Week 2: 01/08 - 01/14

1 Diamond,Shurman - Chapter 1: Modular Forms, Elliptic Curves, and Modular Curves

The goal of this chapter is to define the objects in the title. Importantly, we will develop different languages to talk about elliptic curves. A point of great interest will be that elliptic curves and complex torii are in bijection.

1.1 1.1-1.2: Modular forms

The story begins in the complex upper half plane $\mathcal{H} = \{\tau \in \mathbb{C} : Im(\tau) > 0\}$. We are intrested in the action of $SL_2(\mathbb{Z})$, given by the following:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$$

Proposition 1.1. *This is indeed an action.*

Proof. Let $j(\gamma, \tau) = c\tau + d$. We need to verify:

- $Im(\gamma(\tau)) > 0$; we can in fact show $Im(\gamma(\tau)) = \frac{Im(\tau)}{|j(\gamma,\tau)|^2}$
- $1(\tau) = \tau$
- $\gamma(\gamma'(\tau)) = (\gamma\gamma')(\tau)$

All three are routine, using the identity $ad - bc = 1$. □

We extend this idea further, and apply it to function of the upper half plane.

Definition 1.1. For $\gamma \in SL_2(\mathbb{Z})$ and $k \in \mathbb{Z}$ we define the weight-k operator $[\gamma]_k$ on $f : \mathcal{H} \to \mathbb{C}$ by

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau))$$

Notice that f and $f[\gamma]_k$ have the same zeros and poles. We say a function is *weakly modular (of weight k)* if $f[\gamma]_k = f$ for all $\gamma \in SL_2(\mathbb{Z})$. It can be shown that $SL_2(\mathbb{Z})$ is generated by $\tau \to \tau + 1$ and $\tau \to -1/\tau$. Also, $[\gamma]_k[\gamma']_k = [\gamma\gamma']_k$. Together, these facts imply that being to check weakly modularity, we only need to check $f(\tau + 1) = f(\tau)$ and $f(-1/\tau) = \tau^k f(\tau)$. This might seem like an extremely restrictive condition, and indeed it is. For example,

Proposition 1.2. *There are no nonzero weakly modular forms of odd weight.*

Proof. The matrix -1 is in $SL_2(\mathbb{Z})$, and remark that $f[-1]_k = -f$. Suppose f is weakly modular of odd weight k. Then, $f[-1]_k = f$, so $f = -f$ for all τ which implies $f = 0$. □

For a function to be (fully) modular, we add a ”niceness” condition.

Definition 1.2. A function $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k if

- $f[\gamma]_k = f$ for all $\gamma \in \Gamma$
- f is holomorphic on $\mathcal{H}$
- f is holomorphic at ∞

If we add that $a_0 = 0$ in the Fourier expansion of all $f[\alpha]_k$, then f is a cusp form.

Recall that f being holomorphic at ∞ means $g(q) = g(log(q)/(2\pi i))$ defined on $B' = B(0,1)\backslash 0$ extends holomorphically to $q = 0$. This comes from the intuition that under the biholomorphic equivalence of $\mathcal{H}$ and D, the ”point at infinity” is mapped to 0. Recall also that this condition guarantees existence of a Fourier expansion, justifying the last remark.

We now ask what structure the set $\mathcal{M}_k$ of modular forms of weight k has. Further, let $\mathcal{M} = \bigoplus \mathcal{M}_k$.

Proposition 1.3. *Each $\mathcal{M}_k$ forms a complex vector space. Further, $\mathcal{M}$ is a graded ring.*

Proof. Let $f \in \mathcal{M}_k$, $g \in \mathcal{M}_{k'}$, and $\lambda \in \mathbb{C}$.
Suppose $k = k'$. Then, $(f + \lambda g)[\gamma]_k = f[\gamma]_k + \lambda g[\gamma]_k = f + \lambda g$, and the holomorphy conditions are respected. This shows $\mathcal{M}_k$ is a vector space over $\mathbb{C}$.
Now, we show that fg is also modular, but of weight $k + k'$. This gives the (graded) ring structure to $\mathcal{M}$.

$$(fg)[\gamma]_{k+k'}(\tau) = j(\gamma, \tau)^{k+k'} f(\tau)g(\tau) = j(\gamma, \tau)^k f(\tau) j(\gamma, \tau)^{k'} g(\tau) = f(\tau)g(\tau)$$

□

1.2 Particular functions

We describe explicitely a family of modular forms, called Eisenstein series. Then, we make a cusp form out of them.

Definition 1.3. The Eisenstein series of weight k is a modular form, for k an even number bigger than 3.

$$G_k(\tau) = \sum_{\omega \in \mathbb{Z} \oplus \tau\mathbb{Z} \backslash 0} \frac{1}{w^k}$$

It is indeed modular, since $\gamma(\tau)$ is a lattice point of $\mathbb{Z} \oplus \tau\mathbb{Z}$.

