemble $\mathbb{C}/\Lambda$ est naturellement muni d'une structure de groupe; on veut exprimer celle-ci sur $A_{\mathbb{C}}$. Nous allons montrer que si $P_1 = (1,x_1,y_1)$ et $P_2 = (1,x_2,y_2)$ alors $P_3 = P_1 + P_2 = (1,x_3,y_3)$ s'exprime avec des fonctions rationnelles en x_1,x_2,y_1,y_2. Géométriquement on procède comme dans le dessin suivant: la droite (P_1P_2) intersecte $A_{\mathbb{C}}$ en un troisième point $Q_3 = -P_3$ et P_3 est le symétrique de Q_3 par rapport à l'axe des x.

(i) Soient $u_1,u_2 \in \mathbb{C}-\Lambda$ et supposons $u_1 \not\equiv u_2 \mod \Lambda$. Soient $a,b \in \mathbb{C}$ tels que

$$\mathfrak{P}'(u_1) = a\mathfrak{P}(u_1) + b$$

$$\mathfrak{P}'(u_2) = a\mathfrak{P}(u_2) + b$$

Montrer que $g(z) = \mathfrak{P}'(z) - a\mathfrak{P}(z) - b$ a 3 zéros comptés avec leur multiplicités. A quelle condition n'a-t-ont que 2 zéros distincts?

(ii) On suppose que gz a 3 zéros distincts. En notant u_3 le troisième, montrer que $u_3 \equiv -(u_1+u_2) \mod \Lambda$. En déduire que

$$x_3 = -x_1 - x_2 + \frac{1}{4}\Big(\frac{y_1 - y_2}{x_2 - x_2}\Big)^2.$$

(iii) Pour $u_1 \equiv u_2 \mod \Lambda$ montrer que

$$\mathfrak{P}(2u) = -2\mathfrak{P}(u) + \frac{1}{4}\Big(\frac{\mathfrak{P}"(u)}{\mathfrak{P}'(u)}\Big)^2.$$

Exercice 3. ***Une introduction à la géométrie algébrique***

(1) En vous appuyant sur la classification des coniques projectives de $\mathbb{P}^2_{\mathbb{R}}$, montrez qu'une conique non dégénérée C non vide de $\mathbb{P}^2_{\mathbb{R}}$ est projectivement équivalente à la courbe $XZ = Y^2$.

Montrez que cette courbe admet un paramétrage par $\mathbb{P}^1_{\mathbb{R}}$ via l'application qui à (U, V) associe (U^2, UV, V^2). Quelle est l'application inverse?

(2) ***Cas simples du théorème de Bézout***

(i) Soit

$$F(U, V) = a_d U^d + a_{d-1} U^{d-1} V + \cdots + a_0 V^d$$

un polynôme homogène non nul de degré d en 2 variables à coefficients dans un corps k. On lui associe le polynôme en une variable $f(u) = F(u, 1)$ et on définit la multiplicité d'un zéro (u, v) de F dans $\mathbb{P}^1_k$ comme la multiplicité de u/v dans f si $v \neq 0$ et sinon en $(1, 0)$ comme l'entier $d - \deg f$.

Montrer que F a au plus d zéros dans $\mathbb{P}^1_k$ comptés avec multiplicités.

(ii) Soit $L \subset \mathbb{P}^2_k$ une droite et $D \subset \mathbb{P}^2_k$ une courbe définie par une équation $G(X, Y, Z) = 0$ où G est un polynôme homogène de degré d en X, Y, Z. On suppose $L \nsubseteq D$. Montrer que le cardinal de $L \cap D$ est inférieur ou égal à d.

(iii) Même hypothèse qu'en (ii) en remplaçant L par une conique non dégénérée C: montrer que le cardinal de $C \cap D$ est inférieur ou égal à $2d$.

Remarque: On peut définir une notion de multiplicité d'une intersection en un point de sorte que les résultats précédents soient vrais en comptant avec multiplicité. En outre si k est algébriquement clos, on a alors égalité. Le théorème de Bézout concerne des courbes C et D de degré n et m: leur intersection est alors nm, en comptant les multiplicités et en travaillant sur un corps algébriquement clos.

(3) ***L'espace des coniques*** *Dans la suite on note $S_d(k)$ l'espace des polynômes homogènes de degré d à coefficients dans k, en les variables X, Y, Z. Etant donnés des points $P_1, \cdots, P_r$ de $\mathbb{P}^2_k$, on notera $S_d(P_1, \cdots, P_n)$ le sous-ensemble de $S_d(k)$ constitué des éléments F qui s'annulent sur les P_i.*

(i) Soient $P_1, \cdots, P_5 \in \mathbb{P}^2_{\mathbb{R}}$ des points distincts tels que 4 quelconques ne sont pas colinéaires. Montrer qu'il existe au plus une conique passant par ces 5 points.

(ii) Soit $n \geq 5$ et soient $P_1, \cdots, P_n$ des points tels que 4 quelconques ne sont jamais colinéaires. Montrer alors que l'ensemble des formes quadratiques qui s'annulent sur ces poitns est de dimension $6 - n$.

(iii) ***Un pinceau de coniques*** *est une famille de la forme*

$$C_{\lambda,\mu} := (\lambda Q_1 + \mu Q_2 = 0)$$

où Q_1 et Q_2 sont des coniques. On suppose que le pinceau possède au moins une conique dégénérée, montrer alors qu'elle en possède au plus 3. En outre si $k = \mathbb{R}$, montrer que le pinceau admet toujours une conique dégénérée.

