Week 1: 01/01 - 07/01

1 Diamon-Shurman, Chap 1

1.1 Modular forms (1.1, 1.2)

Definition 1.1 (Congruence subgroup)**.**

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} mod N\} = ker(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z}))$$

A subgroup $\Gamma < SL_2(\mathbb{Z})$ is a congruence subgroup of level N if $\Gamma(N) \subset \Gamma$.

Definition 1.2. 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

$$(f[\gamma]_k)(\tau) = (c\tau + d)^{-k} f(\gamma(\tau))$$

Definition 1.3. Let Γ a congruence subgroup. $f : \mathcal{H} \to \mathbb{C}$ is a modular form of weight k w.r.t Γ if

- f is holomorphic
- $f[\gamma]_k = f$ for all $\gamma \in \Gamma$
- $f[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$

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

1.2 Geometry (1.3, 1.4)

Definition 1.4. A complex torus is a quotient of $\mathbb{C}$ by a lattice. Addition in $\mathbb{C}$ descends to the qutient to make the torus an abelian group.

Proposition 1.1 (Equivalence between Complex Torus and Elliptic Curve)**.** *Let $\mathcal{P}(z)$ be the Weirstrass function for some lattice Λ. Then,*

$$(\mathcal{P}'(z))^2 = 4(\mathcal{P}(z))^3 - a\mathcal{P}(z) - b$$

where a, b depend on the lattice. This property show that $(\mathcal{P}(z), \mathcal{P}'(z))$ map points in $\mathbb{C}/\lambda$ to an elliptic curve.
This map works in reverse: one can produce a complex torus from an elliptic curve, whose image under $(\mathcal{P}(z), \mathcal{P}'(z))$ will be that elliptic curve.
The map can be used to equip elliptic curves with an group law, that of the complex torus.

Definition 1.5 (Torsion subgroup of Complex Torus and Weil pairing)**.** Let $[N](z + \Lambda) = Nz + \Lambda$, and $E[N] = \{P \in \mathbb{C}/\Lambda : [N]P = 0\}$. Let also $\mu_N =< e^{2\pi i/N} >$, the cyclic subgroup of C^*.
The Weil pairing e_N takes two elements P, Q of the torsion subgroup to one in μ_N. Notably, if P, Q generate $E[N]$, then $e_N(P, Q)$ is a primitive root of unity.

1.3 Modular curve

Definition 1.6. Let E an elliptic curve and (P, Q) points that generate $E[N]$ such that $e_N(P, Q) = e^{2\pi i/N}$. Then, $(E, (P, Q)) = (E', (P', Q'))$ if there is an isomorphism of elliptic curves taking P to P' and Q to Q'. The moduli space is $S(N) = \{(E, (P, Q)) \quad for \quad \Gamma(N)\}/ =$.
Then, define $Y(\Gamma) = \Gamma\backslash\mathcal{H} = \{\Gamma\tau : \tau \in \mathcal{H}\}$ to be the modular curve for Γ.

Proposition 1.2. *There is a bijection $S(N) \equiv Y(\Gamma(N))$.*

1.4 Geometry of the modular curve

Proposition 1.3. *The surjection $\pi : \mathcal{H} \to Y(\Gamma)$ given by $\pi(\tau) = \Gamma\tau$ is a quotient map. The modular curve thus inherits a topology from that of $\mathcal{H}$. With this topology, $Y(\Gamma)$ is Haussdorf.*

Definition 1.7. For $\tau \in \mathcal{H}$, let $\Gamma_\tau = \{\gamma \in \Gamma : \gamma(\tau) = \tau)\}$, the isotropy subgroup of τ.
τ is elliptic for Γ if Γ_τ is non-trivial (i.e. $\Gamma_\tau\{\pm I\} \supset \{\pm I\}$).

The goal is to make $Y(\Gamma)$ into a Riemanian surface (i.e. a complex 1-manifold). The charts around $\pi(\tau)$ will depend on Γ_τ, as one can see $\pi(U)$ is homeomorphic to U if Γ_τ is trivial.

Proposition 1.4. *There exists a small enough neighborhood of $\tau \in \mathcal{H}$ such that U contains no elliptic points (except maybe τ itself). Then, $\pi(U)$ will work as the neighborhood for the chart at $\pi(\tau)$.*

Example 1.1. *The modular curve for the full modular group $Y(1) = SL_2(\mathbb{C})\backslash\mathcal{H}$ can be identified with the fundamental domain for $SL_2(\mathbb{Z})$, with sides identified. Note that every point $\tau \in \mathcal{D}$ represents an elliptic curve (up to isomorphism), by $\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}$.*
Note that $Y(1)$ on the Riemann sphere is a triangle with the vertex at the north pole removed. We thus compactify $Y(1)$ to obtain $X(1)$. In general:

Definition 1.8 (Modular Curve, compactified)**.** Let Γ a congruence subgroup. Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Now, $X(\Gamma) = \Gamma\backslash\mathcal{H}^*$
Note that $X(\Gamma) = Y(\Gamma) \bigcup \Gamma\backslash(\mathbb{Q} \cup \{\infty\})$. The points in the second term are called cusps of the modular curve.