Proposition 1.4. *The sum $G_k(\tau)$ converges uniformly.*

An intresting result, to be proven in chapter 3, is that Eisenstein series generate $\mathcal{M}_k$. In fact, $\mathcal{M} = \mathbb{C}[E_4, E_6]$. For example, $\mathcal{M}_8 = \mathbb{C}[E_8]$. Note that E_4^2 is of weight 8, and has constant term 1. Hence, $E_4^2 = E_8$.
For a cusp form, we can combine Eisenstein series to cancel the constant term.

Definition 1.4. Write $g_2(\tau) = 60G_4(\tau)$, and $g_3(\tau) = 140G_6(\tau)$.
Then, the discriminant function $\Delta(\tau) = (g_2(\tau))^3 - 27(g_3(\tau))^2$ is a cusp form.

Finally, we define a weakly-modular form of weight 0. That is, an $SL_2(\mathbb{Z})$-invariant function. To do this, divide two modular forms of same weight. The difficulty lies in getting a modular form that never vanishes. That $\Delta(\tau)$ does the job will be proven later.

$$j(\tau) = 1728\frac{(g_2(\tau))^3}{\Delta(\tau)}$$

Note that both the numerator and denominator have the same weight, so the function is indeed weakly-modular of weight 0. It has a pole at infinity, so it is not modular.
We end by computing some values of the aforedefined functions.

Proposition 1.5. *We have $j(i) = 1728$, $g_2(i) = 4\varpi_4^4$, $g_3(i) = 0$. Also, $j(\zeta_3) = 0$, $g_2(\zeta_3) = 0$, $g_3(\zeta_3) = \frac{27}{16}\varpi_3^6$.*

Proof. Note that $\gamma\mu_3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\mu_3 = -1/\mu_3 = -\mu_3^2 = \mu_3 + 1$, so $g_2(\gamma\mu_3) = g_2(\mu_3)$. But, again using modularity, $g_2(\gamma\mu_3) = \mu_3^4 g_2(\mu_3)$. Hence $g_2(\mu_3) = 0$. The same argument shows $g_3(i) = 0$.
Since $\Delta(\tau)$ is never 0 on $\mathcal{H}$, $g_2(\tau) = 0$ forces $g_3(\tau) \neq 0$ and inversly. For the values of $j(i)$ and $j(\mu_3)$, simply plug in the previous results.
The other identities are more difficult; the proofs do not fit on this margin. □

We can already get a taste of the relation with number theory with the following fact.

Proposition 1.6. *The normalized Eisenstein series $E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)}$ has rational coefficient for $k \geq 2$ even.*

Proof. The proof is at the end of this notes, for it is long and would crowd the discussion. □

1.3 1.3: Complex Torii

A lattice is an abelian group $\Lambda_{\omega_1}^{\omega_2} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} \subset \mathbb{C}$. Notice that the quotient $\mathbb{C}/\Lambda$, geometrically, is a torus. Since the set is unchanged as we replace ω_i by a multiple, we can make the normalizing convention that $\omega_1/\omega_2 \in \mathcal{H}$.

Lemma 1.1. $\Lambda_{\omega_1}^{\omega_2} = \Lambda_{\omega_1'}^{\omega_2'}$ *iff* $\omega_1'/\omega_2' = \gamma(\omega_1/\omega_2)$ *for some* $\gamma \in SL_2(\mathbb{Z})$.

Proof. Since $\omega_i \in \Lambda_{\omega_1'}^{\omega_2'}$, we have $\omega_1 = a\omega_1' + b\omega_2'$ and $\omega_2 = c\omega_1' + d\omega_2'$. In matrix form, $\omega_1'/\omega_2' = \gamma(\omega_1/\omega_2)$. Because the lattices are equal, their cells (parallelograms) have the same area. Since $det(\gamma)$ is governing how area is scaled, this forces $det(\gamma) = \pm 1$. The assumption that ω_1'/ω_2' and ω_1/ω_2 were both in the upper half plane guarantees $det(\gamma) = 1$. □

Algebraically, this quotient is $\mathbb{C}/\Lambda = \{z + \Lambda\}$. We will be intrested in the study of functions $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$. Given the structure, we can ask that these are both holomorphic and group homomorphisms. Such a function is called an isogeny. The following results give a classification.

Proposition 1.7. *Let $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be holomorphic. Then, $\phi(z + \Lambda) = mz + b\Lambda'$ for complex numbers m, b such that $m\Lambda \subset \Lambda'$. Moreover, ϕ is a bijection iff there is equality.*

Proof. Consider $\widetilde{\phi} : \mathbb{C} \to \mathbb{C}$, the lift of ϕ. This $\widetilde{\phi}$ is still holomorphic.
Now, for all $\lambda \in \mathbb{C}$, consider $f_\lambda(z) = \widetilde{\phi}(z + \lambda) - \widetilde{\phi}(z)$. The image of this map is discrete by construction, and hence constant. Thus $\widetilde{\phi}'$ is bounded, which makes it constant by Liouville. Hence $\widetilde{\phi}(z) = mz + b$, which composes with the covering map to give $\phi(z + \Lambda) = mz + b + \Lambda'$. □

