Une relation de distribution satisfaite par la fonction zêta de Weierstrass associée à un réseau complexe

par Abdelmejid BAYAD

Pour tout réseau complexe L, on associe les fonctions de Weierstrass suivantes

$$(0.1)\quad \zeta(z,L)=\frac{1}{z}+\sum_{\substack{\omega\in L\\ \omega\neq 0}}\Big[\frac{1}{z-\omega}+\frac{1}{\omega}+\frac{z}{\omega^2}\Big];\quad \wp_L(z)=\frac{1}{z^2}+\sum_{\substack{\omega\in L\\ \omega\neq 0}}\Big[\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\Big],$$

On associe aussi à L les séries d'Eisenstein suivantes:

$$(0.2)\qquad E_k^*(z,L)=\lim_{s\to 0+}\sum_{w\in L}^{(e)}(w+z)^{-k}|w+z|^{-s}, k=1,...$$

Où la sommation $\sum^{(e)}$ est celle d'Eisenstein donnée par

$$\sum\nolimits^{(e)}=\sum_m^{(e)}\sum_n^{(e)}=\lim_{M\to\infty}\sum_{m=-M}^{m=M}\left(\lim_{N\to\infty}\sum_{n=-N}^{n=N}\right).$$

Dans le paragraphe 2, nous prouvons une relation de distribution additive satisfaite par $\zeta(z,L)$. Cette relation est simple et de nature arithmétique. En effet, dans le paragraphe 3, elle permet de donner une relation de distribution additive satisfaite par les séries d'Eisenstein $E_k^*(z,L)$, ainsi on retrouve tous les résultats fondamentaux du livre d'André Weil [16]. D'autre part, dans le paragraphe 4, nous en déduisons de notre résultat principal d'autres formules de distribution satisfaites par les fonctions $\wp_L(z)^k$ et $\wp_L^{'}(z)^k$, pour tout $k\in\mathbb{N}^*$. Ces dernières relations de distributions permettent, en particulier, de rendre plus explicite l'algorithme CCR [6] et l'algorithme d'Atkin liés aux sommes de valeurs de la fonction $\wp_L$ de Weierstrass, [3]. De façon plus précise, nous calculons

$$\sum_t\zeta(z+t,L),\sum_t\wp_L(z+t)^k,\sum_t\wp_L^{'}(z+t)^k,$$

respectivement en fonction de

$$\zeta(z,\Lambda),\wp_\Lambda(z),\wp_\Lambda^{'}(z).$$

et nous déduisons les sommes suivantes

$$\sum_{t\neq 0}\wp_L(t)^k,\sum_{t\neq 0}\wp_L^{'}(t)^k,$$

où t parcourt un système de représentants de Λ/L dans $\mathbb{C}$ contenant o. Il est à noter que L'algorithme d'Atkin s'occupe plus précisément du calcul numérique des quantités suivantes $\sum_{t\neq 0} \wp_L(t)^k$.

Dans le paragraphe 5, nous améliorons le théorème 8.3 [11] de René Schoof, pour les isogénies entre courbes elliptiques de degré quelconque.

Dans une note en préparation, notre relation de distribution additive satisfaite par $\zeta(z, L)$ nous fournit un moyen pour étudier les sommes de Dedekind $D_n(a, c)$ liées aux séries d'Eisenstein, où bien sûr

$$D_n(a,c) := \frac{1}{c} \sum_{k\in L/cL\setminus\{\bar{0}\}} E_n^*\left(\frac{k}{c}, L\right) E_n^*\left(\frac{ak}{c}, L\right),$$

$a, c \in O_L$ non nuls et premiers entre eux, O_L étant l'ordre associé au réseau complexe L. Les résultats connus les concernant traitent seulement le cas $n = 1$. Plus précisément, d'après R.Sczech [12], on sait que:

$$D_1(a,c) + D_1(c,a) = 2iG_2(L)\,\mathrm{Im}\left(\frac{a}{c} + \frac{1}{ac} + \frac{c}{a}\right)$$

où $G_2(L)$ est précisé dans le lemme 1.2.

Le paragraphe 1 contient les définitions et propriétés fondamentales sur les fonctions de Weierstrass et les séries d'Eisenstein.

1. Fonctions de Weierstrass et séries d'Eisenstein.

Soient L un réseau complexe et $\{\omega_1, \omega_2\}$ en est une base orientée c'est-à-dire $\mathrm{Im}\,\frac{\omega_1}{\omega_2} > 0$. On désigne par $a(L)$ l'aire du tore complexe $\mathbb{C}/L$ qui est donné par

$$a(L) = \frac{1}{2i}\begin{vmatrix} w_1 & \overline{w}_1 \\ w_2 & \overline{w}_2 \end{vmatrix} = \frac{w_1\overline{w}_2 - w_2\overline{w}_1}{2i} = |w_2|^2\,\mathrm{Im}\left(\frac{\omega_1}{\omega_2}\right);$$

$a(L)$ est un nombre réel > 0. On déduit de l'action de $\mathrm{SL}_2(\mathbb{Z})$ sur la base orientée (w_1, w_2) de L que $a(L)$ est indépendant du choix de la base orientée (w_1, w_2) de L. De plus, pour tout $\lambda \in \mathbb{C}^*$, $a(\lambda L) = |\lambda|^2 a(L)$. De même, $a(L) = [\Lambda : L]a(\Lambda)$, pour tout réseau complexe Λ contenant L et d'indice fini $[\Lambda : L]$.