(4) ***Cubiques: exemples***

(i) On considère la cubique de $\mathbb{R}^2$ définie par l'équation $y^2 = X^3 + x^2$. Donnez en une paramétrisation.

(ii) Même question avec la cubique $y^2 = x^3$.

(iii) Soit k un corps de caractéristique différente de 2 et soit $\lambda \in k$ avec $\lambda \neq 0, 1$. Montrer que pour si $f, g \in k(t)$ sont tels que $f^2 = g(g-1)(g-\lambda)$ alors $f, g \in k$. Quelle interprétation en donnez-vous sur la cubique $y^2 = x(x-1)(x-\lambda)$?

(5) ***Cas simples du Nullstellensatz****: soit k un corps infini et soit $F \in S_d(k)$ un polynôme homogène de degré d à coefficients dans k en les variables X, Y, Z.*

(i) Soit $L \subset \mathbb{P}^2_k$ une droite. Montrer que si F s'annule sur L alors $F = HF'$ où H est une équation de L et $F' \in S_{d-1}(k)$. En déduire que si $P_1, \cdots, P_n$ sont des points de $\mathbb{P}^2_k$ tels que $P_1, \cdots, P_a \in L$ et $P_{a+1}, \cdots, P_n \notin L$ avec $a > d$, alors

$$S_d(P_1, \cdots, P_n) = HS_{d-1}(P_{a+1}, \cdots, P_n)$$

(ii) Soit $C \subset \mathbb{P}^2_k$, une conique non dégénérée et non vide. Montrer que si F s'annule sur C alors $F = QF'$ où Q est une équation de C et $F' \in S_{d-2}(k)$. En déduire que si $P_1, \cdots, P_n$ sont des points de $\mathbb{P}^2_k$ tels que $P_1, \cdots, P_a \in C$ et $P_{a+1}, \cdots, P_n \notin C$ avec $a > 2d$, alors

$$S_d(P_1, \cdots, P_n) = QS_{d-2}(P_{a+1}, \cdots, P_n)$$

(iii) Soient $P_1, \cdots, P_8 \in \mathbb{P}^2_k$ des points distincts tels que 4 quelconques ne sont pas colinéaires et que 7 quelconques ne sont pas sur une conique non dégénérée. Montrer alors que $\dim S_3(P_1, \cdots, P_8) = 2$.
Indication*: on traitera séparément le cas où 3 points quelconques ne sont pas colinéaires et 6 quelconques ne sont pas sur une conique non dégénérée.*

(iv) Soient C_1, C_2 deux coniques dont l'intersection est 9 points distincts. Montrer que toute conique D qui passe par 8 d'entre eux passe aussi par le neuvième.

(6) ***Loi d'addition sur une conique****: soit $k \subset \mathbb{C}$ et $C \subset \mathbb{P}^2_k$ une cubique d'équation $F = 0$. On suppose que F est irréductible et que pour tout point $P \in C$, il existe une unique droite $L \subset \mathbb{P}^2_k$ telle que P est un zéro multiple de $F_{|L}$. On fixe un point $O \in C$ et on considère la construction suivante:*

Construction*: (a) Soit $A \in C$ et soit $\bar{A}$ le troisième point d'intersection de C avec la droite OA.*

(b) Pour $A, B \in C$ soit R le troisième point d'intersection de AB avec C et on définit $A + B$ comme étant égal à $\bar{R}$.

On veut montrer que l'on définit ainsi une loi de groupe abélien sur C avec O comme élément neutre.

(i) Montrer que la construction précédente est bien définie.

(ii) Montrer que O est bien un élément neutre et que la loi est commutative.

(iii) Montrer que l'inverse de A est le troisième point d'intersection de $\bar{O}A$ avec C.

(iv) ***Associativité****: soient A, B, C trois points de C; la construction de $(A+B)+C = \bar{S}$ utilise les 4 droite (cf. la figure (1)):*

$$L_1 = ABR, \quad L_2 = RO\bar{R}, \quad L_3 = C\bar{R}S, \quad L_4 = SO\bar{S}$$

La construction de $(B + C) + A = \bar{S}'$ utilise les 4 droites

$$M_1 = BCQ, \quad M_2 = QO\bar{Q}, \quad M_3 = A\bar{Q}S', \quad M_4 = S'O\bar{S}'$$

Il s'agit de prouver $\bar{S} = \bar{S}'$ ou de manière équivalente $S = S'$. On considère les deux cubiques

$$D_1 = L_1 + M_2 + L_3 \qquad D_2 = M_1 + L_2 + M_3$$

de sorte que

$$C \cap D_1 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\} \qquad C \cap D_2 = \{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S'\}$$

Conclure en supposant les 9 points $\{A, B, C, O, R, \bar{R}, Q, \bar{Q}, S\}$ distincts.