Proposition 1.8. *Let $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be holomorphic. TFAE:*

- *ϕ is a homomorphism*
- *$b \in \Lambda'$*
- *$\phi(0) = 0$.*

Proof. We write $Z = z + \Lambda$. $(i) \iff (ii)$: By the previous proposition, $\phi(z + \Lambda) = mz + b + \Lambda'$. If $\phi(Z + Z') = \phi(Z) + \phi(Z')$, then $mz + b + mz' + b + \Lambda' = m(z + z') + b + \Lambda'$. That is to say, $b + \lambda' = \Lambda'$. Conversly, $\phi(Z + Z') = mz + mz' + \Lambda' = mz + \Lambda' + mz' + \Lambda' = \phi(Z) + \phi(Z')$.
That (ii) and (iii) are equivalent is trivial. □

Hence, complex torri are holomorphically isomorphic iff $m\Lambda = \Lambda'$ for some m. This allows us to rewrite every torus as $\Lambda_{\omega_1}^{\omega_2} = \mathbb{Z} + \tau\mathbb{Z}$ for $\tau = \omega_1/\omega_2$, since the map $\phi(z + \Lambda_{\omega_1}^{\omega_2}) = z/\omega_2 + \Lambda_\tau$ is an isomorphism (since $1/\omega_2\Lambda_{\omega_1}^{\omega_2} = \Lambda_\tau$). By the first above lemma, $\Lambda_\tau = \Lambda_{\tau'}$ iff τ and τ' are in the same $SL_2(\mathbb{Z})$-orbit. Hence, isogeny classes of torii are in correspondence with orbits of $SL_2(\mathbb{Z})$ acting on $\mathcal{H}$.
General things can be said about isogenies.

Proposition 1.9. *Every (nontrivial) isogenie ϕ is sujective and has finite kernel.*

Proof. This comes from topology and complex analysis. Every torus is compact, and by the open mapping theorem, $\phi(\mathbb{C}/\Lambda)$ is clopen. Since ϕ is nontrivial, this makes it surjective. From complex analysis, the preimage of singletons under holomorphic maps is discrete. In particular, $ker(\phi)$ is discrete, and hence finite since $\mathbb{C}/\Lambda$ is compact. □

A particular type of isogeny is $[N] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ given by $[N](z + \Lambda) = Nz + \Lambda$. The kernel is written $E[N]$, and it's elements can be thought of as torsion points.
Another type of isogeny is $\pi_C : \mathbb{C}/\Lambda \to \mathbb{C}/C$ for C a cyclic subgroup of $E[N]$ (note $\mathbb{C}/C$ forms a superlattice of $\mathbb{C}/\Lambda$.

Proposition 1.10. *Every isogeny is a composition of some $[N]$ and π_C.*

1.4 1.4: Complex torii and Elliptic Curves

Definition 1.5. An elliptic curve is a the solution set of the equation $y^2 = 4x^3 - a_2x - a_3$.

The goal of this section is to establish a correspondence between the torii and elliptic curves. To this end, we use the Weirstress $\wp$ function. Note that it is doubly periodic.

$$\wp(z) = \frac{1}{z^2} + \sum_{\Lambda \backslash 0} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

It's derivative, $\wp'(z) = -1 \sum_\Lambda \frac{1}{(z-\omega)^3}$ is also of interest. Note that $\wp$ depends on the lattice, which we omit from the notation. By using the geometric series, swapping order of the summation (since things converge), and cancelling odd powers when summed over the lattice, we get

$$\wp(z) = \frac{1}{z^2} + \sum_{2 \leq n \text{ even}} (n+1)G_{n+2}(\Lambda)z^n$$

Before stating the result, we need to introduce a new function. We generalize the Eisenstein series to $G_k(\Lambda) = \sum' \frac{1}{\omega^k}$, so $G_k(\tau) = G_k(\Lambda_\tau)$.

Theorem 1.1. *For a lattice Λ, the map $z \to (\wp(z), \wp'(z))$ is a map from $\mathbb{C}/\Lambda \to$ elliptic curve. Precisely, for all $z \in \mathbb{C}\backslash\Lambda$,*

$$(\wp(z))^2 = 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$$

Proof. Recall that $\wp(z) = \frac{1}{z^2} + 3G_4(\Lambda)z^2 + 4G_6(\Lambda)z^4 + z^6(...)$. Keeping track of the terms of order less than z^2, we get $(\wp'(z))^2 \sim_2 4(\wp(z))^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$ (by which we mean their difference is $\mathcal{O}(z^2)$).
So their difference is a holomorphic and doubly periodic function, so it's bounded, hence constant. But it goes to 0 as $z \to \infty$, so the difference is 0. □

Theorem 1.2. *Given an ellitpic curve $E : y^2 = 4x^3 - a_2x - a_3$ with $\Delta = a_2^3 - 27a_3^2 \neq 0$, there is a lattice with $a_2 = g_2(\Lambda)$ and $a_3 = g_3(\Lambda)$, hence a complex torus such that $(\wp, \wp')(\mathbb{C}/\Lambda) = E$.*