1.5 Hecke Operators

The first goal is to transform modular forms for Γ_1 into modular forms for Γ_2. This is done by the weight-k $\Gamma_1\alpha\Gamma_2$ operator.

Definition 1.9. Let $\alpha \in GL_2^+(\mathbb{Q})$. The weight-k $\Gamma_1\alpha\Gamma_2$ operator $[\Gamma_1\alpha\Gamma_2]_k : \mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$ is defined by

$$f[\Gamma_1\alpha\Gamma_2]_k = \sum f[\beta_j]_k$$

where $\{\beta_j\}$ is a transversal of the orbit equivalence $\Gamma_1 \curvearrowright \Gamma_1\alpha\Gamma_2$

Many things are required to make this operator work as advertized. For the sum to make sense, we need the action to have finitely many orbits. Then, we need to show that for $f \in \mathcal{M}_k(\Gamma_1)$, we indeed have $f[\Gamma_1\alpha\Gamma_2]_k \in \mathcal{M}_k(\Gamma_2)$. We only show invariance.

Proof. Let $\gamma \in \Gamma_2$. Recall that $[\beta]_k[\gamma]_k = [\beta\gamma]_k$. Note that right-multiplication by γ_2 sends an orbit $\Gamma_1\beta_j$ of the action to another orbit: $(\Gamma_1\beta_j)\gamma = \Gamma_1(\beta_j\gamma)$. Hence, if $\{\beta_j\gamma\}$ is another transversal of $\Gamma_1 \curvearrowright \Gamma_1\alpha\Gamma_2$, so the sums are the same. □

This machinery is made useful when Γ_1 and Γ_2 are related. First, note that if Γ is a congruence subgroup, then for all $\alpha \in GL_2^+(\mathbb{Q})$, $\alpha^{-1}\Gamma\alpha$ is too.

2 Geometric Group Theory

2.1 Refreshers from topology

Perhaps surprisingly, we will study groups using results from geometry. In particular, we will look at groups by realizing them as fundamental groups. The following results will be used together repeatedly.

Lemma 2.1. *Topological spaces that are homotopic have the same fundamental group.*

Lemma 2.2. *Let X a CW-complex, and let A be a contractible subcomplex. Then, X/A is homotopic to X. In particular, $\pi_1(X) \cong \pi_1(X/A)$.*

Free groups are easily realized as topological spaces.

Lemma 2.3. *The n-bouquet B_n ($n \leq \infty$), the graph with 1 vertex and n edges, has $\pi_1(B_n) = F_n$.*

Proof. Recall $\pi_1(S^1) = \mathbb{Z}$. The n-bouquet is the wedge product of S^1 with itself n times. That is, gluing of circles along a single point. Since we work only up to homotopy, the choice of point does not matter.
The Van Kampen theorem then yields that $\pi_1(S^1 \# S^1) = \mathbb{Z} * \mathbb{Z}$, and so on. □

Proposition 2.1. *If Y is a covering space of X, then $\pi_1(Y) < \pi_1(X)$.*

2.2 Prologue

Definition 2.1 (Free Product)**.** The free product $A * B = (S, \cdot)$ of groups is the following set and product:

- S is the set of all reduced words $a_1b_1a_2b_2...a_nb_n$, where $a_i \in A$ and $b_i \in B$ are all non-identity elements except maybe a_1 and b_n,
- $w \cdot w'$ is the concatenation of words, followed by reduction (perform the possible operations inside of A or B that might happen where the words meet).

Note that A and B both live as subgroups of their free product.

Definition 2.2 (Free Group)**.** The free group F_n is a free product of $\mathbb{Z}$ with itself n-times, where $n \leq \infty$.