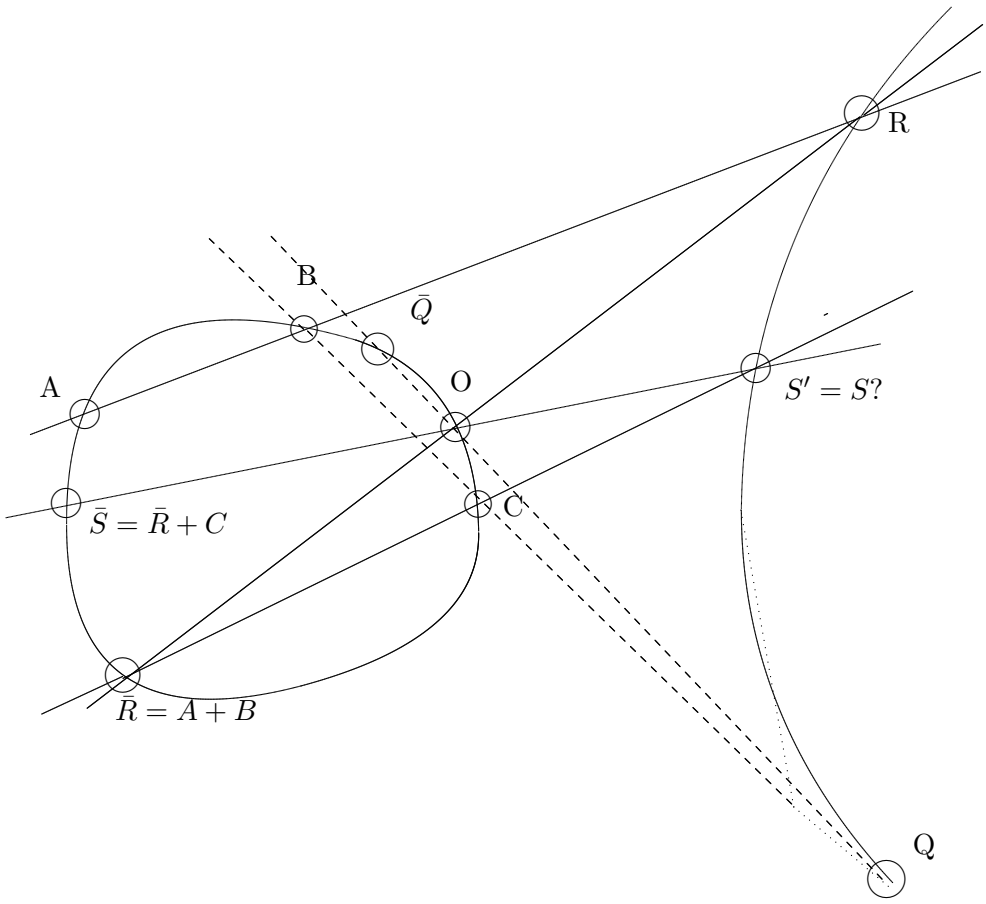

Figure 1: Loi d'addition sur une courbe elliptique

(v) *Conclure dans le cas général en utilisant un argument de continuité et en utilisant l'hypothèse* $k \subset \mathbb{C}$. *Remarque: On peut montrer le cas général pour tout* k *avec une bonne notion de multiplicité, ou bien en utilisant la topologie de Zariski.*

(vi) *Soit* $C \subset \mathbb{P}^2_k$ *une cubique possédant un point d'inflexion* P. *Montrer qu'un changement de coordonnées dans* $\mathbb{P}^2_k$ *permet de se ramener à une équation de la forme* ***normale****, i.e.*

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$$

Indication*: choisissez les coordonnées telles que* $P = (0, 1, 0)$ *et la droite d'inflexion* $Z = 0$.

(vii) ***Loi de groupe simplifiée****: on considère une cubique sous forme normale et on prend* $O = (0, 1, 0)$ *comme élément neutre. Montrer que l'on a les propriétés suivantes et retrouver la loi de groupe donnée par les fonctions de Weierstrass.*

(a) $C = \{O\} \cup C_0$, *où* $C_O : (y^2 = x^3 + ax + b)$ *est un courbe affine;*

(b) les droites passant par O *sont les droite projectives* $X = \lambda Z$ *et donc les droites affines* $x = \lambda$*;*

(c) $-P = \bar{P}$.

Remarque: Essayez de prouver ***le théorème de l'hexagone de Pascal****: Soit un hexagone* $ABCDEF$ *dans* $\mathbb{P}^2_k$ *dont les paires de cotés opposés se rencontrent aux points* P, Q, R. *On suppose les 9 points et les 6 droites distinctes. Montrer alors que*

$$ABCDEF \text{ sont sur une même conique non dégénérée} \Leftrightarrow PQR \text{ sont colinéaires}$$

