Last week: we defined $Y_1(N)$ over $\mathbb{Z}[\frac{1}{N}]$ and showed it was smooth, + compatible with existing defⁿ $/\mathbb{C}$.

Recall: we characterized $Y_0(N)/\mathbb{Q}$ using q-expansions.

<u>Prop 3.5.4</u> (Siegel, Kato 2004)

Let E/S ell. curve, $c > 1$ integer not div^{ble} by 2 or 3.

Then $\exists !$ elt ${}_c\Theta_E \in \mathcal{O}(E \setminus E[c])^\times$ with the following properties:

(i) $\mathrm{div}({}_c\Theta_E) = c^2 \cdot (0) - E[c]$

(ii) $N_a({}_c\Theta_E) = {}_c\Theta_E$ for a coprime to c,

where N_a is the norm map $\mathcal{O}(E - E[ac])^\times \to \mathcal{O}(E - E[c])^\times$ attached to the a-multⁿ on E.

Moreover, if $E = \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$, $S = \mathbb{C}$, we have

$$ {}_c\Theta_E = q^{\frac{c^2-1}{12}} (-t)^{-c(c-1)/2} \, \gamma_q(t)^{c^2} \, \gamma_q(t^c)^{-1} $$

where $t = e^{2\pi i z}$ $\left(z \in \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau\right)$ and $q = e^{2\pi i \tau}$,

$$ \gamma_q(t) = \prod_{n \geq 0} (1 - q^n t) \prod_{n \geq 1} (1 - q^n t^{-1}) $$

<u>Proof</u> First, note that this unit is unique if it exists.

Assume some f satisfying (i), (ii) exists.

Any other g satisfying (i), (ii) is $g = uf$ some $u \in \mathcal{O}(S)^\times$.

$$ N_3(g) = g \Rightarrow N_3(uf) = uf $$
$$ \Rightarrow u^{3^2} f = uf $$
$$ u^8 = 1. $$

Similarly $N_2(g) = g \Rightarrow u^3 = 1$

$$ \Rightarrow u = (u^3)^2 (u^8)^{-1} = 1 $$

Hence we get uniqueness.

$\Rightarrow$ can prove existence locally on S.

Suffices to show that $c^2(0) - E[c]$ is <u>locally on S</u> a principal divisor.

$\exists$ a theory of "relative Cartier divisors" and a map

$$ \frac{(\text{deg } 0 \text{ divisors on } E)}{(\text{pullbacks of ones on } S)} \longrightarrow E(S). $$

Since $c^2(0) - E[c] = 0$ in $E(S)$

hence $c^2(0) - E[c]$ is the pullback of a divisor on S, hence locally-on-S principal.

Let f be st $\operatorname{div}(f) = c^2(0) - E[c]$.

Since $\operatorname{div}(f)$ is inv^t under N_a, we must have $N_a(f) = u_a f$ some $u_a \in \mathcal{O}(S)^\times$

Since $N_a N_b = N_b N_a$,

$$u_a^{(b^2-1)} = u_b^{(a^2-1)} \quad \forall a, b \text{ coprime to } c.$$

So if we put $g = u_2^{-3} u_3 f$, we have

$$\begin{aligned} N_a(g) &= u_2^{-3a^2} u_3^{a^2} u_a f \\ &= u_2^{-3(a^2-1)} u_3^{(a^2-1)} u_a g \\ &= u_a^{-3(2^2-1)} u_a^{3^2-1} u_a g \\ &= u_a^0 g = g. \end{aligned}$$

So ${}_c\Theta_E$ exists locally + by uniqueness it exists globally.

For case $S = \mathbb{C}$, $E = E_\tau$ we just check that the given function has properties (i), (ii). (cf. 3rd problem sheet.)

Def^n 3.5.5

For $N \geq 4$ and $c > 1$ with $(c, 6N) = 1$, the Siegel unit ${}_c g_N$ is the pullback of ${}_c\Theta_{\mathcal{E}}$ along the order N section $Y_1(N) \to \mathcal{E}$, where $\mathcal{E}/Y_1(N)$ is universal ell. curve.