Maintenant, précisons les définitions et propriétés connues des fonctions de Weierstrass. D'après [14], Propositions 5.2 et 5.4 p.41-44 on a

Proposition définition 1.1.

La fonction σ_L de Weierstrass est définie par :

$$\sigma_L(z) = z \prod_{\ell \in L, \ell \neq 0} \Big(1 - \frac{z}{\ell}\Big) e^{\frac{z}{\ell} + \frac{1}{2}\left(\frac{z}{\ell}\right)^2}.$$

Elle est liée aux fonctions $\wp_L$ et $\zeta(z, L)$ par:

$$\zeta(z, L) = \frac{d}{dz}\log(\sigma_L(z)), \quad \frac{d^2}{dz^2}\log(\sigma_L(z)) = -\wp_L(z).$$

D'autre part, $\wp_L$ est elliptique de périodes L et $\zeta(z, L)$ vérifie

$$\zeta(z + \omega, L) = \zeta(z, L) + \eta(\omega, L),$$

où $\eta(\omega, L)$ est la fonction eta de Dedekind. Elle est indépendante de z et morphisme de L sur $\mathbb{C}$.

Commençons par le lemme suivant sur les fonction σ_L et $\eta(., L)$

LEMME 1.2. — **(1)** *La série* $\displaystyle\sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^2|\omega|^{2s}}$ *est holomorphe en* $s = 0$. *On définit alors:* $G_2(L) = \displaystyle\lim_{s\to 0} \sum_{\omega \in L\setminus\{0\}} \frac{1}{\omega^2|\omega|^{2s}}$.

(2) *Les fonctions* σ_L *et* $\eta(., L)$ *vérifient, pour tout* $z \in \mathbb{C}$ *et* $\omega \in L$,

$$\sigma_L(z + \omega) = \chi_L(\omega) e^{\eta(\omega, L)(z + \frac{1}{2}\omega)} \sigma_L(z),$$

$$\eta(z, L) = G_2(L)z + \frac{\pi}{a(L)}\bar{z}, \quad \chi_L(\omega) = \begin{cases} 1 & Si\ \omega \in 2L \\ -1 & Si\ \omega \in L\setminus 2L \end{cases}.$$

Démonstration. — Pour **(1)** se reporter à [13],Theorem 3,p.69, pour le **(2)** confère [9],p.225-226, theorems 1.1 et 1.2. Donnons, maintenant, les liens entre les fonctions de Weierstrass et les séries d'Eisenstein

LEMME 1.3. — *On a*

(i) $$E_1^*(z, L) = \zeta(z, L) - \eta(z, L)$$

(ii) $$E_2^*(z, L) = \wp_L(z) + G_2(L)$$

(iii) $$E_n^*(z, L) = \frac{(-1)^n}{(n-1)!} \wp_L{}^{(n-2)}(z), \forall n \geq 3$$

Démonstration. — Le (iii) se déduit par dérivation de (ii), en utilisant le lemme 1.1 le (i) et (ii) se déduisent du travail [7] pp.242-243.

Maintenant rappelons quelques propriétés des séries d'Eisenstein $G_{2m}(L), m \in \mathbb{N}^*$ et leur lien avec les fonctions $\wp_L$.

DÉFINITION ET PROPOSITION 1.4. — *Soit L un réseau complexe. Les séries G_{2m} d'Eisentein sont définies par*

$$G_{2m}(L) = \sum_{\omega \in L \setminus \{0\}} \frac{1}{\omega^{2m}}, \forall m \geq 2.$$

Elles vérifient la relation de récurrence suivante:
(i)

$$(2m+1)(m-3)(2m-1)G_{2m}(L) = 3\sum_{r=2}^{m-2}(2r-1)(2m-2r-1)G_{2r}(L)G_{2m-2r}(L), \forall m \geq 4.$$

Elles sont liées à la fonction $\wp_L$ par

$$(ii) \qquad \wp_L(z) = \frac{1}{z^2} + \sum_{k \geq 2}(2k-1)G_{2k}(L)z^{2k-2}.$$

De plus, elles permettent de préciser le modèle de Weierstrass complexe

$$\wp_L^{'}(z)^2 = 4\wp_L(z)^3 - 60G_4(L)\wp_L(z) - 140G_6(L).$$

Démonstration. — Se reporter à [16], Chap V§ 1 et Chap III§ 7 ou [1] pp.12-13 et [8], p.89. .