Exercice 4. ***Méthode de factorisation de Lenstra****:*

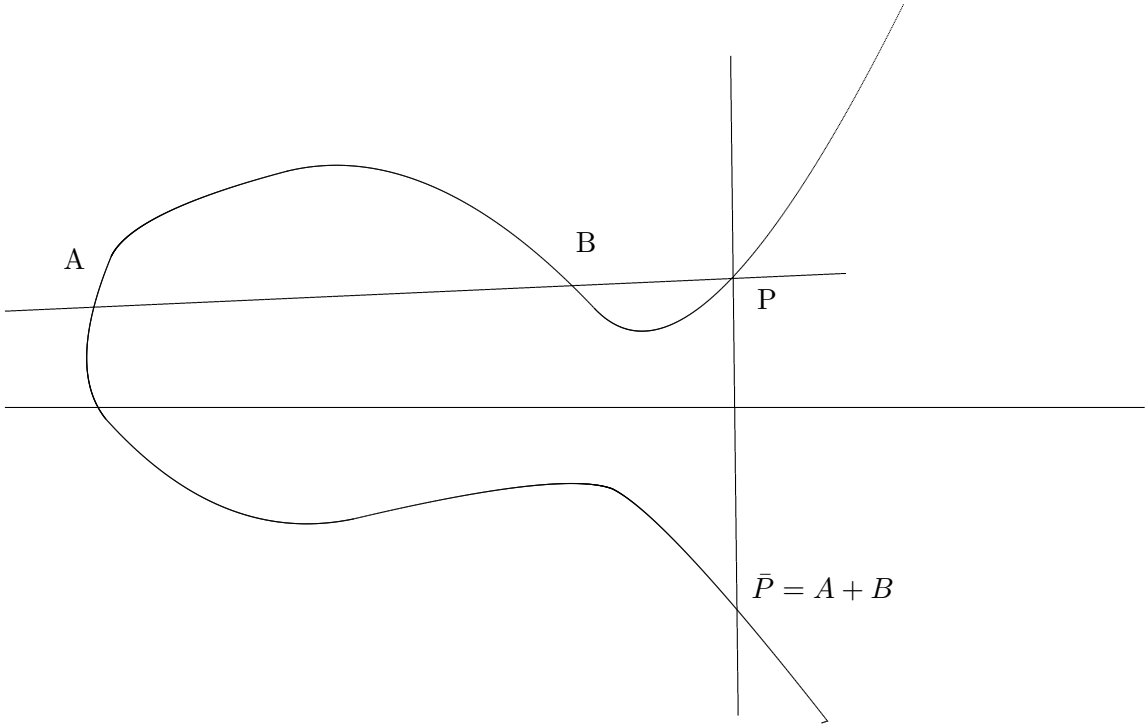

Figure 2: Loi d'addition simplifiée

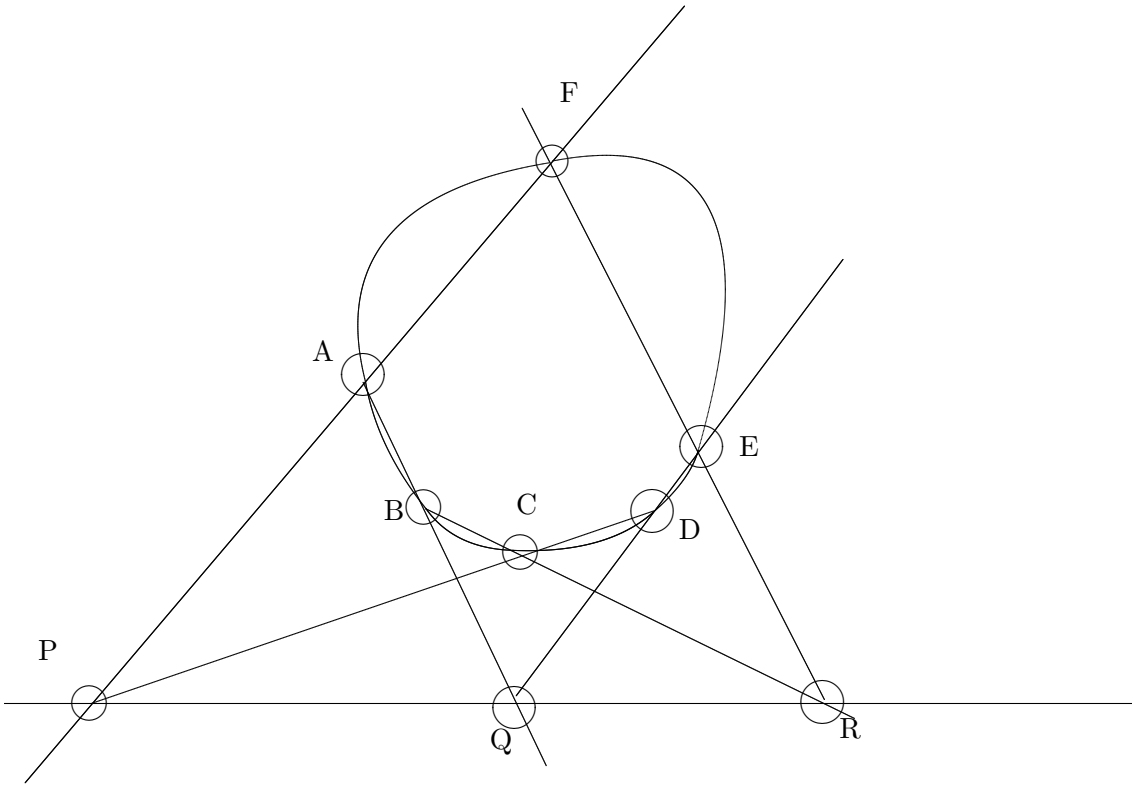

Figure 3: L'hexagone de Pascal

- *On choisit une courbe elliptique au hasard à coefficients dans $\mathbb{Z}$ avec un point P sur celle-ci. On considère alors la loi de groupe sur cette courbe modulo n.*
- *On calcule $eP = (u, x, y)$ dans ce groupe où e est un produit de petit nombres premiers pris à de petites*

puissances comme dans la méthode $p-1$ de Pollard.

- *On calcule le pgcd de u (ou du dénominateur de x) avec n.*
- *Si on trouve 1, alors on essaye avec une nouvelle courbe elliptique et un autre point.*

Commentez cet algorithme et expliquez en quoi il est plus souple que celui de Pollard.
Remarque: L'ordre d'une courbe elliptique prise au hasard sur $\mathbb{Z}/p\mathbb{Z}$ varie de manière aléatoire entre $p+1-2\sqrt{p}$ et $p+1+2\sqrt{p}$.

