RECAP

Last week we defined an action of $SL_2(\mathbb{Z})$ on

$$\mathcal{H} := \{ z \in \mathbb{C} \mid \mathrm{Re}\, z > 0 \}$$

given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \circ \tau = \dfrac{a\tau + b}{c\tau + d}$. We considered the groups

$$\begin{aligned}
\Gamma(N) &= \ker\left(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z}) \right) \\
&\cap\!| \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\} \\
&\cap\!| \\
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}
\end{aligned}$$

We obtained (affine) Riemann surfaces $Y_\Gamma := \mathcal{H}/\Gamma$; for $\Gamma = \Gamma(N), \Gamma_1(N), \Gamma_0(N)$, these are denoted by

$$Y(N), \quad Y_1(N), \quad Y_0(N).$$

The corresponding compact surfaces are denoted by $X(N), X_1(N), X_0(N)$.
We computed the function fields of these: letting

$$f^v(\tau) = \wp_\tau\left(\frac{c + d\tau}{N} \right) \quad \text{for } v = (c, d) \in (\mathbb{Z}/N\mathbb{Z})^2,$$

equal for $\pm v$

we obtained

$$\begin{array}{llcl}
& X(N) & & \mathbb{C}(j, f^v) \\
& \quad | & & \quad | \\
& X_1(N) & & \mathbb{C}(j, f^{(0,i)} \mid i = 1, \dots, N-1) \\
PGL_2(\mathbb{Z}/N\mathbb{Z}) & \quad | & (\mathbb{Z}/N\mathbb{Z})^* & \quad | \\
& X_0(N) & & \mathbb{C}(j, j_N) \supseteq \mathbb{C}(j, \text{symm. functions in } f^{(i,0)}) \\
& \quad | & & \quad | \\
& X(1) & & \mathbb{C}(j)
\end{array}$$

TODAY

① Y_Γ as moduli spaces over $\mathbb{C}$
② Y_Γ " " " " $\mathbb{Q}$: statements
③ Construction of Heegner points
④ Y_Γ over $\mathbb{Q}$: proofs (maybe)

§1. Y_Γ as mod. spaces over $\mathbb{C}$

<u>Thm</u> $\mathcal{H} \xrightarrow{\Phi} \{(E,C)\}/\sim$ $\quad C \subseteq E, \quad C \simeq \mathbb{Z}/N\mathbb{Z}$

$\tau \longmapsto (\underbrace{\mathbb{C}/\mathbb{Z}\oplus\mathbb{Z}\tau}_{E_\tau}, \langle \tfrac{1}{N} \rangle)$ $\quad (E,C) \sim (E',C')$

$\Leftrightarrow \exists\, \varphi : E \xrightarrow{\sim} E'$ t.c. $\varphi(C) = C'$

è surgettiva, e induce

$$\mathcal{H}/\Gamma_0(N) \xrightarrow{\sim} \{(E,C)\}/\sim$$

<u>Proof</u> ~~Every (E,C) is $(E_\tau, <$~~

First, the fibres. $\Phi(\tau) = \Phi(\tau') \Rightarrow \exists\, \gamma \in \mathbb{C}^\times$ s.t.

$$\gamma \Lambda_\tau = \Lambda_{\tau'} \quad \& \quad \gamma \cdot \frac{1}{N} = \frac{k}{N} \pmod{\Lambda_{\tau'}} \quad \circledast$$
for some $(k,N) = 1$

$\gamma \cdot 1 = c\tau' + d$ $\qquad \tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau'$
$\gamma \cdot \tau = a\tau' + b$

$\circledast \Leftrightarrow$ $c\tau' + d \equiv k \pmod{N\Lambda_{\tau'}}$

$\Leftrightarrow c \equiv 0\,(N)$, i.e. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

Surjectivity: (E,C) is $(E_{\tau'}, \langle \frac{x+y\tau'}{N} \rangle)$.