REMARQUES 1.5. — **1)** On déduit du 1.4, les relations suivantes

$$G_8 = \frac{3}{7}G_4^2, G_{10} = \frac{5}{11}G_4G_6, G_{12} = \frac{18}{143}G_4^3 + \frac{25}{143}G_6^2, G_{14} = \frac{30}{143}G_4^2G_6, G_{16} = \frac{9}{221}G_4^4 + \frac{300}{2431}G_4G_6^2, ...$$

2) On sait, d'après F. Rankin et Swinnerton-Dyer [10], que les zéros des séries G_{2m} se trouvent dans l'intersection du cercle unité complexe et du domaine fondamental du groupe modulaire $\mathrm{SL}_2(\mathbb{Z})$. Néanmoins, on peut explicitement déterminer les zéros de certaines séries d'Eisenstein en se basant sur l'équation fonctionnelle suivante:

$$G_{2m}\left(\frac{-1}{\tau}\right) = \tau^{2m}G_{2m}(\tau), \forall \tau : \mathrm{Im}\,\tau > 0.$$

Il en résulte que:

$$\begin{cases} G_{2m}(i) = 0 & \text{si m est impair} \\ G_{2m}(e^{\frac{2\pi i}{3}}) = 0 & \text{si m=1,2(mod3)} \end{cases}.$$

Donc, d'après le corollaire 1.4, G_{12} ne s'annule pas en $\tau = i$ ni en $\tau = e^{\frac{2\pi i}{3}}$, G_{10} et G_{14} ne s'annulent qu'en $\tau = i, e^{\frac{2\pi i}{3}}$. Car G_6 ne s'annule qu'en $\tau = i$ et G_4 ne s'annule qu'en $\tau = e^{\frac{2\pi i}{3}}$.

2. Formule de distribution additive satisfaite par la fonction $\zeta(.,L)$.

Dans ce paragraphe, nous prouvons une formule de distribution satisfaite par la fonction $\zeta(.,L)$. Ensuite, dans le paragraphe suivant, nous l'appliquons pour obtenir des formules de distribution satisfaites par les fonctions $\wp_L(z)^k$, $\wp_L^{'}(z)^k$, pour tout $k \in \mathbb{N}^*$, puis aux séries d'Eisenstein $E_n^*(.,L), \forall n \geq 1$. Nous commençons par le lemme suivant, dont la démonstration est élémentaire.

LEMME 2.1. — *Soient L et Λ deux réseaux complexes tels que: $L \subset \Lambda$ et $[\Lambda : L]$ est fini. On fixe $\mathcal{R}$ un système de représentants de Λ/L, contenant 0. Soient χ_Λ et χ_L définies comme dans le lemme 1.2. On a alors:*

$$\chi_\Lambda(\rho) = \chi_L(\rho)^{[\Lambda:L]} e^{\frac{2\pi i}{a(L)} Im\left(\bar{\rho} \sum\limits_{t\in\mathcal{R}} t\right)}, \forall \rho \in L.$$

Démonstration. — Si $\underline{[\Lambda : L] \text{ est impair}}$ alors $\sum\limits_{t\in\mathcal{R}} t \in L$. Par conséquent, $e^{\frac{2\pi i}{a(L)} \mathrm{Im}\left(\bar{\rho} \sum_{t\in\mathcal{R}} t\right)} = 1$, $\chi_L(\rho)^{[\Lambda:L]} = \chi_L(\rho), \forall \rho \in L$. De plus, on a $2\Lambda \cap L = 2L$. Donc, $\chi_\Lambda(\rho) = \chi_L(\rho)$. D'où le lemme lorsque $[\Lambda : L]$ est impair.

Examinons le cas où $\underline{[\Lambda : L] \text{ est pair}}$. On a: $\chi_L(\rho)^{[\Lambda:L]} = 1$. Deux cas à distinguer: $\sum\limits_{t\in\mathcal{R}} t \in L$ ou $\sum\limits_{t\in\mathcal{R}} t \notin L$. Si $2\Lambda \cap L \neq L$, par un calcul élémentaire, on obtient $\sum\limits_{t\in\mathcal{R}} t \notin L$ mais $2\sum\limits_{t\in\mathcal{R}} t \in L$. On déduit que :

$$\chi_\Lambda(\rho) = e^{\frac{2\pi i}{a(L)} \mathrm{Im}\left(\bar{\rho} \sum\limits_{t\in\mathcal{R}} t\right)}, \forall \rho \in \ L.$$

Le lemme est vérifié pour ce cas. Si maintenant, $2\Lambda \cap L = L$, on obtient que $\sum\limits_{t\in\mathcal{R}} t \in L$, et $\chi_\Lambda(\rho) = 1, \forall \rho \in L$, de plus $\chi_L(\rho)^{[\Lambda:L]} = 1$. Ce qui termine la démonstartion du lemme 2.1.

<u>Exemple de calcul de</u> $\sum\limits_{t\in\mathcal{R}} t$:

On considère le cas générique suivant, (ω_1, ω_2) et (ω_1', ω_2') sont respectivement des bases orientées de L et Λ tels que:

$$\omega_1' = \frac{\omega_1}{m}, \omega_2' = \frac{\omega_2}{n}, \mathcal{R} = \left\{ \frac{k}{n}\omega_1 + \frac{k'}{m}\omega_2, 0 \leq k \leq n-1; 0 \leq k' \leq m-1 \right\}.$$

On obtient,

$$\sum_{t\in\mathcal{R}} t = \frac{m(n-1)}{2}\omega_1 + \frac{n(m-1)}{2}\omega_2.$$

THÉORÈME PRINCIPAL 2.2. — *Soient L et Λ deux réseaux complexes tels que: $L \subset \Lambda$ et $[\Lambda : L]$ est fini. On a alors:*

$$\sum_{t\in\Lambda/L} \Big(\zeta(z+t,L) - \eta(t,L)\Big) = \zeta(z,\Lambda) + \Big([\Lambda : L]G_2(L) - G_2(\Lambda)\Big)z.$$

Démonstration.