2 Séries théta

Dans la preuve de l'équation fonctionnelle de la fonction zéta de Riemann, on utilise la fonction théta usuelle

$$\theta(z) = \sum_{n\in\mathbb{Z}} e^{\frac{n^2 z}{2}}$$

pour $z = iy$, $y > 0$. Celle-ci définit une fonction holomorphe sur le demi-plan de Poincaré; la formule sommatoire de Poisson donne par prolongement analytique l'équation fonctionnelle

$$\theta(-\frac{1}{z}) = (-iz)^{1/2}\theta(z)$$

où $(-iz)^{1/2}$ est donné par la branche de la fonction sur $\mathcal{H}$ qui envoie iy sur $\sqrt{y}$. Cette relation jointe à la relation évidente $\theta(z+1) = \theta(z)$ donne une règle de transformation pour $f(\gamma z)$ pour tout $\gamma \in PSL_2(\mathbb{Z})$ agissant sur $\mathcal{H}$ par homographies. De même pour tout $k \geq 1$, $\theta(2z)^k$ satisfait à des formules de transformation analogues. Par ailleurs les égalités

$$\theta(2z)k = \sum_{n\geq 0} r_k(n) e^{nz}$$

où $r_k(n)$ désigne le nombre de représentations de n comme somme de k carrés d'entiers, justifient à elles seules, l'acharnement qu'ont subies ces séries. En particulier, on peut montrer les identités suivantes:

$$\begin{aligned} r_2(n) &= 4\textstyle\sum_{d|n} \chi_4(d) \\ r_4(n) &= 8(3+(-1)^n)\textstyle\sum_{d|n} d \\ r_6(n) &= 16\textstyle\sum_{d|n} d^2\chi_4(\frac{n}{d}) - 4\sum_{d|n} d^2\chi_4(d) \end{aligned}$$

avec $\chi_4(n) = d_1(n) - d_3(n)$ où $d_1(m)$ (resp. $d_3(m)$) est le nombre de diviseur $d \equiv 1 \mod 4$ (resp. $d \equiv 3 \mod 4$) de n.

Nous verrons dans la feuille de TD suivante, comment la théorie des formes modulaires permet d'expliquer la forme générale de ces formules, pourquoi il n'y a pas de formules élémentaires du même type pour k plus grand, et de donner une relation asymptotique sur $r_k(n) \sim n^{k-1}$ pour $k \geq 5$.

Exercice 1. *Montrez les égalités*

$$\prod_{m=1}^{\infty}(1+x^m z) = \sum_{m=0}^{\infty} \frac{x^{\frac{n(n+1)}{2}}}{(1-x)\cdots(1-x^n)} z^n$$

$$\prod_{m=1}^{\infty}(1-x^m z)^{-1} = \sum_{m=0}^{\infty} \frac{x^n}{(1-x)\cdots(1-x^n)} z^n$$

et en déduire que le nombre de manières différentes d'exprimer n comme somme de m nombres entiers:

- compris entre 1 et m, est égal au nombre de manières différentes d'exprimer $n+m$ comme somme de m nombres ≥ 1.

- est égal au nombre de manières différentes d'écrire $n + \frac{m(m-1)}{2}$ comme somme de m nombres inégaux.

Définition des fonctions théta: nous cherchons à définir des fonctions **entières** pour le réseau de périodes $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, où τ désigne un nombre complexe du demi-plan de Poincaré. Les propriétés de "périodicité" que nous prendrons ici sont:

$$\begin{cases} \Theta(z+1) = \Theta(z) \\ \Theta(z+\tau) = F(z)\Theta(z) \end{cases}$$

où $F(z)$ est un facteur à déterminer vérifiant en particulier $F(z+1) = F(z)$. Le choix habituel de F est

$$F(z) = \frac{1}{ce^{2i\pi z}},\ c \in \mathbb{C}^\times$$

Puisque Θ est holomorphe de période 1, elle peut être développée en série de Fourier

$$\Theta(z) = \sum_{-\infty}^{+\infty} a_n e^{2i\pi nz}$$

où les a_n sont les coefficients de Fourier de Θ.

Exercice 2. *On pose $q = e^{i\pi\tau}$. Montrez que l'on a*

$$\Theta(z) = a_0 \sum_{-\infty}^{+\infty} c^n q^{n(n-1)} e^{2i\pi nz}$$

On définit la fonction θ_3 en prenant $c = q$ dans l'expression précédente puis pour $\lambda = q^{-1/4}e^{-i\pi z}$, les fonctions θ_1, θ_2 et θ_4 définies par les relations données dans le tableau suivant:

	$z+\frac{1}{2}$	$z+\frac{\tau}{2}$	$z+\frac{1+\tau}{2}$
θ_1	θ_2	$i\lambda\theta_4$	$\lambda\theta_3$
θ_2	$-\theta_1$	$\lambda\theta_3$	$-i\lambda\theta_4$
θ_3	θ_4	$\lambda\theta_2$	$i\lambda\theta_1$
θ_4	θ_3	$i\lambda\theta_1$	$\lambda\theta_2$

Exercice 3. *Montrez que θ_1, θ_2 appartiennent au réseau $\mathbb{Z}2 + \mathbb{Z}\tau$ mais que les carrés des fonctions théta appartiennent tous au réseau $\mathbb{Z} + \mathbb{Z}\tau$ et ont tous les mêmes multiplicateurs. En déduire que les quotients des carrés de fonctions théta sont des fonctions elliptiques pour Λ.*

Nous verrons plus loin que ces fonctions sont d'ordre 2, de sorte que trois fonctions de ce type sont linéairement dépendantes, dont nous proposons dans l'exercice suivant quelques exemples suivant la méthode ci-après: remarquer que les séries qui définissent ces fonctions sont absolument convergentes et que les termes d'un produit peuvent être réarrangés suivant les puissances de q.