Choose $\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \cdot \tau'$. Then $\gamma := c\tau + d$ carries

$\gamma \cdot \Lambda_{\tau'} = \Lambda_\tau$ and $\frac{x+y\tau'}{N}$ to $(c\tau + d) \cdot \frac{x+y\tau'}{N} \equiv \frac{1}{N} (\Lambda_\tau)$

$$(c\tau + d)x + y(a\tau + b) \equiv 1 \quad (N\Lambda_\tau)$$

$$\Leftrightarrow \begin{cases} cx + ay \equiv 0 & (N) \\ dx + by \equiv 1 & (N) \end{cases} \qquad \exists \begin{pmatrix} +x & b \\ -y & d \end{pmatrix} \in SL_2(\mathbb{Z}/N\mathbb{Z})$$

Bézout + lift. $SL_2(\mathbb{Z}/N\mathbb{Z}) \twoheadleftarrow SL_2(\mathbb{Z})$ $\square$

Rmk $Y_1(N) \xleftrightarrow{1:1} \{(E, P)\}/\sim$, $P \in E[N]$ ex. order N

§2. Moduli spaces over $\mathbb{Q}$

Thm Let $Y_0(N)_{\mathbb{Q}}$ be the unique curve obtained as follows: let $X_0(N)_{\mathbb{Q}}$ be the unique smooth proj. curve $/\mathbb{Q}$ with function field $\mathbb{Q}(j(z), j(Nz))$. ~~Then~~ Let $Y_0(N)_{\mathbb{Q}} = X_0(N)_{\mathbb{Q}} \cap Y_0(N)_{\mathbb{C}}$. For every field K with $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, there is a bijection

$$Y_0(N)_{\mathbb{Q}}(K) \longleftrightarrow \{(E/K, C)\}/\sim,$$

where:

- E/K is an ell. curve def. over K;
- $C \subseteq E(\bar{K})[N]$ is a cyclic subgroup of order N
- C is stable under $\mathrm{Gal}(\bar{K}/K)$ as a set;
- $(E_1, C_1) \sim (E_2, C_2)$ if $\exists\, \varphi : (E_1)_{\mathbb{C}} \to (E_2)_{\mathbb{C}}$ that carries C_1 to C_2.

Rmk These conditions imply $j(E) \in K$, $j(E/C) \in K$. But they are stronger: consider $E = E/C = y^2 = x^3 + x$ and $C = \ker[2-i]$. Then $j(E), j(E/C) \in \mathbb{Q}$, but C is NOT Galois-stable. Thus, $E \to E/C$ does NOT give a point of $Y_0(5)(\mathbb{Q})$.

§3. Construction of Heegner points

~~Setup~~ **Def** (Modularity) Let $E/\mathbb{Q}$ be an elliptic curve. We say that E is MODULAR if $\exists N > 0$ and a non-constant algebraic morphism, defined over $\mathbb{Q}$, from $X_0(N)$ to E. This is called a MODULAR PARAMETRISATION; it can be chosen so that $\varphi(\infty) = O_E$

Thm (Wiles; Breuil - Conrad - Diamond - Taylor)
Every $E/\mathbb{Q}$ is modular; the optimal N coincides with the conductor of E.

Setup $E/\mathbb{Q}$ an ell. curve, $E_{\overline{\mathbb{Q}}}$ without CM,
$N =$ conductor E, $\varphi : X_0(N) \to E$ a modular parametrisation, $K = \mathbb{Q}(\sqrt{-D})$ a quadratic field satisfying the $D \neq 3, 4$

Heegner condition: every prime ℓ dividing N is split in K, hence $N = \mathcal{N} \cdot \overline{\mathcal{N}}$ for some $\mathcal{N} \lhd \mathcal{O}_K$ with $\mathcal{O}_K / \mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$.

Def. (Heegner points) Fix a positive integer n, prime to N let $\mathcal{O}_n := \mathbb{Z} + n\mathcal{O}_K$ be the order of conductor n, and let $\mathcal{N}_n := \mathcal{N} \cap \mathcal{O}_n$. Then $(\mathcal{N}_n, n) = 1$, hence $\mathcal{N}_n$ is an invertible ideal of $\mathcal{O}_n$. ↳ Lorenzo S.'s lecture

Consider $\mathcal{O}_n / \mathcal{N}_n = \mathcal{O}_n / \mathcal{N} \cap \mathcal{O}_n \simeq \dfrac{\mathcal{O}_n + \mathcal{N}}{\mathcal{N}} \simeq \mathcal{O}/_{\mathcal{N}} \simeq \mathbb{Z}/N\mathbb{Z}$.