Première méthode:

Tout d'abord, d'après la définition et proposition 1.1, il faut remarquer que la fonction $z \to \zeta(z+t,L) - \eta(t,L)$, ne dépend pas de t mais seulement de t modulo L.

Considérons les deux fonctions suivantes

$$F(z) = \sum_{t\in\Lambda/L} \Big(\zeta(z+t,L) - \eta(t,L)\Big) \quad \text{et } G(z) = \zeta(z,\Lambda) + \Big([\Lambda : L]G_2(L) - G_2(\Lambda)\Big)z$$

Elles sont méromorphes et ont les mêmes pôles (éléments de Λ) avec la même multiplicité qui est égale à 1. De plus,

$$F(z+\rho) = F(z) + ([\Lambda : L]\eta(\rho,L), G((z+\rho) = G(z) + ([\Lambda : L]\eta(\rho,L), \forall\rho \in \Lambda,$$

Ceci découle du fait que Λ/L est invariante par translation par $\rho, \forall\rho \in \Lambda$ et du fait que $a(L) = [\Lambda : L]a(\Lambda)$. Par conséquent, $(F-G)(z+\rho) = (F-G)(z), \forall\rho \in \Lambda$, et $F - G$ est méromorphe. En réalité $F - G$ est holomorphe. En effet, F et G ont la même partie principale, car les résidus en $z = \rho, \rho \in \Lambda$ vaut 1 pour F et G, de plus les pôles étants simples. Donc, $F - G$ est elliptique pour Λ, sans pôles, alors d'après le théorème de Liouville c'est une constante. En passant aux limites, $z \to 0$, on obtient

$$\lim_{z\to 0}(F(z) - G(z)) = \sum_{t\in\Lambda/L\setminus\{0\}} \Big(\zeta(t,L) - \eta(t,L)\Big).$$

Donc, cette méthode démontre le théorème sans pouvoir donner exactement la constante. Il est à noter que cette constante ne dépend que de Λ/L et non pas du choix d'un système de représentants de celui-ci. Dans ce qui suit nous donnons une autre méthode qui permet de montrer que

$$\sum_{t\in\Lambda/L\setminus\{0\}} \Big(\zeta(t,L) - \eta(t,L)\Big) = 0.$$

Seconde méthode:

Introduisons la fonction suivante

$$G : z \to e^{-\frac{1}{2}\Big([\Lambda:L]G_2(L)-G_2(\Lambda)\Big)z^2-\eta\left(\sum_{t\in\mathcal{R}} t, L\right)z} \times \sigma_L(z) \prod_{t\in\mathcal{R}}{}' \frac{\sigma_L(z+t)}{\sigma_L(t)}$$

où l'on a fixé $\mathcal{R}$ un système de représentants de Λ/L, contenant 0. Cette fonction vérifie les propriétés suivantes: Elle est holomorphe, ses zéros sont les éléments de Λ, de multiplicité 1. Comme σ_L vérifie $\sigma_L(z+\rho) = \chi_L(\rho)e^{\eta(\rho,L)(z+\frac{1}{2}\rho)}\sigma_L(z), \forall \rho \in L$ (Lemme 2.1), G vérifie aussi

$$G(z+\rho) = \chi_L(\rho)^{[\Lambda:L]} e^{\frac{2\pi i}{a(L)}\mathrm{Im}\left(\bar{\rho}\sum_{t\in\mathcal{R}} t\right)} e^{\eta(\rho,\Lambda)\left(z+\frac{\rho}{2}\right)} G(z), \forall \rho \in L.$$

Ce résultat se déduit, par un calcul simple, du Lemme 1.2 (2). D'autre part, par le même Lemme 1.2 (2), la fonction $z \to \sigma_\Lambda(z)$ elle aussi est holomorphe, ses zéros sont les éléments de Λ, de multiplicité 1 et

$$\sigma_\Lambda(z+\rho) = \chi_\Lambda(\rho)e^{\eta(\rho,\Lambda)\left(z+\frac{\rho}{2}\right)}\sigma_\Lambda(z), \forall \rho \in \Lambda.$$

Donc, d'après le lemme 2.1, ces deux fonctions ont le même facteur d'automorphie lorqu'on translate z par $\rho \in L$, qui est $\chi_\Lambda(\rho) = \chi_L(\rho)^{[\Lambda:L]} e^{2\pi i \mathrm{Im}\left(\bar{\rho}\sum_{t\in\mathcal{R}} t\right)}$. Donc, d'après le théorème de Liouville, elles diffèrent d'une constante multiplicative non nulle près. Comme $\lim_{z\to 0} \frac{\sigma_L(z)}{z} = 1$, alors cette constante vaut 1. Donc, on obtient une formule de distribution multiplicative pour la fonction σ_L

$$\sigma_\Lambda(z) = e^{-\frac{1}{2}\Big([\Lambda:L]G_2(L)-G_2(\Lambda)\Big)z^2-\eta\left(\sum_{t\in\mathcal{R}} t, L\right)z} \times \sigma_L(z) \prod_{t\in\mathcal{R}}{}' \frac{\sigma_L(z+t)}{\sigma_L(t)}.$$