Exercice 4. *Prouvez la relation*

$$\theta_1(x,q)\theta_2(y,q) = \theta_3(x+y,q^2)\theta_2(x-y,q^2) - \theta_2(x+y,q^2)\theta_3(x-y,q^2)$$

où x, y sont deux éléments quelconques de $\mathbb{C}$ et où l'on a fait apparaître la variable muette q. En effectuant les translations par $\frac{1}{2}$, $\frac{\tau}{2}$, $\frac{1=\tau}{2}$ sur x et y, prouvez:

$$\begin{cases} \theta_1(x,q)\theta_2(y,q) = \theta_3(x+y,q^2)\theta_2(x-y,q^2) - \theta_2(x+y,q^2)\theta_3(x-y,q^2) \\ \theta_1(x,q)\theta_2(y,q) = \theta_1(x+y,q^2)\theta_4(x-y,q^2) + \theta_4(x+y,q^2)\theta_1(x-y,q^2) \\ \theta_2(x,q)\theta_2(y,q) = \theta_2(x+y,q^2)\theta_3(x-y,q^2) + \theta_3(x+y,q^2)\theta_2(x-y,q^2) \\ \theta_3(x,q)\theta_3(y,q) = \theta_3(x+y,q^2)\theta_3(x-y,q^2) + \theta_2(x+y,q^2)\theta_2(x-y,q^2) \\ \theta_3(x,q)\theta_4(y,q) = \theta_4(x+y,q^2)\theta_4(x-y,q^2) - \theta_1(x+y,q^2)\theta_1(x-y,q^2) \\ \theta_4(x,q)\theta_4(y,q) = \theta_3(x+y,q^2)\theta_3(x-y,q^2) - \theta_2(x+y,q^2)\theta_2(x-y,q^2) \end{cases}$$

- *En remplaçant y par 0 dans ces relations, on obtient les relations linéaires prévues entre les carrés des fonctions théta. En déduire la célèbre* ***relation de Jacobi****:*

$$\theta_3^4(0) = \theta_2^4(0) + \theta_4^4(0)$$

- *En dérivant par rapport à x et en remplaçant x et y par zéro, montrez que*

$$\theta_1'(0,q)\theta_2(0,q) = 2\theta_1'(0,q^2)\theta_4(0,q^2)$$

puis en déduire la relation

$$\theta_1'(0) = \pi\theta_2(0)\theta_3(0)\theta_4(0)$$

Expression des fonctions théta sous forme de produits infinis: posons

$$\Phi(\xi,q) = \prod_{n=1}^{\infty}(1+q^{2n-1}\xi)(1+q^{2n-1}\xi^{-1})$$

pour $\xi \in \mathbb{C}^\times$ et $0<|q|<1$. On rappelle aussi que $\sin \pi z = \pi z \prod_{n=1}^{\infty}(1-\frac{z^2}{n^2})$.

Exercice 5. - *Montrez que le produit infini ci-dessus, converge uniformément sur tout compact vers une fonction holomorphe.*

- *On pose $\Theta(z) = \Phi(e^{2i\pi z}, e^{i\pi\tau})$ est une fonction théta avec $F(z) = \frac{1}{qe^{2i\pi z}}$.*
- *Montrez que $\Theta = a_0\theta_3$ puis que*

$$\begin{cases} a_0\theta_1(z,q) = -i\nu\Phi(-qe^{2i\pi z},q) \\ a_0\theta_2(z,q) = \nu\Phi(qe^{2i\pi z},q) \\ a_0\theta_3(z,q) = \Phi(e^{2i\pi z},q) \\ a_0\theta_4(z,q) = \Phi(-e^{2i\pi z},q) \end{cases}$$

- *En utilisant la relation $\theta_1'(0) = \pi\theta_2(0)\theta_3(0)\theta_4(0)$, montrez que $a_0^{-1} = \prod_{n=1}^{\infty}(1-q^{2n})$ et finalement*

$$\begin{cases} \theta_1(z,q) = 2q^{1/4}\sin(\pi z)\prod_{n=1}^{\infty}(1-q^{2n})(1-2q^{2n}\cos(2\pi z)+q^{4n}) \\ \theta_2(z,q) = 2q^{1/4}\prod_{n=1}^{\infty}(1-q^{2n})(1+2q^{2n}\cos(2\pi z)+q^{4n}) \\ \theta_3(z,q) = \prod_{n=1}^{\infty}(1-q^{2n})(1+2q^{2n-1}\cos(2\pi z)+q^{4n-2}) \\ \theta_4(z,q) = \prod_{n=1}^{\infty}(1-q^{2n})(1-2q^{2n-1}\cos(2\pi z)+q^{4n-2}) \end{cases}$$

- *En déduire que tous les zéros des fonctions théta dans $\mathbb{C}$ sont simples, puis que les zéros de θ_1 (resp. θ_2, θ_3, θ_4) sont congrus à 0 (resp. $\frac{1}{2}$, $\frac{1+\tau}{2}$, $\frac{\tau}{2}$) modulo Λ.*

Equation de la chaleur: les fonctions θ_1, θ_2, θ_3, θ_4 vérifient l'équation

$$\frac{\partial^2\Theta}{\partial z^2} = 4\pi i\frac{\partial\Theta}{\partial\tau}$$

Fonctions théta et sin amp: on a les identités

$$\mathrm{sn}(x,k) = \frac{\theta_3(0)}{\theta_2(0)}\frac{\theta_1}{\theta_4}(\frac{x}{\pi\theta_3^2(0)}|\tau)$$

avec $k^2 = \frac{\theta_2^4(0)}{\theta_3^4(0)}$, $(k')^2 = \frac{\theta_4^4(0)}{\theta_3^4(0)}$.

