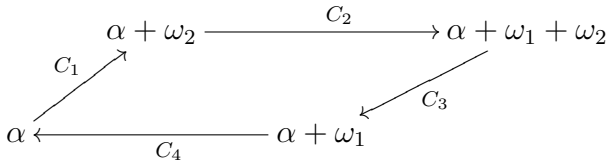
18.785 Analytic Number Theory Problem Set #1

Holden Lee

2/4/11

Problem 1

Label the edges of the fundamental parallelogram as follows.



We calculate $\int_{\partial P} \frac{zf'(z)}{f(z)}\,dz$ in two ways.

Way 1:

$$\int_{\partial P} \frac{zf'(z)}{f(z)}\,dz = \left[\int_{C_1} \frac{zf'(z)}{f(z)}\,dz + \int_{C_3} \frac{zf'(z)}{f(z)}\,dz\right] + \left[\int_{C_2} \frac{zf'(z)}{f(z)}\,dz + \int_{C_4} \frac{zf'(z)}{f(z)}\,dz\right].$$

Noting that C_3 is just C_1 shifted by ω_1 and reversed, and that C_2 is just C_4 shifted by ω_2 and reversed, this equals

$$\int_{\partial P} \frac{zf'(z)}{f(z)}\,dz = \int_{C_1} \left[\frac{zf'(z)}{f(z)} - \frac{(z+\omega_1)f'(z+\omega_1)}{f(z+\omega_1)}\right] dz + \int_{C_4} \left[\frac{zf'(z)}{f(z)} - \frac{(z+\omega_2)f'(z+\omega_2)}{f(z+\omega_2)}\right] dz.$$

Since f is elliptic, $f(z) = f(z+\omega_1) = f(z+\omega_2)$, giving

$$\int_{\partial P} \frac{zf'(z)}{f(z)}\,dz = -\omega_1 \int_{C_1} \frac{f'(z)}{f(z)}\,dz - \omega_2 \int_{C_4} \frac{f'(z)}{f(z)}\,dz.$$

Now $\ln(f(z))$ can be defined in a neighborhood around C_1 and C_4, since f has no poles or zeros on ∂P. Since $f(\alpha) = f(\alpha+\omega_1) = f(\alpha+\omega_2)$, we have $\ln(f(\alpha+\omega_1)) - \ln(f(\alpha)) = 2\pi i c_1$ and $\ln(f(\alpha)) - \ln(f(\alpha+\omega_2)) = 2\pi i c_2$ for some integers c_1 and c_2. But these equal the above integrals by definition of $\ln f(z)$, so

$$\int_{\partial P} \frac{zf'(z)}{f(z)}\,dz = -2\pi i(\omega_1 c_1 + \omega_2 c_2). \tag{1}$$

Way 2: Note $\operatorname{Res}_a \frac{f'(z)}{f(z)} = \operatorname{ord}_a f$ so $\operatorname{Res}_a \frac{zf'(z)}{f(z)} = a \operatorname{ord}_a f$. Letting a_k be the poles and zeros of f in P, we get by Cauchy's Theorem that

$$\int_{\partial P} \frac{zf'(z)}{f(z)} = 2\pi i \sum_k \operatorname{Res}_{a_k} \frac{f'(z)}{f(z)} = 2\pi i \sum_k m_k a_k. \tag{2}$$

Equating (1) and (2) give

$$\sum_k m_k a_k = -\omega_1 c_1 - \omega_2 c_2 \equiv 0 \pmod{\Lambda}.$$

Problem 2

For $\alpha \in \Lambda$, let $P_\alpha = \{\alpha + t_1\omega_1 + t_2\omega_2 | t_i \in [0,1)\}$. Let d be the diameter of P. Let $C_{m,n} = \{x : m \le |x| < n\}$. Let

$$\mathcal{R}_n = \bigcup_{\alpha \in \Lambda \cap C_{n-1,n}} P_\alpha.$$

The area of $\mathcal{R}_n$ is related to the number of points of Λ in the annulus by a constant:

$$[\mathcal{R}_n] = |\Lambda \cap C_{n-1,n}|[P] \tag{3}$$

($[\cdot]$ denotes area.) Next note that no point of $\mathcal{R}_n$ can be more than distance d away from $C_{n-1,n}$, since each P_α has diameter d and contains the point $\alpha \in C_{n-1,n}$. Hence $R_n \subseteq C_{n-d-1,n+d}$, and for $n \ge d+1$,

$$[\mathcal{R}_n] \le [C_{n-d-1,n+d}] = \pi((n+d)^2 - (n-d-1)^2) \le \pi(4d+2)n. \tag{4}$$