<u>Remark</u> These units are the building blocks of <u>Euler systems</u> — cf. Kato's paper (Asterisque 295, 2004) + my 2013 paper with Lei & Zerbes.

Important corollary: $Y_1(N)$ is <u>not</u> characterized over $\mathbb{Q}$ by having q-expansions of elts of $\mathbb{Q}(Y_1 N)$ in $\mathbb{Q}((q))$.

Calculate q-exp^n of ${}_c g_5 \in \mathbb{Q}(Y_1(5))^\times$.

The order N section is $z = \frac{1}{5} \bmod \mathbb{Z} + \mathbb{Z}\tau$,

so $t = e^{2\pi i z} = e^{2\pi i/5} \notin \mathbb{Q}$

$${}_c g_5 = q^{(c^2-1)/12} \left(-e^{2\pi i/5}\right)^{-c(c-1)/2} \prod (\cdots)$$

has ζ_5's everywhere.

(One can show: $f \in \mathbb{Q}(Y_1(N))$ $\Leftrightarrow$ $f \in \mathbb{C}(Y_1(N))$ and its q-exp^n lands in $\mathbb{Q}(\zeta_N)((q))$ and satisfies

$$a_n(f)^\sigma = a_n(\langle \sigma \rangle f)$$

for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ $\cong (\mathbb{Z}/N)^\times$.

---

§ 3.6 Quotients and $Y_0(N)$

<u>Prop 3.6.1</u> Let X be a quasiprojective S-scheme (for some base scheme S) + G a finite group acting on X by S-automorphisms.

Then $\exists!$ a S-scheme X/G and a morphism $X \to X/G$ representing the functor

$$Y \longmapsto (\text{homs of } S\text{-schemes } X \to Y \text{ commuting with } G\text{-action}).$$

<u>Proof</u> Uniqueness is obvious (representing a functor). Existence: for $X = \mathrm{Spec}(A)$ affine, $\mathrm{Spec}(A^G)$ works; + can show these patch nicely. (need quasiproj. + finiteness of G here.)

<u>Def 3.6.2</u> For $N \geq 4$ let

$$Y_0(N) = Y_1(N) / (\mathbb{Z}/N)^\times. \quad (\text{as a } \mathbb{Z}[\tfrac{1}{N}]\text{-scheme}).$$

The $\mathbb{C}$-pts of this are $\Gamma_0(N) \backslash \mathcal{H}$.

<u>Construction</u>

Let S be a $\mathbb{Z}[\frac{1}{N}]$-scheme.

There is a map

$$\left\{ \begin{array}{l} \text{iso. classes of pairs } (E, C), \\ E/S \text{ ell. curve}, \\ C \subset E \text{ subgroup-scheme} \\ \text{étale locally isomorphic to } \mathbb{Z}/N \end{array} \right\} \longrightarrow Y_0(N)(S)$$

defined as follows: let $(E,C) \in$ LHS; then $\exists$ $S' \to S$ étale and $P \in E(S')$ st $C = \langle P \rangle$, and this gives a pt of $Y_1(N)(S')$. Changing P changes this by an elt of $G = (\mathbb{Z}/N)^\times$. So get a G-orbit of elts of $Y_1(N)(S')$.
By a scary lemma ("étale descent of morphisms") this gives an S-pt of $Y_0(N)$.

Thus we have a well-def. map

$$\iota_S : \{(E,C)/S\} \longrightarrow Y_0(N)(S).$$

In general this is neither injective nor surjective, but if S is $\mathrm{Spec}(\bar{k})$ for $\bar{k}$ alg. closed it's a bijection.

Injectivity: if L/K is a finite field ext^n, $Y_0(N)(K) \to Y_0(N)(L)$ is obviously injective, but $\left((E,C)/_K\right) \to \left((E,C)/_L\right)$ is not injective ($\exists$ obstructions coming from quadratic twists, etc).