Fonctions théta et fonction de Weierstrass: on a

$$\mathfrak{P}(x) = -[\log\theta_1(x)]'' + e_1 + [\log\theta]''(1/2) = e_1 + [\frac{\theta_1'(0)}{\theta_1(x)}.\frac{\theta_2(x)}{\theta_2(0)}]^2 ...$$

Exercice 6. - *Montrez, en regardant la périodicité, les racines et les résidus en $x=0$ et 1, que*

$$\sqrt{\mathfrak{P}(x)-e_3} = \frac{\theta_1'(0)\theta_4(x)}{\theta_4(0)\theta_1(x)}$$

- *En prenant* $x = 1/2$ *et en utilisant l'égalité*

$$\frac{q^n}{1+q^{2n}} = q^n \frac{1-q^{2n}}{1-q^{4n}} = (q^n - q^{3n}) \sum_{l=0}^{\infty} q^{4nl}$$

que

$$\pi^{-1}\sqrt{e_1 - e_3} = 1 + 4\sum_{n=1}^{\infty} \frac{q^n}{1+q^{2n}} = 1 + R\sum_{n=1}^{\infty}\sum_{l=0}^{\infty} q^{n(4l+1)} - 4\sum_{n=1}^{\infty}\sum_{l=0}^{\infty} q^{n(4l+3)}$$

- *Montrez que* $\sqrt{e_1 - e_3} = \frac{\theta_1'(0)\theta_3(0)}{\theta_2(0)\theta_4(0)} = \pi\theta_3(0)^2$.

- *En déduire alors que* $r_2(m)$ *qui par définition est le nombre de représentations de* m *en somme de deux carrés, est égal à* $4d_1(m) - 4d_3(m)$ *où* $d_1(m)$ *(resp.* $d_3(m)$*) est le nombre de diviseurs de* m *congrus à* 1 *(resp.* 3*) de* m.

Exercice 7. - *A partir de l'égalité* $\sqrt{\mathfrak{P}(x) - e_3} = \frac{\theta_1'(0)\theta_4(x)}{\theta_1(x)\theta_4(0)}$, *montrez que* $e_3 = -\theta_4"(0)/\theta_4(0)$.

- *Montrez que*

$$\theta_3(0)^4 = \pi^{-2}[\frac{\theta_4"(0)}{\theta_4(0)} - \frac{\theta_2"(0)}{\theta_2(0)}]$$

- *Montrez que*

$$\theta_3^4(0) = 1 - 32\sum_{n=1}^{\infty} n\sum_{l=1}^{\infty} q^{4ln} + 8\sum_{n=1}^{\infty} n\sum_{l=1}^{\infty} q^{ln}$$

- *En déduire alors que* $r_4(n)$ *est égal à* 8 *fois la somme des diviseurs* d *de* n *qui ne sont pas divisibles par* 4.

Exercice 8. *En substituant à l'écriture de* θ_3 *sous forme de produit,* $iq^{1/4}$ *à la place de* p *et* $q^{3/2}$ *à* q, *montrez que*

$$\sum_{n\in\mathbb{Z}} (-1)^n q^{n(3n+1)/2} = \prod_{n=1}^{\infty}(1-q^n)$$

En déduire alors que $p_+(m) - p_-(m) = (-1)^m$ *ou* 0 *selon que* $m = n(3n \pm 1)/2$ *ou non, où* $p_+(m)$ *(resp.* $p_-(m)$*) est le nombre de partitions de* m *en un nombre pair (resp. impair) de parts* $n \geq 1$.

Soit $p(n)$ le nombre de façons d'écrire n comme somme de nombres entiers ≥ 1:

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{m=1}^{\infty} \frac{1}{(1-x^m)}$$

On peut montrer en utilisant les séries théta (cf. la littérature) les congruences de Ramanujan:

$$\begin{cases} p(5n+4) \equiv 0 \mod 5 \\ p(7n+5) \equiv 0 \mod 7 \\ p(11n+5) \equiv 0 \mod 11 \end{cases}$$

Soit V un espace vectoriel réel de dimension finie n, muni d'une mesure invariante μ et on note $\hat{V}$ son dual. Soit f une fonction indéfiniment différentiable à décroissance rapide sur V, la transformée de Fourier $\hat{f}$ de f est définie par la formule

$$\hat{f}(y) = \int_V e^{-2i\pi<x,y>} f(x)\mu(x)$$

C'est une fonction indéfiniment différentiable à décroissance rapide sur $\hat{V}$. Soit alors Γ un réseau de V, de réseau dual $\hat{\Gamma}$ dans $\hat{V}$. La formule sommatoire de Poisson est alors

$$\sum_{x\in\Gamma} f(x) = \frac{1}{\mu(V/\Gamma)} \sum_{y\in\hat{\Gamma}} \hat{f}(y)$$