From (3) and (4) we get

$$|\Lambda \cap C_{n-1,n}| \le \frac{\pi(4d+2)}{[P]} n$$

Hence for $s > 2$, letting $m = \lceil d \rceil$,

$$\sum_{\lambda \in \Lambda - \{0\}} \frac{1}{|\lambda|^s} = \sum_{\lambda \in (\Lambda - \{0\}) \cap C_{0,m}} \frac{1}{|\lambda|^s} + \sum_{n=m+1}^{\infty} \sum_{\lambda \in \Lambda \cap C_{n-1,n}} \frac{1}{|\lambda|^s}.$$

The first sum is finite since a lattice is discrete, while

$$\sum_{\lambda \in \Lambda \cap C_{n-1,n}} \frac{1}{|\lambda|^s} \le |\Lambda \cap C_{n-1,n}| \frac{1}{(n-1)^s} \le \frac{\pi(4d+2)}{[P]} \cdot \frac{n}{(n-1)^s}.$$

Hence the second sum converges by comparison to the convergent series $\sum_{n \ge 1} \frac{1}{n^{s-1}}$ (since $s - 1 > 1$).

Problem 3

(A)

There exists α such that $\alpha\Lambda_1 = \Lambda_2$ (the lattices are homothetic) if and only if their corresponding elliptic curves are isomorphic, $E(\Lambda_1) \cong E(\Lambda_2)$. The j-invariant of Λ is equal to the j-invariant of $E(\Lambda)$ so it suffices to show that two elliptic curves in the form $y^2 = x^3 + ax + b$ are isomorphic iff their j-invariants are equal.

(The equation of $E(\Lambda)$ is $y^2 = 4x^3 - g_2x - g_3 = 0$ which under change of coordinates becomes $y^2 = x^3 - 4g_2x - 16g_3$. By definition the j-invariant of this elliptic curve is $j(E) = \frac{1728(4(-4g_2)^3)}{16(4(-4g_2)^3+27(-16g_3)^2)} = \frac{1728g_2^3}{g_2^3-27g_3^2} = j(\Lambda)$.)

Let $y^2 = x^3 + ax + b$ be an elliptic curve. Two elliptic curves are isomorphic over $\mathbb{C}$ iff they are related by a change of coordinates; the only possible change of coordinates keeping this form of the equation are $x = u^2x', y = u^3y'$ which transform the equation to

$$y'^2 = x'^3 + a'x' + b', \quad a' = \frac{a}{u^4}, b' = \frac{b}{u^6}. \tag{5}$$

The new j-invariant is

$$j' = \frac{1728(4a')^3}{16(4a'^3 + 27b'^2)} = \frac{1728(4a)^3}{16(4a^3 + 27b^2)} = j.$$

Hence if two elliptic curves are isomorphic then their j-invariants are equal. Conversely, suppose the j-invariants of $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$ are equal. Then $\frac{1728(4a')^3}{16(4a'^3+27b'^2)} = \frac{1728(4a)^3}{16(4a^3+27b^2)}$, giving $a^3b'^2 = a'^3b^2$. Either none of a, a', b, b' are zero, or a, a' are zero, or b, b' are zero (since a, b can't both be zero, and neither can a', b'). Hence one of $\left(\frac{b}{b'}\right)^{\frac{1}{6}}$ or $\left(\frac{a}{a'}\right)^{\frac{1}{4}}$ is defined (or they're both defined and equal). Taking u in (5) to be this value transforms the first equation into the second. Hence if two elliptic curves have the same j-invariant then they are isomorphic.