For k field, can check that image(ι_k) is the set of pairs (E,C) def $/k$ modulo isomorphism $/\bar{k}$.

Surjectivity: can show that for k field, ι_k is surjective (fairly hard, cf. Prop VI.3.2 of Deligne-Rapoport) but for non-field S surjectivity can also fail.

For instance, $S = Y_0(N)$ itself: in general there is no (E,C) corresp. to identity map.

(Can try to use $E/(\mathbb{Z}/N)^\times$ but fibres over pts of $Y_0(N)$ with nontriv. stabilizers might not be ell. curves!)

Fact: $Y_0(N)$ is smooth $/\mathbb{Z}[\frac{1}{N}]$, + agrees with our earlier construction $/\mathbb{Q}$.

(Sketch of last point: suffices to show $j(z)$ and $j(Nz)$ lie in $\mathbb{Q}(Y_1(N))^G$ — just take $j(E)$ and $j(E/\langle P\rangle)$.)

---

§3.7 General modular curves.

(following Katz-Mazur)

Def 3.7.1 Let R be a ring

(i) Let $\underline{Ell/R}$ be the following category:

- objects are diagrams $\begin{array}{c} E \\ \downarrow \\ S \end{array}$ where S is some R-sch. & E is an ell. curve $/S$.
- morphisms are squares

$$\begin{array}{ccc} E & \longrightarrow & E' \\ \downarrow & & \downarrow \\ S & \longrightarrow & T \end{array}$$

where $E \cong E' \times_T S$.

(ii) A "moduli problem for ell. curves $/R$" is a contravariant functor $P: \underline{Ell/R} \to \underline{Set}$.

(iii) We say P is · representable if it's representable

· relatively representable if, for every $E/S \in \mathrm{Obj}(\underline{Ell/R})$, the functor $\underline{Sch/S} \longrightarrow \underline{Sets}$

$$T \longmapsto \mathcal{P}(E \times_S T / T)$$

is representable.

(Aside: The category $\underline{\mathrm{Ell}/R}$ is "$\underline{\mathrm{Sch}/Y}$ for a Y that doesn't exist".
If functor $S \mapsto \{\text{ell. curves}/S\}$ were representable, by some $(Y, E/Y)$, then objects of $\underline{\mathrm{Ell}/R}$ would be (just) maps $S \to Y$.
This is the idea of <u>stacks</u>.)

<u>Prop 3.7.2</u> For $\mathcal{P}$ a moduli problem let $\tilde{\mathcal{P}} : \underline{\mathrm{Sch}/R} \to \underline{\mathrm{Sets}}$

$$S \longmapsto (\text{pairs } (E, \alpha),\ E/S \text{ ell. curve},\ \alpha \in \mathcal{P}(E/S))$$

If $\mathcal{P}$ is representable on $\underline{\mathrm{Ell}/R}$, then $\tilde{\mathcal{P}}$ " on $\underline{\mathrm{Sch}/R}$.

(Converse is not quite true).

<u>Proof</u> If $(E/S, \alpha)$ represents $\mathcal{P}$, can check $(S, (E, \alpha))$ represents $\tilde{\mathcal{P}}$. $\square$

<u>Def$^{\wedge}$ 3.7.3</u> $\mathcal{P}$ is <u>rigid</u> if for all $E/S \in \mathrm{Obj}(\underline{\mathrm{Ell}/R})$, $\mathrm{Aut}(E/S)$ acts on $\mathcal{P}(E/S)$ without fixed points.

(Exercise:
i) A representable functor is rigid;
ii) if $\mathcal{P}$ is rigid and $\tilde{\mathcal{P}}$ is rep^{ble}, $\mathcal{P}$ is rep^{ble}.
)

<u>Theorem 3.7.4</u> (Katz–Mazur):
$\mathcal{P}$ is representable if + only if it is relatively rep^{ble} and rigid.