Proof. Suppose first $a_2 \neq 0 \neq a_3$. Then, there is a τ such that $j(\tau) = 1728a_2^3/\Delta$ since j surjects. After some algebra, we get

$$\frac{a_2^3}{g_2(\tau)^3} = \frac{a_3^2}{g_3(\tau)^2}$$

Choose ω_2 so that $\omega_2^{-4} = a_2/g_2(\tau)$. Take power $2/3$, and use the above equality to get $\omega_2^{-6} = a_3/g_3(\tau)$.
Now, let $\Lambda = \omega_1\mathbb{Z} \oplus \omega_2\mathbb{Z}$. Note that $\Lambda = \omega_2\Lambda_\tau$, so $g_2(\Lambda) = \omega_2^{-4}g_2(\tau)$ and $g_3(\Lambda) = \omega_2^{-6}g_3(\tau)$, so we are done.
Now if $a_2 = 0$, choose $\Lambda = m\Lambda_{\zeta_3}$. Thus, $g_2(\Lambda) = m^{-3}g_2(\zeta_3) = 0$ and $g_3(\Lambda) = m^{-3}\frac{27}{16}\varpi_3^6$, so we can choose an appropriate m to make $g_3(\Lambda) = a_3$.
For $a_3 = 0$, choose $\Lambda = m\Lambda_i$ for $m = \frac{16\varpi_4^8}{a_2^2}$. □

Hence to every complex torus, we can associate an ellptic curve, and inversly. Write E_τ for the elliptic curve corresponding to $\mathbb{C}/\Lambda_\tau$.

We end this section by noting that since $\mathbb{C}/\Lambda$ was an abelian group, we can carry the group law on the elliptic curve it corresponds to. In a word, the group law is defined by colinear triples on E summing to 0.

1.5 1.5: Modular Curves

We have shown that complex torii and elliptic curves are in correspondence, so we use the terms interchangably. Recall $E[N] = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, the kernel of the map $[N]$.
Our goal is to link this story back to the upper half plane, and later to modular forms. First, we have to introduce the notion of congruence subgroups. Being modular for the whole modular group is very restrictive (there are no forms of odd weights), so we relax the condition.

Definition 1.6. The principal congruence subgroup of level N is

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod N \right\}$$

A congruence subgroup of $SL_2(\mathbb{Z})$ is a subgroup Γ with the property that $\Gamma(N) \subset \Gamma$ for some positive N.
We single out $\Gamma_0(N)$ and $\Gamma_1(N)$.

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \colon \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod N \right\}$$

Definition 1.7. An enhanced elliptic curve for $\Gamma_0(N)$ is a pair (E, C) consisting of an elliptic curve along with a specified cyclic subgroup.
We impose the following equivalence relation: $(E, C) \sim (E', C')$ if there is an isomorphism $E \to E'$ taking $C \to C'$. Then, define

$$S_0(N) = \{(E, C)\}/\sim$$

Similarily, define enhanced elliptic curves for $\Gamma_1(N)$ by pairs (E, Q) for Q a point of order N, and for $\Gamma(N)$ by triples (E, P, Q) where P, Q generate $E[N] = ker([N])$ such that the Weil pairing $e_N(P, Q) = e^{2\pi i/N}$. We also define relations $(E, Q) \sim (E', Q')$ and $(E, P, Q) \sim (E', P', Q')$ in the obvious way. Then,

$$S_1(N) = \{(E, Q)\}/\sim \qquad S(N) = \{(E, P, Q)\}/\sim$$

The point is that $S_i(N)$ captures the isomorphism classes of elliptic curves, with some torsion-data preserved. In particular, $S_i(1)$ is just the isomorphism classes without looking at the torsion data. These are called *moduli spaces*, and on one side of the bijection we wish to create. We can give an explicit description of these spaces.

Theorem 1.3.

$$S_0(N) = \{[E_\tau, \langle 1/N + \Lambda_\tau \rangle] : \tau \in \mathcal{H}\}$$

$$S_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] : \tau \in \mathcal{H}\}$$

$$S(N) = \{[E_\tau, \tau/N + \Lambda_\tau, 1/N + \Lambda_\tau] : \tau \in \mathcal{H}\}$$

Proof. We do the case of $\Gamma_1(N)$.
By the previous section, E corresponds to a complex torus, so $E = E_\tau$ for some τ'. In this point of view, $Q = (c\tau' + d)/N + \Lambda'_\tau$, where $gcd(c, d, N) = 1$ otherwise Q would have order less than Λ. The goal is to write this element in a simpler form.

Using Bezout's theorem, there are numbers a, b, k so that $ac - bd + kN = 1$, so $ac - bd = 1 \pmod N$. Write $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, which is in $SL_2(\mathbb{Z}/N\mathbb{Z})$. Since $SL_2(\mathbb{Z})$ surjects, we can just as well consider γ as an element of the modular group. Let $\tau = \gamma(\tau')$, and $m = c\tau' + d$. We claim $z + \Lambda_\tau \mapsto mz + \Lambda_{\tau'}$ is a desired isomorphism.