Pour achever la démonstration du théorème 2.2, il suffit de passer au dérivé logarithmique de cette quantité. Bien sûr lorsqu'on passe à la limite, $z \to 0$, on obtient

$$\sum_{t\in\Lambda/L\setminus\{0\}} \Big(\zeta(t,L) - \eta(t,L)\Big) = 0.$$

3. Une application directe de notre résultat.

Notre théorème principal donne une preuve à la fois plus simple et plus préçise aux résultats suivants

PROPOSITION 3.1. — *Soient L et Λ deux réseaux complexes tels que: $L \subset \Lambda$ et $[\Lambda : L]$ est fini. Alors, pour tout $z \in \mathbb{C}\backslash\Lambda$, on a*

$$(i) \qquad \sum_{t\in\Lambda/L} \wp_L(z+t) = \wp_\Lambda(z) + G_2(\Lambda) - [\Lambda : L]G_2(L),$$

$$(ii) \qquad \sum_{t\in\Lambda/L} \wp_L^{(k)}(z+t) = \wp_\Lambda^{(k)}(z), \forall k \geq 1,$$

$$(iii) \qquad \sum_{t\in\Lambda/L\backslash\{0\}} \wp_L^{(2k-1)}(\sigma+t) = 0, \forall \sigma \in \frac{1}{2}\Lambda, \forall k \geq 1.$$

$$(iv) \qquad \sum_{t\in\Lambda/L\backslash\{0\}} \wp_L^{(2k-2)}(t) = (2k-1)!\Big(G_{2k}(\Lambda) - G_{2k}(L)\Big), \forall k \geq 1.$$

Démonstration. — En effet, le (i) s'obtient du théorème 2.2 par dérivation. Le (ii) s'obtient de (i) aussi par dérivation. Brièvement, pour obtenir le (iv) avec $k = 1$, il suffit de calculer $\lim\limits_{z\to 0}\Big[\wp_L(z) - \wp_\Lambda(z) + \sum\limits_{t\in\Lambda/L\backslash\{0\}} \wp_L(z+\ t)\Big]$. Pour $k \geq 2$, il suffit de dériver deux fois de proche en proche et refaire le même procédé de calcul de limite. De la même manière s'obtient le (iii) pour $k = 1$, en calculant $\lim\limits_{z\to 0}\Big[\wp_L^{'}(z) - \wp_\Lambda^{'}(z) + \sum\limits_{t\in\Lambda/L\backslash\{0\}} \wp_L^{'}(z+\ t)\Big]$. D'où le (iii) lorsque $\sigma = 0$. Le cas $\sigma \in \frac{1}{2}\Lambda\backslash\{0\}$, se déduit du fait que le diviseur de $\wp_\Lambda^{'}$ vaut $\sum\limits_{t\in\frac{1}{2}\Lambda/\Lambda\backslash\{0\}} (t) - 3(0)$. Pour $k \geq 2$, il suffit de dériver deux fois de proche en proche et refaire le même procédé de calcul de limite, en remarquant bien sûr que les zéros de $\wp_\Lambda^{'}$ sont encore des zéros pour la fonction $\wp_\Lambda^{(2k-1)}$. Pour ce dernier point, on utilise l'équation de Weierstrass qui lie $\wp_\Lambda$ et $\wp_\Lambda^{'}$, qui est ${\wp_\Lambda}^{'2} = 4{\wp_\Lambda}^3 - 60G_4(\Lambda)\wp_\Lambda - 140G_6(\Lambda)$. Pour le (iv), on calcule la limite de $\lim\limits_{z\to 0}\Big[\wp_L^{(k)}(z) - \wp_\Lambda^{(k)}(z) + \sum\limits_{t\in\Lambda/L\backslash\{0\}} \wp_L^{(k)}(z+\ t)\Big]$ en utilisant le (ii) pour k pair et l'écriture de $\wp_L^{(k)}(z)$ en série de Laurent au voisinage de 0 qui s'obtient de celle de $\wp_L(z)$ par dérivation, proposition définition 1.4 (ii).

Le contenu de la proposition suivante améliore largement les résultats d'Eisenstein-Kronecker qui font l'objet du livre d'André weil [16].

PROPOSITION 3.2. — *Soient L et Λ deux réseaux complexes tels que: $L \subset \Lambda$ et $[\Lambda : L]$ est fini. Alors, pour tout $z \in \mathbb{C}\backslash\Lambda$, on a*

$$\sum_{t\in\Lambda/L} E_n^*(z+t, L) = E_n^*(z, \Lambda), \forall n \geq 1.$$

Se déduit du théorème 2.2 et du Lemme 1.3 pour $n = 1$, puis par dérivation pour $n \geq 2$.