(B)(i)

Let Λ_1 be the set of all points in Λ in the first quadrant or on the positive real axis. Then $\Lambda^* = \Lambda_1 \cup i\Lambda_1 \cup i^2\Lambda_1 \cup i^3\Lambda_1$. Hence

$$\begin{aligned} G_6(\Lambda) &= \sum_{\lambda\in\Lambda^*} \frac{1}{\lambda^6} \\ &= \sum_{\lambda\in\Lambda_1} \left(\frac{1}{\lambda^6} + \frac{1}{(i\lambda)^6} + \frac{1}{(-\lambda)^6} + \frac{1}{(-i\lambda)^6}\right) \\ &= \sum_{\lambda\in\Lambda_1} \left(\frac{1}{\lambda^6} - \frac{1}{\lambda^6} + \frac{1}{\lambda^6} - \frac{1}{\lambda^6}\right) \\ &= 0. \end{aligned}$$

Then $g_3 = 0$ and hence

$$j(\Lambda) = \frac{1728g_2^3}{g_2^3 - 27g_3^2{}^0} = 1728.$$

(ii)

Let Λ_1 be all the points of Λ between the positive real axis and the ray with angle $\frac{2\pi}{3}$, including

the positive real axis but not the other ray. Let $\omega = e^{\frac{2\pi i}{3}}$. Then $\Lambda^* = \Lambda_1 \cup \omega\Lambda_1 \cup \omega^2\Lambda_1$ so

$$\begin{aligned} G_4(\Lambda) &= \sum_{\lambda\in\Lambda^*} \frac{1}{\lambda^4} \\ &= \sum_{\lambda\in\Lambda_1} \left(\frac{1}{\lambda^4} + \frac{1}{(\omega\lambda)^4} + \frac{1}{(\omega^2)^4}\right) \\ &= \sum_{\lambda\in\Lambda_1} (1+\omega+\omega^2)\frac{1}{\lambda^4} \\ &= 0. \end{aligned}$$

Thus $g_2 = 0$ and $j(\Lambda) = 0$.

Problem 4

(A)
Taking logs,

$$\ln\sigma(z) = \ln(z) + \sum_{\lambda\in\Lambda^*} \ln\left(1-\frac{z}{\lambda}\right) + \frac{z}{\lambda} + \frac{1}{2}\left(\frac{z}{\lambda}\right)^2.$$

Then

$$\begin{aligned} \frac{d}{dz}\ln\sigma(z) &= \frac{1}{z} + \sum_{\lambda\in\Lambda^*} \frac{-1/\lambda}{1-\frac{z}{\lambda}} + \frac{1}{\lambda} + \frac{z}{\lambda^2} \\ \frac{d^2}{dz^2}\ln\sigma(z) &= -\frac{1}{z^2} + \sum_{\lambda\in\Lambda^*} -\frac{1}{\lambda^2}\left(\frac{1}{1-\frac{z}{\lambda}}\right)^2 + \frac{1}{\lambda^2} = -\wp(z). \end{aligned}$$

(B)
By periodicity $\wp(z) = \wp(z+\lambda)$. Integrating twice and using (A) gives

$$\ln\sigma(z+\lambda) = \ln\sigma(z) + az + b$$

for some constants a, b. Exponentiating gives

$$\sigma(z+\lambda) = e^{az+b}\sigma(z).$$

(C)(i)
If $\sum_{k=1}^r n_i(z_i) = \lambda$, then replace it with $(\sum_{k=1}^r n_i(z_i)) - (\lambda) + (0)$, to make it equal to 0. (This is okay since modulo Λ, $(\lambda) = (0)$.)

From the infinite product, $\sigma(z)$ has a simple zero at each $z \in \Lambda$ and no other zeros or poles. Let $f(z) = \prod_{k=1}^r \sigma(z-z_k)^{n_k}$; note f is meromorphic. From the above observation, $f(z)$ has a zero/pole of order n_k at each z_k, and no other zeros modulo Λ, so $\operatorname{div}(f) = \sum_{k=1}^r n_i(z_i)$.

Next we show that f is elliptic. From (B), for $\lambda \in \Lambda$ we have

$$\begin{aligned} f(z+\lambda) &= \prod_{k=1}^{r} \sigma(z+\lambda-z_k)^{n_k} \\ &= \prod_{k=1}^{r} e^{n_k(a(z-z_k)+b)} \sigma(z-z_k)^{n_k} \\ &= e^{(az+b)\sum_{k=1}^{r} n_k + (-a)\sum_{k=1}^{r} n_k z_k} f(z) = f(z). \end{aligned}$$

Hence f is elliptic.

(ii)

First we show that f is an analytic isomorphism. Let (x, y) on the elliptic curve be given. Now $\wp(z) - x$ is a non-constant elliptic function, so it has a zero, say $z = a$. Since $\wp$ is even $z = -a$ is also a zero, and $\wp'(z) = \pm\wp(a)$ depending on whether $z = a$ or $-a$. Now $(x, \pm\wp'(a))$ are exactly the points on E with first coordinate x (from the equation $y^2 = ax^3 + bx + c$). Hence f is surjective. (Note 0 gets sent to the point at infinity.)