Exercice 9. *Au réseau Γ, on associe la fonction suivante définie sur $\mathbb{R}_+^*$:*

$$\Theta_\Gamma(t) = \sum_{x\in\Gamma} e^{-\pi t<x|x>}$$

ou encore si $(e_i)_i$ est une base de Γ et $A = (< e_i|e_j >)$, $\Theta_\Gamma(t) = \sum_{X\in\mathbb{Z}^n} e^{-\pi t {}^tXAX}$. Montrez l'égalité

$$\Theta_\Gamma(t) = \frac{t^{-n/2}}{\mu(V/\Gamma)}\Theta_{\hat\Gamma}(t^{-1})$$

Exercice 10. *On suppose désormais que Γ est unimodulaire, i.e. $\hat\Gamma = \Gamma$ ce qui est équivalent à demander que $A \in SL_2(\mathbb{Z})$. On suppose (dans un premier temps) que Γ est de type II, i.e. que les éléments diagonaux de A sont pairs. Pour $m \in \mathbb{N}$, on note $r_\Gamma(m)$ le nombre d'éléments $x \in \Gamma$ tels que $< x|x >= m$.*

- *Montrez, en toute généralité, que si $r_\Gamma(m) = r_{\Gamma'}(m)$ pour tout $m \in \mathbb{N}$, alors Γ et Γ' sont semblables, ou encore que $\tau = \tau' \in \mathbb{H}/SL_2(\mathbb{Z})$, ou Γ est semblable à $< 1, \tau >$ et Γ' à $< 1, \tau' >$.*
- *Montrez que $r_\Gamma(m) = O(m^{n/2})$ et en déduire que la série entière*

$$\sum_{m=0}^{\infty} r_\Gamma(m)q^n$$

  converge pour $|q| < 1$ et donc que $\Theta_\Gamma(z) = \sum_{x\in\Gamma} e^{i\pi z<x|w>}$ définit une fonction sur $\mathbb{H}$.
- *On suppose que $n \not\equiv 0 \mod 8$. Montrez que quitte à remplacer Γ par $\Gamma \oplus \Gamma$ ou $\Gamma \oplus \Gamma \oplus \Gamma \oplus \Gamma$, on peut supposer $n \equiv 4 \mod 8$. Montrez alors que ST transforme la forme différentielle $w(z) = \Theta_\Gamma(z)dz^{n/4}$ en $-w$ et en déduire qu'en fait $n \equiv 0 \mod 8$.*
- *Montrez que Θ_Γ est une forme modulaire de poids $n/2$.*

Exercice 11. *On considère ici le réseau unimodulaire $\mathbb{Z}^n$ et $\widetilde\theta := \Theta_{\mathbb{Z}^n}$ défini sur $\mathbb{H}$.*

- *Montrez que $\widetilde\theta(z+2) = \widetilde\theta(z)$.*
- *Montrez que $\widetilde\theta(-1/z) = \sqrt{iz}\widetilde\theta(z)$, où $\sqrt{\ }$ désigne la branche positive sur $\mathbb{R}^+$.*
- *En déduire, après calcul, que*

$$\widetilde\theta(\gamma z) = (\frac{2c}{d})\epsilon_d^{-1}(cz+d)^{1/2}\widetilde\theta(z)$$

  pour tout $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ tel que $b \equiv c \equiv 0 \mod 2$ où $\epsilon_d = 1$ ou i selon que $d \equiv 1$ ou $3 \mod 4$ et le symbole $(\frac{\cdot}{\cdot})$ est le symbole de Legendre étendu comme suit:
  - *$(\frac{a}{b}) = 0$ si $a \wedge b \neq 1$;*
  - *si b est un nombre premier impair alors $(\frac{a}{b})$ est le symbole de Legendre habituel;*
  - *$b > 0$ alors $(\frac{a}{b})$ est un caractère modulo b;*
  - *$a \neq 0$ alors $(\frac{a}{b})$ est un caractère modulo $4a$;*
  - *$(\frac{a}{-1}) = 1$ si $a > 0$ et -1 si $a < 0$ et $(\frac{0}{\pm 1}) = 1$.*
- *En déduire alors que $\theta(z) = \widetilde\theta(2z)$ vérifie*

$$\theta(\gamma z) = j(\gamma, z)\theta(z) \qquad \forall \gamma \in \Gamma_0(4)$$

  où $j(\gamma, z) = (\frac{c}{d})\epsilon_d^{-1}(cz+d)^{1/2}$.

La fonction θ ci-dessus, est notre exemple fondamental de forme modulaire de poids demi-entier et le facteur $j(\gamma, z)$ est utilisé pour définir les formes modulaires de poids demi-entier: pour $4|N$, une forme modulaire $f(z)$ de poids k un demi-entier, pour $\Gamma_0(N)$ est une fonction holomorphe sur $\mathbb{H}$ et en chaque cusp telle que

$$f(\gamma z) = j(\gamma, z)^{2k} f(z) \qquad \forall \gamma \in \Gamma_0(N)$$

Pour Γ unimodulaire de type I, la fonction Θ_γ définit alors une forme modulaire de poids demi-entier.

Exercice 12. *Soit pour* $\mathrm{Re}(s) > 1$, $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ *la fonction zéta de Riemann et pour* $\mathrm{Re}(s) > 0$, $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1} dt$ *la fonction* Γ *usuelle. On pose*

$$\Lambda(s) = \pi^{-s/2} \Gamma(s/2) \zeta(s)$$

Montrez que $\Lambda(s) + \frac{1}{s} + \frac{1}{s-1}$ *peut-être prolongée holomorphiquement à tout le plan complexe et que l'on a l'équation fonctionnelle*

$$\Lambda(s) = \Lambda(1-s)$$

Indication*: écrivez* $\Lambda(2s) = \int_0^\infty \left(\sum_{n=1}^{\infty} e^{-\pi n^2 t} \right) t^{s-1} dt$.