Remarque 3.3. —

1) Pour $n \geq 3$, la proposition 3.2 est exactement les formules de distribution additives satisfaites par les $E_n^*(z, L)$ démontrées par Eisenstein et améliorées par Kronecker. Quant à la formule de distribution additive satisfaite par la fonction $E_2^*(z, L)$ n'a été connue que pour les réseaux Λ de la forme $\frac{1}{c}L$, où $c \in O_L \backslash \{0\}$, confère [16].

2) Il est à noter que nos démonstrations sont très simples, élémentaires et différentes de celles d'Eisenstein et Kronecker qui sont très techniques et calculatoires. La proposition 3.1 me semble moins bien connue, du moins je n'ai aucunne référence pour ce résultat.

3) Sous une forme moins explicite, la relation (iv) de la proposition 3.1 n'a pas échappé à la sagacité d'Eisenstein. D'ailleurs D. Bertrand l'a utilisé, d'une façon indirecte (sans avoir une formule précise, [5] p.110) pour la recherche des isogénies entre courbes elliptiques et le calcul des hauteurs [5]. D.Bertrand m'avait demandé d'expliciter ce genre de relation de distribution. Je tiens à le remercier à l'occasion

4. Une remarque sur les algorithmes CCR et d'Atkin.

Précisons ces deux algorithmes pour une isogénie de degré l, $l \in \mathbb{N}^*$, entre deux courbes elliptiques. Soient L un réseau complexe, (ω_1, ω_2) en est une base orientée et $E_L : Y^2 = 4X^3 - 60G_4(L)X - 140G_6(L)$ une courbe elliptique définie sur $\mathbb{C}$. Elle est alors isomorphe au quotient $\mathbb{C}/L$. Pour fixer les idées, lorsqu'une isogénie $\mathcal{I}$ de degré l existe à partir de E_L, nous obtenons alors une courbe isogène $E_{\Lambda=[\frac{\omega_1}{l},\omega_2]} : Y^2 = 4X^3 - 60G_4(\Lambda)X - 140G_6(\Lambda)$ isomorphe au quotient $\mathbb{C}/\Lambda$. Vu en termes de résaux, est particulièrement simple puisqu'il s'agit de

$$\mathbb{C}/L \to \mathbb{C}/\Lambda, \quad z \to z.$$

Notons $I(X) = \frac{G(X)}{H(X)}$ l'image par $\mathcal{I}$ d'un point (X, Y) de E_L. Nous avons alors

$$\wp_\Lambda(z) = I(\wp_L(z)).$$

D'après les relations de Vélu [15], seul le calcul de $H(X)$ égal ici à

$$H(X) = \prod_{i=1}^{l-1} \left(X - \wp_L(i\frac{\omega_1}{l}) \right).$$

est nécéssaire pour déterminer complètement $\mathcal{I}$. Plusieurs algorithmes sont connus pour calculer directement $H(X)$. Les deux principaux sont: l'algorithme CCR et

l'algorithme d'Atkin. Pour déterminer $H(X)$, dans l'algorithme CCR et celui d'Atkin, sur $\mathbb{C}$, on calcule numériquement les sommes suivantes

$$s_k = \sum_{i=1}^{l-1} \wp_L\left(i\frac{\omega_1}{l}\right)^k, k \in \mathbb{N}^*,$$

ensuite via les formules des sommes de Newton ils obtiennent $H(X)$. Dans la littérature, il n'y a pas de formules explicites qui donnent les valeurs des s_k. Dans ce qui suit nous nous proposons de démontrer des formules explicites pour $k = 1, 2, 3$. Puis montrer, comment on peut les obtenir pour $k \geq 4$. En fait pour $k = 1$ la réponse est contenue dans la proposition 3.1 (iii) k=1, $\sigma = 0$.

THÉORÈME 4.1. — *Soient L et Λ deux réseaux complexes tels que: $L \subset \Lambda$ et $[\Lambda : L]$ est fini. On a alors, pour tout $z \in \mathbb{C}\backslash\Lambda$,*

$$(i) \qquad \sum_{t\in\Lambda/L} \wp_L(z+t)^2 = \wp_\Lambda(z)^2 + 5\left(G_4(L)[\Lambda : L] - G_4(\Lambda)\right),$$

$$(ii) \qquad \sum_{t\in\Lambda/L} \wp_L(z+t)^3 = \wp_\Lambda(z)^3 - 9\left(G_4(\Lambda) - G_4(L)\right)\wp_\Lambda(z)$$
$$-140\left(G_6(\Lambda) - G_6(L)[\Lambda : L]\right) + 9G_4(L)\left(G_2(\Lambda) - G_2(L)[\Lambda : L]\right).$$

Démonstration. — D'après l'équation de Weierstrass $\wp_L^{'}(z)^2 = 4\wp_L(z)^3 - 60G_4(L)\wp_L(z) - 140G_6(L)$, on en tire la relation suivante:

$$\wp_L^{''}(z) = 6\wp_L(z)^2 - 30G_4(L).$$

Donc, $\wp_L(z)^2 = \frac{1}{6}\wp_L^{''}(z) + 5G_4(L)$. La partie (i) du théorème 4.1 se déuit directement de la proposition 3.1 (ii) pour $k = 2$. Pour obtenir le (ii) du théorème 4.1, on utilise encore l'équation de Weierstrass $\wp_L^{'}(z)^2 = 4\wp_L(z)^3 - 60G_4(L)\wp_L(z) - 140G_6(L)$, pour calculer $\wp_L^{(4)}(z)$, qui donne

$$\wp_L^{(4)}(z) = 120\wp_L(z)^3 - 1080G_4(L)\wp_L(z) - 1680G_6(L).$$

Pour conclure, on utilise à nouveau la proposition 3.1 (ii) pour $k = 4$.

