Elliptic curves, Eisenstein series, and Bernoulli numbers

Nicolas Diaz-Wahl

1 Recap

We looked at complex tori $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \subset \mathbb{C}$, and wanted to understand meromorphic Λ-periodic (doubly periodic) functions. We associated to them their Weierstrass $\wp$-function

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\lambda \neq 0} \frac{1}{\lambda^2} - \frac{1}{(z-\lambda)^2} = \frac{1}{z^2} + \sum_{n \geq 1} (2n+1) G_{2n+2}(\Lambda) z^{2n}.$$

which was Λ-periodic and satisfied the differential equation

$$\wp'_\Lambda(z)^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda), \quad g_2(\Lambda) = 60G_4(\Lambda), \quad g_3 = 140G_6(\Lambda)$$

and that all meromorphic Λ-periodic functions are in $\mathbb{C}(\wp_\Lambda, \wp'_\Lambda)$ which is precisely the function field of an algebraic curve. We found that there were correspondences

$$SL_2(\mathbb{Z})\backslash\mathcal{H} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Lattices} \\ \Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2 \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Complex tori} \\ \mathbb{C}/\Lambda \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Complex elliptic curves} \\ y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \end{array} \right\}$$

$$SL_2(\mathbb{Z})\tau \longmapsto \Lambda_\tau = \mathbb{Z} \oplus \mathbb{Z}\tau \longmapsto \mathbb{C}/\Lambda_\tau \longmapsto \begin{array}{c} V_+(y^2z = 4x^3 - g_2(\tau)xz^2 - g_3(\tau)z^3)(\mathbb{C}) \\ \subset \mathbb{P}^2(\mathbb{C}) \end{array}$$

We found that the *Eisenstein series*

$$G_{2k}(\Lambda) = \sum_{\lambda \in \Lambda'} \frac{1}{\lambda^{2k}}$$

could be considered as functions on $\mathcal{H}$ via

$$G_{2k}(z) = G_{2k}(\Lambda_z = \mathbb{Z} + \mathbb{Z}z)$$

and these functions were modular of weight $2k$.

Definition 1. A *modular form of weight k for* $\Gamma \subset SL_2(\mathbb{Z})$ is a map $f : \mathcal{H} \to \mathbb{C}$ such that

(a) $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ for all $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma$,

(b) f is holomorphic on $\mathcal{H}$,

(c) f is *holomorphic at* ∞, i.e. $f(z)$ is bounded as $\Im z \nearrow \infty$.

Dropping (b) and (c) is called *weakly modular*; replacing (b) with "meromorphic" and (c) with the obvious definition of "meromorphic at ∞" gives the notion of an *modular function of weight k for Γ*.

Since $SL_2(\mathbb{Z})$ is generated by $\left[\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right]$, and $\left[\begin{smallmatrix}0 & 1\\ -1 & 0\end{smallmatrix}\right]$, hence (weak) modularity is equivalent to the two conditions

$$f(z+1) = f(z), \quad f(-1/z) = z^k f(z).$$

In particular, modular functions are periodic, and therefore admit Fourier expansions (called *q-series*)

$$f(z) = \sum_{n \geq 0} a_n q^n, \quad \sum_{n \gg -\infty} a_n q^n, \quad q = \exp(2\pi i z).$$

Condition (c) means that the Laurent series is a power series. If $a_0 = 0$, f is a *cusp form*.

Example 1. All our examples so far are for $SL_2(\mathbb{Z})$;

1. $G_{2k}(z)$ is modular of weight $2k$. It's Fourier expansion is

$$G_{2k}(q) = 2\zeta(2k)\left(1 - \frac{2k}{B_{2k}} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n\right).$$

   $E_{2k} = \frac{1}{\zeta(2k)} G_{2k}$ is the *normalized Eisenstein series*, and has rational coefficients.

2. The *modular discriminant* $\Delta(z) = g_2(z)^3 - 27 g_3(z)^2$ is modular of weight 12; it's a *cusp form* with Fourier series

$$\Delta(q) = q - 24q^2 + 252q^3 - 1472q^4 + \cdots$$

3. The *modular/j-invariant* $j(z) = 1728 \frac{g_2(z)^3}{\Delta(z)}$ is modular of weight 0; it's Fourier series is

$$j(q) = \frac{1}{q} + 744 + 197884q + \cdots.$$

   In particular, j is a modular function, not a modular form. Determines complex elliptic curves up to isomorphism, and is surjective. Hence

$$SL_2(\mathbb{Z}) \backslash \mathcal{H} \xrightarrow{SL_2(\mathbb{Z}) z \mapsto j(z)} \mathbb{A}^1_{\mathbb{C}}$$

   is an isomorphism of Riemann surfaces. We will compactify later.