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

$$m(1/N + \Lambda_\tau) = (c\tau' + d)/N + \Lambda_{\tau'} = Q$$

Hence, $(E, Q) = (E_\tau, 1/N + \Lambda_\tau)$ in $S_1(N)$.

Now, the case for $\Gamma_0(N)$.
Let (E, C) an enhanced elliptic curve. Then, $E = E_\tau$ for some $\tau \in \mathcal{H}$, and □

The other side is the following construction. Recall that lattices Λ_τ and Λ'_τ are isomorphic iff $\tau = \tau' \pmod{SL_2(\mathbb{Z})}$. This motivates the following definition.

Definition 1.8. Let Γ a congruence subgroup, which acts on $\mathcal{H}$. The modular curve for Γ is

$$Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}$$

We write $Y_i(N)$ for the modular curve for $\Gamma_i(N)$.

Theorem 1.4. *The modulii spaces and modulii curves are related by the following bijections:*

$$\psi_0 : S_0(N) \to Y_0(N) \qquad [\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] \mapsto \Gamma_0(N)\tau$$

$$\psi_1 : S_1(N) \to Y_1(N) \qquad [\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] \mapsto \Gamma_1(N)\tau$$

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

Proof. Again, we do the case for $\Gamma_1(N)$.

Injectivity: Suppose $\Gamma_1(N)\tau = \Gamma_1(N)\tau$, or simply $\tau = \gamma(\tau')$ for some $\gamma \in \Gamma_1(N)$. Since that $m = j(\gamma, \tau') \equiv 1 \pmod{(N)}$, the isogeny $z + \Lambda_\tau \mapsto mz + \Lambda_{\tau'}$ has $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$. Hence $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$ in $S_1(N)$.

Well-defined: Suppose $[\mathbb{C}/\Lambda_\tau, 1/N + \Lambda_\tau] = [\mathbb{C}/\Lambda_{\tau'}, 1/N + \Lambda_{\tau'}]$. Then, since isogenies are of the form $[m]$, there is $m \in \mathbb{C}$ so that $m\Lambda_\tau = \Lambda_{\tau'}$. Hence $\begin{bmatrix} m\tau \\ m \end{bmatrix} = \gamma \begin{bmatrix} \tau' \\ 1 \end{bmatrix}$ for $\gamma \in SL_2(\mathbb{Z})$, from which $\tau = \gamma(\tau')$; the goal is to show $\gamma \in \Gamma_1(N)$. We also have $mQ = Q'$, so $c\tau' + d = 1 \pmod{N}$. This forces $a = 1$, so we have indeed $\gamma \in \Gamma_1(N)$. Hence $\psi_1(E_\tau, Q) = \psi_1(E_{\tau'}, Q')$ □

We can use these equivalences to create modular forms.

1.6 Extra Computations

The following amounts to exercise 1.1.4. We want to show absolute and uniforme convergence of $G_k(\tau)$ on compact subsets of $\mathcal{H}$, and so holomorphicity on $\mathcal{H}$.

Proof. Let $k \geq 3$. Let's first show that the following series converges :

$$\begin{aligned}
\sideset{}{'}\sum_{(c,d)\in\mathbb{Z}^2} (\sup\{|c|, |d|\}^{-k} &= \lim_{N\to\infty} \sideset{}{'}\sum_{(c,d)\in[-N,N]^2\subset\mathbb{Z}^2} (\sup\{|c|, |d|\}^{-k} \\
&\leq 4 \lim_{N\to\infty} \sideset{}{'}\sum_{(c,d)\in[0,N]^2\subset\mathbb{N}^2} (\sup\{|c|, |d|\})^{-k} \\
&= 4 \lim_{N\to\infty} (\sum_{j=1}^{N} \frac{1}{j^k} + 2\sum_{l=1}^{N} \frac{l}{l^k}) \\
&= 4 \lim_{N\to\infty} (\sum_{j=1}^{N} \frac{1}{j^k} + 2\sum_{l=1}^{N} \frac{1}{l^{k-1}}) \text{ where both terms converge for } k > 2.
\end{aligned}$$

Now, fix positive number A and B and let

$$\Omega = \{\tau \in \mathcal{H} : |\mathrm{Re}(\tau)| \leq A, \mathrm{Im}(\tau) \geq B\}.$$

We show that there is constant $C > 0$ such that $|\tau + \delta| > C\sup\{1, |\delta|\}$ for all $\tau = x + iy \in \Omega$ and $\delta \in \mathbb{R}$. We consider 4 cases :

1. Suppose $|\delta| < 1$. Then $|\tau + \delta| > \sqrt{B^2 + y^2} \geq= B = B\sup\{1, |\delta|\}$.
2. Suppose next that $1 \leq |\delta| \leq 3A$ and $y > A$. Then, $|z + \delta| = \sqrt{(x + \delta)^2 + y^2} \geq A > |\delta|/3 = 1/3\max\{1, |\delta|\}$.