Proposition 2.2. *Every subgroup of F_n is itself free.*

Proof. We have $\pi_1(B_n) = F_n$. So, subgroups of F_n can be determined by looking at covering spaces of B_n.
Every covering space of B_n is a graph Γ. Let S a spanning tree of Γ. Since S is contractible, we have $\pi_1(\Gamma) = \pi_1(\Gamma/S)$. The proof is done since Γ/S has a single vertex, and thus is a bouquet. □

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.
NEXT TIME (on wednesday)...
At this point, we have Y is a compact 2-complex with $\pi_1(Y) = F$ so that $f : Y \to X$ is a continuous map with $f_* = \phi$. Moreover, 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, and □

2.3 PS1

Problem 2.1. *Let $\mu(G)$ the min cardinality of a generating set of G. Show $\mu(G*H) = \mu(G)+\mu(H)$.*

Solution 2.1. *The case where either side is ∞ is the statement that a free product is not finitely generated iff one of the term is not, which is trivial.*
Let $X = \{g_i\}$, $Y = \{h_i\}$ be generating sets of minimal size. Then, $X \cup Y$ is a generating set for $G * H$ by definition. $|X \cup Y| = |X| + |Y|$ so we proved $\leq$.
Let $T = \{t_i\}$ be any generating set for $G * H$.

Problem 2.2. *Let G a f.g. group. Show that for some n, $G = G_1 * ... * G_n$ for G_i indecomposables.*

Solution 2.2. *Suppose G is indecomposable. Then we are done. Suppose not, so $G = A*B$. Repeat the argument on A and B, and so on. The algorithm is bound to terminate since, by problem 1, the rank of the groups strictly decrease as we go down the tree.*

3 The Arithmetic of Elliptic Curves, J-H Silverman

3.1 Rudiments of Algebraic Geometry

Write K a perfect field (i.e. all extensions are separable), and $\bar{K}$ an algebraic extension.

Definition 3.1. The Affine space over K is $\mathbb{A}^n = \bar{K}^n$. The set of K-rational points is the subspace $\mathbb{A}^n(K) = K^n$.

Remark 3.1. The Galois group $Gal(\bar{K}/K)$ acts on $\mathbb{A}^n$, by $\sigma(P) = (\sigma(p_1), ..., \sigma(p_n))$. Note that $\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : \sigma(P) = P\}$.

Definition 3.2. Let I a subring of $\bar{K}[X]$. Then $V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}$ is an algebraic set.
Oppositly, $I(V) = \{f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in V\}$. If $I(V)$ can be generated by polynomials in $K[X]$, say V is defined over K.

Definition 3.3. An algebraic set V is an affine variety if $I(V)$ is a prime ideal of $\bar{K}[X]$.

4 *Galois Cohomology*, J.P. Serre

This book is slightly too advanced for me right now (or rather, it is slightly off the path of what I must study now so I don't want to dedicate enough time to it). The content, however, seems highly intresting. I will simply state the theorems that surprised me most.
Let G a pro-p-group. Let $n(G)$ and $r(G)$ be the minimum number of generators and relators in any presentation of G. These numbers can be computed using cohomology.

$$n(G) = dimH^1(G, \mathbb{Z}/p\mathbb{Z}) \quad r(G) = dimH^2(G, \mathbb{Z}/p\mathbb{Z})$$

The following inequality is due to Golod and Shafarevic: $r(G) > n(G)^2/4$.

5 Philo of Math, *What numbers could not be*, Paul Benacerraf

This paper thinks about the question of numbers. What are they?
Of course, the intrest lies not so much in the answers as in the questions. I feel however that this time, the answer is intresting: numbers are nothing.
author first explains what previous thoughts in the litterature were. Numbers had been defined as sets, and stuff like "$3 = \{\{\{\emptyset\}\}\}$" were written. The author argues that "$3 = \{\emptyset, \{\emptyset, \{\emptyset\}\}\}$" serves just as well for a definition of the object "3". This is a problem, for these two definitions don't give the same properties. For example, the question "is 3 a subset of 17" has different answers.
The solution the author proposes is to not define numbers as anything at all. Numbers should not be thought of as "objects in a progression", but simply as "a progression". Numebrs are nothing in particular, they are virtual objects and any precise instantiation can work just as well for them ("ex: sets, julius Caesar").

I found this intresting. From what I take, this view doesn't differ from the following: "numbers are elements of a free abelian group of rank 1". Similarily, this doesn't "fix" numbers to be precise objects; one could take $\mathbb{Z}$ but also any isomorphic group.
What I find intresting is that followign the author views, nothing seems to disricminate the natural numbers against all integers. If number are but a progression, why force this progression to go in a single direction? And if so, we could define numbers as a "pointed progression", a progression with a pointed "0". This, however, serves only for algebraic purposes (to make numbers a group), and is perhaps not strictly needed to give a formal idea of what "numbers" should (not) be.

5.1 Intresting (and funny) quotes

Arithmetic is therefore the science that elaborates the abstract structure that all progressions have in common merely in virtue of being pregressions. It is not a science concerned with particular objects - the numbers. The seach for which independently identifiable particular objects the numbers really are is a misguided one.

Number theory is the elaboration of the properties of all structures of the order type of the numbers.

In awaiting enlightenment on the true identity of 3 we are not awaiting a proof of some deep theorem.