REMARQUE 4.2. — Pour obtenir les valeurs de toutes les sommes:

$$\sum_{t\in\Lambda/L} \wp_L(z+t)^k, z \in \mathbb{C}\backslash\Lambda, \forall \text{ k } \geq 4$$

Le procédé consiste tout simplement à calculer de proche en proche $\wp_L^{(2k-2)}(z)$ en appliquant à chaque étape l'équation de Weierstrass $\wp_L^{'}(z)^2 = 4\wp_L(z)^3 - 60G_4(L)\wp_L(z) - 140G_6(L)$, on obtient d'une manière récursive la valeur de la somme $\sum_{t\in\Lambda/L} \wp_L(z+t)^k$. En fait on obtient plus généralement

$\wp_L^{(2k-2)}(z) = (2k-1)!\wp_L(z)^k +$ polynôme en $\wp_L(z)$ de degré $\leq k-1..., \forall k \in \mathbb{N}^*$.

COROLLAIRE 4.3. — Soient L et Λ deux réseaux complexes tels que: $L \subset \Lambda$ et $[\Lambda : L]$ est fini. On a alors

$$\sum_{t\in\Lambda/L\setminus\{0\}} \wp_L(t)^2 = 5\left(G_4(L)[\Lambda : L] - G_4(\Lambda)\right),$$

et

$$\sum_{t\in\Lambda/L\setminus\{0\}} \wp_L(t)^3 = -140\left(G_6(\Lambda) - G_6(L)[\Lambda : L]\right) + 9G_4(L)\left(G_2(\Lambda) - G_2(L)[\Lambda : L]\right).$$

REMARQUE 4.4. —

1) Dans le cas où l est un nombre impair,

$$H(X) = \prod_{i=1}^{l-1}\Big(X - \wp_L(i\frac{\omega_1}{l})\Big) = \left[\prod_{i=1}^{\frac{l-1}{2}}\Big(X - \wp_L(i\frac{\omega_1}{l})\Big)\right]^2,$$

car $\wp_L$ est paire et elliptique pour L. Dans cas précis, le corollaire 4.3 , suffit pour rendre plus explicite les algorithmes CCR et celui d'Atkin pour $l = 3, 5, 7$.

2) Le calcul des sommes $\sum_t \wp_L^{'}(z+t)^k$, se déduit de celui des $\sum_t \wp_L(z+t)^k$, via l'équation de Weierstrass $\wp_L^{'}(z)^2 = 4\wp_L(z)^3 - 60G_4(L)\wp_L(z) - 140G_6(L)$.

5. Le théorème de René Schoof revisité.

Dans ce paragraphe, à partir de notre résultat principal, nous montrons comment obtenir et améliorer le théorème de René Schoof qui fait justement le point sur les algorithmes d'Atkin, CCR(rappelés dans le paragraphe précédent), et d'autres. On a le théorème plus général suivant

THÉORÈME 5.1 . — Soient L et Λ deux réseaux complexes tels que: $L \subset \Lambda$ et $[\Lambda : L]$ est fini. On a alors

(i) $$\prod_{t\in\Lambda/L\setminus\{0\}}\Big(\wp_L(z) - \wp_L(t)\Big) = e^{([\Lambda:L]G_2(L) - G_2(\Lambda))z^2}\frac{\sigma_\Lambda(z)^2}{\sigma_L(z)^{2[\Lambda:L]}}$$

(ii) Si $[\Lambda : L]$ est de plus impair alors

$$\prod_{t\in\Lambda/L\setminus\{0\}/\pm1}\Big(\wp_L(z) - \wp_L(t)\Big) = e^{\frac{1}{2}([\Lambda:L]G_2(L) - G_2(\Lambda))z^2}\frac{\sigma_\Lambda(z)}{\sigma_L(z)^{[\Lambda:L]}}$$

Démonstration. — Rappelons, [9] p.25, la formule de différence suivante

$$\wp_L(z) - \wp_L(t) = -\frac{\sigma_L(z+t)\sigma_L(z-t)}{\sigma_L(z)^2\sigma_L(t)^2}, \forall z, t \in \mathbb{C}\setminus\{0\}$$

Dans la seconde méthode, pour montrer notre résultat principal on a montré d'abord la formule suivante

$$\sigma_\Lambda(z) = e^{-\frac{1}{2}\Big([\Lambda:L]G_2(L)-G_2(\Lambda)\Big)z^2-\eta\left(\sum_{t\in\mathcal{R}} t, L\right)z} \times \sigma_L(z)\prod_{t\in\mathcal{R}}{}' \frac{\sigma_L(z+t)}{\sigma_L(t)}$$