3. Suppose $1 \leq |\delta| \leq 3A$ and $B \leq \mathrm{Im}(\tau) \leq A$. Then, $|\tau+\delta|/|\delta|$ takes a nonzero minimum m, so $|\tau+\delta| \geq m|\delta| = m \cdot \sup\{1, |\delta|\}$.

4. Suppose $|\delta| > 3A$, then $|\tau+\delta| \geq |\delta| - A \geq 2|\delta|/3 = 2\sup\{1,|\delta|\}/3$.

Hence, we can take any positive C less than $\inf\{B, 1/3, m\}$.
We have then on Ω

$$\sum_{(c,d)\in \mathrm{Z}^2}{}' \frac{1}{|c\tau+d|^k} = 2\zeta(k) + \sum_{c\neq 0,d} |c\tau+d|^{-k}$$

Using C from above and with $c \neq 0$,

$$|c\tau+d|^{-k} = (|c||\tau+d/c|)^{-k} \leq \frac{1}{(|c|(C\sup\{1,|d/c|\}))^k} = \frac{1}{((C\sup\{|c|,|d|\}))^k}.$$

By our first result, this shows that $G_k(\tau)$ converges absolutely and uniformly on Ω, and hence is holomorphic on Ω. Since for any compact subset of $\mathcal{H}$ is in some Ω, $G_k(\tau)$, $G_k(\tau)$ is holomorphic on $\mathcal{H}$ by complex analysis. □

The following amounts to exercise 1.1.5, 1.1.7.

Definition 1.9. The Bernoulli numbers are the coefficients in

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

Lemma 1.2.

$$1 - 2\sum_{k=1}^{\infty} \zeta(2k)\tau^{2k} = \pi\tau cot(\pi\tau) = \pi i\tau + \sum_{k=0}^{\infty} B_k \frac{(2\pi i\tau)^k}{k!}$$

Hence, by equating coefficients,

$$2\zeta(k) = -\frac{(2\pi i)^k}{k!}B_k$$

Proof.

$$\begin{aligned}
ln(sin(\pi\tau))' &= \pi cot(\pi\tau) = && \pi\frac{cos(\pi\tau)}{sin(\pi\tau)} \\
ln(\pi\tau\prod_{n=1}^{\infty} 1 - \frac{\tau^2}{n^2}) &= \pi cot(\pi\tau) = && \pi i\frac{e^{\pi i\tau}+e^{-\pi i\tau}}{e^{\pi i\tau}-e^{-\pi i\tau}} \\
\frac{1}{\tau} + \sum_{n=1}^{\infty} \frac{1}{n^2}\frac{n^2}{n^2-\tau^2} &= \pi cot(\pi\tau) = && \pi i\frac{e^{2\pi i\tau}+1}{e^{2\pi i\tau}-1} \\
\frac{1}{\tau} + \sum_{n=1}^{\infty} \frac{1}{n^2}\frac{n^2}{n^2-\tau^2} &= \pi cot(\pi\tau) = && \pi i - 2\pi i\sum_{m=0}^{\infty} e^{2\pi i\tau m}
\end{aligned}$$

Then, we have the following,

$$\begin{aligned}
1+\sum_{d=1}^{\infty}\frac{\tau}{\tau-d}+\frac{\tau}{\tau+d} &= \pi\tau cot(\pi\tau) = & \pi i\tau - 2\pi i\tau\sum_{m=0}^{\infty}e^{2\pi i\tau m}\\
1+\sum_{d=1}^{\infty}\frac{2\tau}{\tau^2-d^2} &= \pi\tau cot(\pi\tau) = & \pi i\tau + \frac{2\pi i\tau}{e^{2\pi i\tau}-1}\\
1-2\sum_{d=1}^{\infty}\frac{\tau^2}{d^2}\frac{1}{1-\frac{\tau^2}{d^2}} &= \pi\tau cot(\pi\tau) = & \pi i\tau + \sum_{k=0}^{\infty}B_k\frac{(2\pi i\tau)^k}{k!}\\
1-2\sum_{d=1}^{\infty}\frac{\tau^2}{d^2}\sum_{k=0}^{\infty}\frac{\tau^{2k}}{d^{2k}} &= \pi\tau cot(\pi\tau) = & \pi i\tau + \sum_{k=0}^{\infty}B_k\frac{(2\pi i\tau)^k}{k!}\\
1-2\sum_{d=1}^{\infty}\sum_{k=1}^{\infty}\frac{\tau^{2k}}{d^{2k}} &= \pi\tau cot(\pi\tau) = & \pi i\tau + \sum_{k=0}^{\infty}B_k\frac{(2\pi i\tau)^k}{k!}\\
1-2\sum_{k=1}^{\infty}\zeta(2k)\tau^{2k} &= \pi\tau cot(\pi\tau) = & \pi i\tau + \sum_{k=0}^{\infty}B_k\frac{(2\pi i\tau)^k}{k!}
\end{aligned}$$