Let $E = \mathbb{C}/\mathcal{O}_n$, ~~and~~ $G_n = \mathcal{N}_n^{-1}/\mathcal{O}_n \simeq \mathbb{Z}/_{N}\mathbb{Z} \subset E$, and $E/G_n \simeq \mathbb{C}/_{\mathcal{N}_n^{-1}} =: E'$. Note that E, G_n and E' are <u>all</u> defined over K_n: this is because $G_n = E[\mathcal{N}_n]$, and the action of $\mathcal{N}_n$ on E is def'd over K_n.

Hence $(E, G_n) = x_n \in X_0(N)(K_n)$.

We may then set $y_n := \varphi(x_n)$ and

$$y_{n,K} := \mathrm{Tr}_{K_n/K}(\varphi(x_n))$$

These are the famous Heegner points!

§4. Moduli spaces over $\mathbb{Q}$: proofs

~~Thm~~ Proof of a weak version

$$\mathbb{Q}(X_0(N)) = \mathbb{Q}(j(z), j(Nz))$$

On an open subscheme, $U = \{F_N(x,y) = 0\}$, where $F_N(x,y) = 0$ is the minpoly of j_N over j.

$\rightsquigarrow$ on an open, $\cancel{K}$-pts of $X_0(N)$ are pairs $(j(E), j(E')) \in K^2$ s.t. $\exists \tau \in H$ with

$$j(E') = j(N\tau), \quad j(E) = j(\tau).$$

But $E \simeq \mathbb{C}/\mathbb{Z} \oplus \tau\mathbb{Z} \twoheadrightarrow \dfrac{\mathbb{C}}{\frac{1}{N}\mathbb{Z} \oplus \mathbb{Z}\cdot\tau} \simeq \dfrac{\mathbb{C}}{\mathbb{Z} \oplus \mathbb{Z}\cdot N\tau} = E'$.

Now suppose $\varphi: E \to E'$ not def'd over K. Then $\exists\ {}^\sigma\varphi: {}^\sigma E = E \to {}^\sigma E' = E'$. However, ${}^\sigma\varphi \circ \varphi^\vee : E' \to E$ has deg N^2 but is not $[N]$, otherwise ${}^\sigma\varphi \circ \varphi^\vee = [N] = \varphi \circ \varphi^\vee \Rightarrow {}^\sigma\varphi = \varphi$.

Hence E' has CM. □

In fact, one also needs to consider the case that \sigma \phi * \phi dual = [-N]. In that case, one shows that ker \phi is still Galois-stable, hence that \phi is (up to isomorphism on the target) defined over K

Problem: j, j_N do NOT separate all pts.

This is akin to $\mathrm{Frac}\left(\dfrac{\mathbb{Q}[x,y]}{y^2 - x^2(x-1)}\right)$: $x = y = 0$ is not a pt!

Need a set of functions that embed $Y_0(N) \hookrightarrow \mathbb{A}^{??}$.

For simplicity: assume N is odd.

Thm (Vélu) $E: y^2 = x^3 + Ax + B$, $G < E(\bar{K})$, $\# G$ odd.

For $(x_Q, y_Q) \in G$ define

$$t_Q := 3x_Q^2 + A, \quad u_Q := 2y_Q^2, \quad w_Q := u_Q + t_Q x_Q,$$

$$t := \sum_{Q \neq 0} t_Q, \quad w = \sum_{Q \neq 0} w_Q, \quad r(x) = x + \sum_{Q \neq 0} \left(\frac{t_Q}{x - x_Q} + \frac{u_Q}{(x - x_Q)^2} \right)$$

Then, letting $E': y^2 = x^3 + (A - 5t)x + (B - 7w)$,

the map $E \longrightarrow E/G \xrightarrow{\sim} E'$ can be taken to be

$$\alpha(x, y) = (r(x), r'(x) \cdot y).$$

[Maybe I don't even need this!]