It is clear that the spaces $M_k(SL_2(\mathbb{Z}))$, $S_k(SL_2(\mathbb{Z}))$ are $\mathbb{C}$-vector spaces. Moreover,

$$M(SL_2(\mathbb{Z})) = \bigoplus_{k \geq 0} M_k(SL_2(\mathbb{Z})) = \mathbb{C}[E_4, E_6],$$

and

$$S(SL_2(\mathbb{Z})) = \bigoplus_{k \geq 0} S_k(SL_2(\mathbb{Z})) = \Delta M(SL_2(\mathbb{Z})).$$

We will see later that $M_k(SL_2(\mathbb{Z}))$ are finite-dimensional.

2 Level Structures

2.1 Concrete motivation

Recall that $E_{2k}(z)$ are only modular for $k \geq 2$. Hence there are no modular functions of weight 2. However, we may define the *twisted Eisenstein series*

$$E_{2,N}(z) = E_2(z) - NE_2(Nz)$$

This function satisfies $E_{2,N}(\gamma z) = j(\gamma, z)^2 E_{2,N}(z)$ *only for* γ in a certain subgroup $\Gamma_0(N)$ of $SL_2(\mathbb{Z})$. It is still holomorphic (at infinity), so $E_{2,N} \in M_2(\Gamma_0(N))$. It has Fourier expansion

$$E_{2,N} = \frac{N-1}{24} + \sum_{n \geq 1} \sigma^*(n) q^n \quad \text{where } \sigma^*(n) = \sum_{0<d|n,\ (d,N)=1} d.$$

Consider the sequences $r_p(n,k) = \{(x_1, \ldots, x_n) \ : \ x_1^p + \cdots + x_k^p = n\}$. Set $r(n,k) = r_2(n,k)$, and define the *theta function*

$$\theta(z,k) = \sum_{n \geq 0} r(n,k) q^n, \ \ q = \exp(2\pi i z), \ z \in \mathcal{H}.$$

For $k = 4$, we have that $\theta(z,4)$ is modular of weight 4 for $\Gamma_0(4)$. One can show that $M_2(\Gamma_0(4))$ is 2-dimensional, and generated by $E_{2,2}(z)$, $E_{2,4}(z)$, so $\theta(4,z) = aE_{2,2} + bE_{2,4}$. In fact,

$$\theta(z,4) = E_{2,4}(z) \implies r(n,4) = 8 \sum_{d|n,\ 4\nmid d} d, \ \ n \geq 1,$$

so every integer is the sum of four squares.

2.2 Abstract motivation

There is a paucity of modular forms for $SL_2(\mathbb{Z})$. Considering subgroups $\Gamma \subset SL_2(\mathbb{Z})$ weakens the modular condition and produces many new families of modular forms. Let $N \geq 1$ be an integer. The reduction map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective (try and prove it!). The subgroups we will be interested are the so-called *congruence subgroups*:

(a)

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \bmod N \right\} = \ker(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})).$$

(b)

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \bmod N \right\}$$

(c)

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \bmod N \right\}$$

We have

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N).$$

We will see that the quotient spaces $Y_{(i)}(N) := \Gamma_{(i)}\backslash\mathcal{H}$ parametrize elliptic curves with *torsion data*. We will now say "(complex) elliptic curve" in place of "complex torus". Given an elliptic curve $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, it's N-torsion is

$$E[N](\mathbb{C}) = \{P \in E(\mathbb{C}) \ : \ NP = 0\} \simeq \frac{1}{N}\Lambda/\Lambda \cong (\mathbb{Z}/N\mathbb{Z})^2.$$

We will consider the sets

$$S_0(N) = \{(E, C) \ : \ E \text{ elliptic curve, } C \subset E[N] \text{ cyclic subgroup of order } N\}/\sim \simeq \{(E_\tau, \langle 1/N + \Lambda_\tau\rangle)\}/\sim$$
$$S_1(N) = \{(E, P) \ : \ E \text{ elliptic curve, } P \in E[N] \text{ a point of exact order } N\}/\sim \simeq \{(E_\tau, 1/N + \Lambda_\tau)\}/\sim$$
$$S(N) = \{(E, (P, Q)) \ : \ E \text{ elliptic curve, } \langle P, Q\rangle \in E[N]\}/\sim \simeq \{(E_\tau, (1/N + \Lambda_\tau, \tau/N + \Lambda_\tau))\}/\sim$$

where $(E, C) \sim (E', C')$ (resp. $(E, P) \sim (E', P')$, resp. $(E, (P, Q)) \sim (E', (P', Q'))$) if there exists $\varphi : E \xrightarrow{\sim} E'$ such that $\varphi(C) = C'$ (resp. $\varphi(P) = Q$, resp. $\varphi(P, Q) = (P', Q')$).