□

Proposition 1.11. *Let $k > 2$ an even number. The normalized Einsenstein series have rational coefficients.*

$$E_k(\tau)=\frac{G_k(\tau)}{2\zeta(k)}$$

Proof. We have

$$\frac{1}{\tau}+\sum_{d=1}^{\infty}\frac{1}{\tau-d}+\frac{1}{\tau+d}=\pi cot(\pi\tau)=\pi i-2\pi i\sum_{m=0}^{\infty}e^{2\pi i\tau m}$$

Differentiate $k-1$ times in τ yields

$$\sum_{d}$$

So that

$$G_k(\tau)=2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$$

Hence, dividing by $2\zeta(k)$ yields

$$\begin{aligned}
E_{2k}(\tau) = &\quad 1-2\tfrac{k!(2\pi k)^k}{B_k(2\pi i)^k(k-1)!}\textstyle\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\\
= &\quad 1-2\tfrac{k}{B_k}\textstyle\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n
\end{aligned}$$

for $\sigma_{k-1}(n)=\sum_{m|n\ m>0}m^{k-1}$. In particular, the coefficients of q^n are rational, and all have the same denominator B_k. □

Proposition 1.12. *In the Fourier expansion of Δ, $a_0 = 0$ and $a_1 = (2\pi)^{12}$ so that Δ is a nonzero cusp form.*

Proof. Recall $\Delta = (60G_4)^3 - 27(140G_6)^2$.
Now, we know

$$G_4(\tau) = 2\zeta(4) + 2\frac{(2\pi i)^4}{(k-1)!}(\sigma_3(1)q + q^2(...)) = 2\frac{\pi^4}{90} + 2\frac{16\pi^4}{3!}(q + q^2(...))$$

$$(60G_4(\tau))^3 = \left(\frac{2\cdot 60}{90}\right)^3 \pi^{12} + 60^3 \cdot 3\left(\frac{2}{90}\right)^2\left(\frac{32}{3!}\right)\pi^{12}q + q^2(...)$$

Similarily,

$$G_6(\tau) = 2\zeta(6) + 2\frac{(2\pi i)^6}{(6-1)!}(\sigma_5(1)q + q^2(...)) = 2\frac{\pi^6}{945} - \frac{2\cdot 64\pi^6}{5!}(q + q^2(...))$$

$$(140G_6(\tau))^2 = \left(\frac{2\cdot 140}{945}\right)^2 \pi^{12} - 140^2 \cdot 2\left(\frac{2}{945}\right)\left(\frac{128}{5!}\right)\pi^{12}q + q^2(...)$$

Plug these inside of Δ.

$$\Delta = 0 + 4096\pi^12 + q^2(...)$$

So indeed, $a_0 = 0$ and $a_1 = (2\pi)^{12}$. We wish to emphasize the miraculous equalities at play:

$$\left(\frac{2\cdot 60}{90}\right)^3 = 27\left(\frac{280}{945}\right)^2 \qquad 60^3 \cdot 3\left(\frac{2}{90}\right)^2\left(\frac{32}{3!}\right) + 27\left(140^2 \cdot 2\left(\frac{2}{945}\right)\left(\frac{128}{5!}\right)\right) = (2\pi)^{12}$$

□

2 GGT

2.1 Lecture Notes

The following theorem is of great importance, and is named after I. A. Gruško. The proof below is by Stalling.

Theorem 2.1 (Gruško)**.** *Let $\phi : F \to G$ is a surjective homomorphism where F is free and $G = G_1 * G_2$.*
Then, $\exists F_1, F_2 < F : \phi(F_i) = G_i$ and $F = F_1 * F_2$.

Proof. As before, we switch to complexes. Let X_i be complex with $\pi_1(X_i) = G_i$, and let X be the complex obtained by joining X_1 and X_2 by an edge. Place a point x on this edge. Note that $\pi_1(X) = G$ by Van Kampen theorem.

We can find Y compact 2-complex with $\pi_1(Y) = F$ so that $f : Y \to X$ is a continuous map with $f_* = \phi$. Our goal is to show that the fiber of x is a tree in Y.

We can now finish the proof. Let $F_i = f^{-1}(X_i)$, and apply Van Kampen Theorem to $Y/f^{-1}(x) = f^{-1}(X_1) \cup f^{-1}(X_2)$, noting that their intersection is $f^{-1}(x)$, a tree. We get

$$F = \pi_1(Y) = \pi_1(Y/f^{-1}(x)) = \pi_1(f^{-1}(X_1)) * \pi_1(f^{-1}(X_2)) = F_1 * F_2$$

So the F_i are subgroups of F, thus free groups by the previous theorem, and we get the advertized free product equality.
Note also that $f_*(F_i) = \phi(F_i) < G_i$. But since f_* is surjective we must have equality.

To find the objects in our goal, we do the following. In general, $f^{-1}(x)$ is a forest. We decrease the number of components by finding a path $l \in Y^{(1)}$ connecting different trees, and so that $f(l)$

falls to a trivial element of $\pi_1(X_i)$. If we can do that, then attach an edge e to the ends of l and a cell D delimited by $e \cup l$. Since $f(l)$ is trivial, we can extend f so that $f^{-1}(x)$ now contains e.