Utilisons cette formule pour obtenir notre théorème 5.1. En fait, lorsque t parcourt $\Lambda/L\backslash\{0\}$, alors le produit

$$\prod_{t\in\Lambda/L\backslash\{0\}}\Big(\wp_L(z)-\wp_L(t)\Big) = \prod_{t\in\Lambda/L\backslash\{0\}} -\frac{\sigma_L(z+t)\sigma_L(z-t)}{\sigma_L(z)^2\sigma_L(t)^2}$$

est égal à

$$e^{([\Lambda:L]G_2(L)-G_2(\Lambda))z^2}\frac{\sigma_\Lambda(z)^2}{\sigma_L(z)^{2[\Lambda:L]}}$$

D'où le (i) du Théorème ci-dessus. Le (ii) se fait de la même manière que le (i).

D'après les propositions 1.1 et 1.4, on a

$$\zeta(z,L) = \frac{1}{z} - \sum_{k\geq 1} G_{2k+2}(L)z^{2k+1}, \sigma_L(z) = z\exp\Big(-\sum_{k\geq 1}\frac{G_{2k+2}(L)}{2k+2}z^{2k+2}\Big).$$

On peut écrire le théorème 5.1 de manière équivalente comme suit

THÉORÈME 5.1 (BIS) . — Soient L et Λ deux réseaux complexes tels que: $L\subset\Lambda$ et $[\Lambda:L]$ est fini. On a alors

(i)
$$\prod_{t\in\Lambda/L\backslash\{0\}}\Big(\wp_L(z)-\wp_L(t)\Big) = z^{2-2[\Lambda:L]}e^{([\Lambda:L]G_2(L)-G_2(\Lambda))z^2}$$
$$\exp\Big(-2\sum_{k\geq 1}\frac{[\Lambda:L]G_{2k+2}(L)-G_2(\Lambda)}{2k+2}z^{2k+2}\Big)$$

Si $[\Lambda:L]$ est de plus impair alors

(ii)
$$\prod_{t\in\Lambda/L\backslash\{0\}/\pm 1}\Big(\wp_L(z)-\wp_L(t)\Big) = z^{1-[\Lambda:L]}e^{\frac{1}{2}([\Lambda:L]G_2(L)-G_2(\Lambda))z^2}$$
$$\exp\Big(-\sum_{k\geq 1}\frac{[\Lambda:L]G_{2k+2}(L)-G_2(\Lambda)}{2k+2}z^{2k+2}\Big)$$

REMARQUE 5.2. — Lorsque $[\Lambda:L]$ est **premier impair**, on a exactement le Théorème 8.3 [11] dû à R. Schoof.

Bibliographie.

[1] Tom M. Apostol. — *Introduction to analytic Number Theory* , Sringer-Verlag, New York, 1976.

[2] A.O.L Atkin. — *Note on a paper of Rankin*, Bull.Lond.Math.Soc, **1** (1969), 191-192.

[3] A.O.L Atkin. — *The number of points on an elliptic curve modulo a prime*, Draft , 1988.

[4] A. Bayad, G. Robert. — *Note sur une forme de Jacobi méromorphe*, C.R.A.S Paris **325** (1997), 455-460.

[5] D. Bertrand. — *Hauteurs et isogénies*, Société mathématique de France, Astérisque **183** (1990), 107-125.

[6] L.S. Charlap,R. Coley,D.P Robbins. — *Enumeration of rational points on elliptic curves over finite fields*, Draft , 1991.

[7] J. Coates, A. Wiles. — *On the conjecture of Birch and Swinnerton-Dyer*, Inventiones Math **39** (1977), 223-251.

[8] Y. Hellegouarch. — *Invitation aux mathématiques de Fermat-Wiles*, Masson, 1997.

[9] D. Kubert, S. Lang. — *Modular units*, (Grundlehren der math. Wiss. 244), Springer-Verlag, 1981.

[10] F.K.C. Rankin, H.P.F Swinnerton-Dyer. — *On the zeros of Eisenstein series*, Bull. Lond. Math. Soc **2** (1970), 169-170.

[11] R.Schoof. — *Counting points on elliptic curves over finite fields*, Journal de Théorie des nombres de Bordeaux, **7** (1995), 219-254.

[12] R.Sczech. — *Dedekindsummen mit elliptischen Funktionen*, Invent.math, **76** (1984), 523-551.

[13] C.L Siegel. — *Lectures on advanced analytic number theory*, Tate Institute **Lecture Notes** (1961), 259-331.

[14] J. Silverman. — *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag,, 1995.

[15] J. Vélu. — *Isogénies entre courbes elliptiques*, C.R.A.S, série A **273** (1971), 238-241.

[16] A. Weil . — *Elliptic functions according to Eisenstein and Kronecker*, Springer-Verlag, Berlin/Heidelberg/New York, 1976.

Abdelmejid BAYAD

Université d'Evry, Département de Mathématiques,

Boulevard François Mitterrand 91025 EVRY Cedex

bayad@lami.univ-evry.fr