Rmk $\mathbb{Q}(X_0(N)) \ni$ symm. fcts in $f^{(0,i)}(\tau)$, call them $e_j(\tau)$. From $\{e_j(\tau)\}$ we can reconstruct the set of x-coords $\{f^{(0,i)}(\tau)\}$, hence C. So

$$\tau \mapsto (j(\tau), e_1(\tau), \ldots, e_N(\tau))$$

is injective. Thus, $Y_1(N)_{\mathbb{Q}}$ has coords $j, e_1, \ldots, e_N$:

a pt is K-rational iff $j, e_1, \ldots, e_N$ are, iff the ~~coords~~ ~~of~~ set $\{f^{(0,i)}(\tau)\}$ is def'd over K.

§5. Bonus Track: constructing $X(3)$ over $\mathbb{Q}$.

Let E be an ell. curve over a field K of char 0. (or just $\neq 3$)
Suppose P is a pt of order 3. By def'n, this means that $\exists$ a function f on E s.t. $\operatorname{div} f = 3(P) - 3(\infty)$.
Now, functions with a triple pole at ∞ lie in $\langle 1, x, y \rangle$, and in order to have an actual pole of order 3, one needs $f = ay + bx + c$ with $a \neq 0$. Replacing y with f, we may as well assume that $y = f$, that is, $\operatorname{div} y = 3(P) - 3(\infty)$.
Write

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Translating $x \to x - x(P)$, we can assume $a_6 = 0$.
Now P is the only pt with $y = 0$, so $x^3 + a_2 x^2 + a_4 x = x^3$, that is, $a_2 = a_4 = 0$. ~~Rescaling~~ $\cancel{x \mapsto u^2 x,\ y \mapsto u^3 y}$ we ~~get~~

$$\cancel{u^6 y^2 + a_1 u^5 xy + a_3 u^3 y = u^6 x^3}$$

Moreover: fcts with a double pole at ∞ are of the form $\alpha x + \beta$, $\alpha \neq 0$; if we want such a funct to vanish at P, $\beta = 0$. Similarly, y is uniquely def'd up to scalars.
Now suppose Q is a 2^{nd} pt of order 3, $(Q \neq \pm P)$

$$3(Q) - 3(\infty) = \operatorname{div}(y - Ax - B).$$

If $A = 0$, then $y(Q) = B$ and $B^2 + a_1 Bx + a_3 B = x^3$ has a triple root: $x^3 - a_1 Bx - (B^2 + a_3 B) = (x - x(Q))^3$.
But then $x(Q) = 0$ (look at coeff. of x^2), so $y^2(Q) + a_3 y(Q) = 0$. the pts $(0,0)$ and $(0, -a_3)$ are $\pm P$, contradiction.
So $A \neq 0$; replacing $y \to y/A^3$ and $x \to x/A^2$ we can assume $A = 1$. Finally, $y - x - B$ vanishes only at Q, so

$$x^3 - \left[(x+B)^2 + a_1 x(x+B) + a_3(x+B)\right] = (x - C)^3$$

Compare coeffs to get

$$\begin{cases} 3C = a_1 + 1 & (1) \\ -3C^2 = 2B + a_1 B + a_3 & (2) \\ C^3 = B^2 + a_3 B & (3) \end{cases}$$

$$(3) - B(2): \quad C^3 + 3C^2B = B^2 - 2B^2 - a_1 B^2$$
$$= B^2(-1 - a_1) = -3CB^2$$

$$\Leftrightarrow \quad (C+B)^3 = B^3.$$

So $Y(3)$: $\quad (B+C)^3 = B^3$

$$\uparrow$$

$$y^2 + (3C-1)xy + (-3C^2 - B - 3BC)y = x^3$$

Rmk The function field contains $\left(\frac{B+C}{B}\right)$, a primitive 3^{rd} root of 1. Over $\mathbb{Q}(\zeta_3)$, $Y(3)$ decomposes; one component is $B + C = \zeta_3 B$, which gives a $\mathbb{P}^1$ w/ a universal elliptic curve