To find l, start with an edge path L joining trees in $f^{-1}(x)$. By surjectivity of $\phi = f_*$, we can find γ a closed edge-path in Y based at the starting point of L with $[f(\gamma)] = [f(L)]$ in $\pi_1(X)$. Let $l = \gamma^{-1}L$. This is a path with $f^{-1}(l)$ trivial in $\pi_1(X)$. Patrtition $l = l_1 l_2 ... l_n$ where all the endpoints aree in $f^{-1}(x)$, and l_i is mapped alternatingly in X_1 and X_2. Let $g_j = [f(l_j)]$. If $g_j = 1$, but then endpoints of l_j lie on the same tree in $f^{-1}(x)$, we can replace l_j by a path in $f^{-1}(x)$ which we merge with l_{j-1} and l_{j+1}. At this point, $[f(l)] = 1 = g_1 .... g_n$ lying alternatingly in G_1 and G_2. So at least one g_j is trivial, and l_j is the desired path. □

3 The Amalgamated Product

In what follows, we have spaces X_1 and X_2, an open cover for X, with fundamental groups G_1 and G_2, and $X_0 = X_1 \cap X_2$ with fundamental group G_0.

Definition 3.1 (Amalgamated product)**.** The amalgamated product of groups $G_1 *_{G_0} G_2$ is a quotient of the free product. The data are injections $\phi_i : G_0 \hookrightarrow G_i$. Then,

$$G_1 *_{G_0} G_2 = G_1 * G_2 / \ll \phi_1(g)\phi_2(g)^{-1} : \forall g \in G_0 \gg$$

Suppose we only know $\phi_i : G_0 \hookrightarrow G_i$, and want to build X whose fundamental group is the amalgamated product. The next corollary follows directly from Van Kampen's theorem. Recall that every ϕ is induced by some f with appropriate fundamental groups, so let $\phi_i = (f_i)_*$.

Corollary 3.1. *The space $X = X_1 \cup X_0 \times [0,1] \cup X_2/\sim$, with the relation $(x,0) \sim f_1(x)$ and $(x,1) \sim f_2(x)$.*

To understand the structure of the amalgamated product, we want to understand its subgroups. To do so, we look at the covers. A good place to start is with the universal cover. We first look at one side of the dumbell.

Lemma 3.1. *The universal cover of $Y_1 = X_1 \cup X_0 \times [0,1]/\sim$ is $\widetilde{Y_1} = \widetilde{X_1} \cup \bigsqcup \widetilde{X_0} \times [0,1]/\sim$.*

Proof. Let $p : \widetilde{Y_i} \to Y_i$ be the universal cover. First, we show $\widetilde{X_0} \times [0,1]$ are the components of $p^{-1}(X_0 \times [0,1])$. If not, then there is α some loop in X_0 giving a nontrivial element in $\pi_1(X_0)$, and it lifts to a loop $\tilde{\alpha}$ in $\widetilde{X_0} \times [0,1]$. Since ϕ^i is injective (by the data), $\phi^i(\alpha)$ is a non-trivial element of $\pi_1(X_1)$, so it's lift $\tilde{alpha}$ must have disjoint endopoints, contradicting that $\tilde{\alpha}$ was a loop.

Then, $\widetilde{Y_1}$ is a copy of $\widetilde{X_1}$ with copys of $\widetilde{X_0} \times [0,1]$ glued via the lifts $\widetilde{X_0} \to \widetilde{X_i}$ of f^i. □

Proposition 3.1. *The universal cover of $X = X_1 \cup X_0 \times [0,1] \cup X_2/\sim$ is copies of $\widetilde{Y_1}$ and $\widetilde{Y_2}$ glued in a tree like fashion by cylinders $\widetilde{X_0}$.*

3.1 PS

The following have been solved, but I do not write the solutions publicly for obvious reasons.

Problem 3.1. *Let $\mu(G)$ the min cardinality of a generating set of G. Show $\mu(G_1 * G_2) = \mu(G_1) + \mu(G_2)$.*

Problem 3.2. *Let G a f.g. group. Show that for some n, $G = G_1 * ... * G_n$ for G_i indecomposables.*

Problem 3.3. *Kuroš theorem: if $H < G_1 * G_2$, then H is the free product of free groups and conjugates of subgroups of G_i.*

Problem 3.4. *Let $G = G_1 * G_2$. If $[g, h] \in G_1$ is nontrivial, then $g, h \in G_1$.*

Problem 3.5. *Show that each indecomposable subgroup of $G_1 * G_2$ is either $\mathbb{Z}$ or contained in a conjugate of G_i.*

Problem 3.6. *Show that if $G = G_1 * G_2$ and for $w \in G$, $w^{-1}G_1w \cap G_i$ is not empty, then $i = 1$ and $w \in G_1$.*

Problem 3.7. *Let G be finitely generated. If $G = G_1 * ... * G_n = H_1 * ... * H_m$, then $m = n$ and G_i is isomorphic to a conjugate of H_i up to permutation.*