Now suppose $\phi(z_1) = \phi(z_2)$. Then $\wp(z) - \wp(z_1)$ has zeros z_1, z_2. Since $\wp(z) - \wp(z_1)$ has exactly two zeros (since it has one pole of order 2), and $\wp$ is even, $z_1 = \pm z_2$. (If $2z_1 \equiv 0 \pmod{\Lambda}$ then $\wp(z) - \wp(z_1)$ has a double zero at z_1, and that is the only zero.) But $\wp'(z_1)$ is odd so

$$\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1)$$

so either $z_1 \equiv z_2 \pmod{\Lambda}$ or $\wp'(z_1) = 0, z_1 \not\equiv z_2 \pmod{\Lambda}$. Let ω_1, ω_2 generate Λ and let $\omega_3 = \omega_1 + \omega_2$. Note $\wp'(\omega_m/2) = 0$ because $\wp'$ is odd and $\omega_m/2 \equiv -\omega_m/2 \pmod{\Lambda}$. Since the equation of the elliptic curve is cubic in x, and $(\wp(z), \wp'(z)) \in E$, these three are the only possible values of $\wp(z)$ given that $\wp'(z) = 0$. Since $\wp(z) - \wp(\omega_m/2)$ is even, it has a double zero at $\omega_m/2$; since its only pole is of order 2 this is its only zero modulo Λ. Hence $\wp(z) \neq \wp(\omega_m)$ for $z \not\equiv \omega_m \pmod{\Lambda}$. This shows ϕ is injective.

Next to show that ϕ is analytically an isomorphism, note $\frac{dx}{y}$ is a nonvanishing holomorphic differential on E, and

$$\phi^*(dx/y) = d\wp(z)/\wp'(z) = dz$$

is nonvanishing holomorphic on $\mathbb{C}/\Lambda$.

From part (i), there exists f such that

$$\operatorname{div}(f) = (z_1 + z_2) - (z_1) - (z_2) + (0).$$

Since every elliptic function is a rational combination of $\wp$ and $\wp'$, we can write $f = F(\wp, \wp')$ for some $F \in \mathbb{C}(x, y)$. The function f on $\mathbb{C}/\Lambda$ corresponds to F on E, since $f = F \circ \phi$. Since ϕ is an analytic isomorphism, it preserves zeros and poles:

$$\operatorname{div}(F) = (\phi(z_1 + z_2)) - (\phi(z_1)) - (\phi(z_2)) + (0).$$

Hence $(\phi(z_1 + z_2)) - (\phi(z_1)) - (\phi(z_2)) + (0)$ is a principal divisor. From [1, III.3.5], $\phi(z_1 + z_2) - \phi(z_1) - \phi(z_2) + 0 = 0$, so $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$.

(D)
Note $\wp(z)$, and hence $\wp(z) - \wp(a)$, has a pole of multiplicity 2 at $z = 0$ and no other poles. Hence its zeros have total multiplicity 2. Now $\wp(z) - \wp(a)$ has a zero at $z = a$; since it is even it has a zero at $z = -a$. (If $a \equiv -a \pmod{\Lambda}$ then this is a zero of multiplicity 2.) By the construction in (C), $\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2}$ has zeros and poles with the same orders as $\wp(z) - \wp(a)$. Now the quotient between these two functions is entire and bounded (since its maximum and minimum are attained on the (closed) fundamental parallelogram, which is compact), so a constant, by Liouville's Theorem.

To find the constant, we note that $z^2(\wp(z) - \wp(a))$ equals 1 at $z = 0$ (the coefficient of $\frac{1}{z^2}$ in the Laurent expansion is 1), while (using the fact that the expansion of $\sigma(z)$ is $z + \cdots$, and σ is odd as $\Lambda^* = -\Lambda^*$)

$$z^2 \left. \frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2} \right|_{z=0} = \sigma(a)\sigma(-a) = -\sigma(a)^2.$$

Hence the constant is $-\frac{1}{\sigma(a)^2}$, and

$$\wp(z) - \wp(z) = -\frac{\sigma(z+a)\sigma(z-a)}{\sigma(z)^2\sigma(a)^2}.$$

References

[1] Silverman, J.: "The Arithmetic of Elliptic Curves," Springer, 1986.