Theorem 2. *Let $N \geq 1$. There are "natural" bijections*

(a)
$$S_0(N) \to Y_0(N)(\mathbb{C}) : [(E_\tau, \langle 1/N + \Lambda_\tau\rangle)] \mapsto \Gamma_0(N)\tau,$$

(b)
$$S_1(N) \to Y_1(N)(\mathbb{C}) : [(E_\tau, 1/N + \Lambda_\tau)] \mapsto \Gamma_1(N)\tau,$$

(c)
$$S(N) \to Y(N)(\mathbb{C}) : [(E_\tau, (1/N + \Lambda_\tau, \tau/N + \Lambda_\tau))] \mapsto \Gamma(N)\tau.$$

Proof. Do (a) and (c) as exercises.

(b) (Surjective and well-defined I) Take $(E, P) \in S_1(N)$. We have $E \simeq \mathbb{C}/\Lambda_\tau$, so $P = (c\tau + d)/N + \Lambda_\tau$ for some $\tau \in \mathcal{H}$ for $c, d \in \mathbb{Z}$ with $\gcd(c, d, N) = 1$ (since P has exact order N). We will multiply Λ_τ and P by some $m \in \mathbb{C}^*$ so that $m^{-1}P$ is of the form $1/N + \Lambda_{\gamma\tau}$. This gives an isomorphic pair of the desired form.

Hence $ad - bc - kN = 1$ for $a, b, k \in \mathbb{Z}$, and $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ reduces to I mod N; since $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective, can choose $\gamma \in SL_2(\mathbb{Z})$.

Set $\tau' = \gamma\tau = \frac{a\tau+b}{c\tau+d}$, so if $m = c\tau + d$, then $m\tau' = a\tau + b$, i.e.

$$m\Lambda_{\tau'} = m(\tau'\mathbb{Z} + \mathbb{Z}) = (a\tau + b)\mathbb{Z} + (c\tau + d)\mathbb{Z} = \tau\mathbb{Z} + \mathbb{Z} = \Lambda_\tau,$$

and

$$m\left(\frac{1}{N} + \Lambda_{\tau'}\right) = \frac{c\tau + d}{N} + \Lambda_\tau = P,$$

so $(E, P) \sim (\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'})$.

(Injective) Suppose $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$, i.e. $\tau = \gamma(\tau')$ for $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \Gamma_1(N)$.

Again, let $m = c\tau' + d$. Then $m\Lambda_\tau = \Lambda_{\tau'}$, $m(1/N + \Lambda_\tau) = (c\tau' + d)/N + \Lambda_{\tau'}$ (as above). Since $(c, d) \equiv (0, 1) \bmod N$, the second equality is now $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$, thus

$$(\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau) \sim (\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}).$$

(Well-defined II) Suppose $(\mathbb{C}/\Lambda_\tau, 1/N+\Lambda_\tau) \sim (\mathbb{C}/\Lambda_{\tau'}, 1/N+\Lambda_{\tau'})$ with $\tau, \tau' \in \mathcal{H}$. Hence $m\Lambda_\tau = \Lambda_{\tau'}$ for some $m \in \mathbb{C}$ and $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$. Therefore

$$\begin{bmatrix} m\tau \\ m \end{bmatrix} = \gamma \begin{bmatrix} \tau' \\ 1 \end{bmatrix} \quad \text{for some } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$$

so $m = c\tau' + d$. The second condition becomes

$$\frac{c\tau' + d}{N} + \Lambda_{\tau'} = \frac{1}{N} + \Lambda_{\tau'},$$

i.e. $(c, d) \equiv (1, 0) \bmod N$, so $\gamma \in \Gamma_1(N)$. Since $\tau = \gamma(\tau')$, we have $\Gamma_1(N)\tau = \Gamma_1(N)\tau'$ and we win. $\square$