Modular Curves (TCC) Problem Sheet 3 – Solutions

David Loeffler

1st April 2014

This is the last of 3 problem sheets, which will be distributed after lectures 3, 6, and 8 of the course. This problem sheet will be marked out of a total of 25; the number of marks available for each question is indicated.

Work should be submitted, on paper or by email, on or before Tuesday 1st April.

Throughout this sheet, all rings are assumed to be commutative and unital.

---

1. [3 points] Let C be the scheme $\operatorname{Spec} k[X,Y]/\{XY=0\}$, where k is a field. Give an example to show that the structure map $C \to \operatorname{Spec} k$ does not satisfy the functorial criterion of smoothness.

Solution: *[Composite of solutions by Diletta Martinelli, Andrea Petracci, and Lars Sektnan]*

It suffices to find a k-algebra A, a nilpotent ideal I, and a homomorphism $k[X,Y]/(XY) \to A/I$ that does not lift to A. Such a homomorphism is given by a pair of elements $x, y \in A$ such that $xy \in I$ but $(x+i_1)(y+i_2) \neq 0$ for all $i_1, i_2 \in I$.

We let $A = k[t]/t^3$ and $I = (t^2)$, so that $A/I = k[t]/t^2$, and consider the pair $(x,y) = (t,t)$. As a group I is just $\{at^2 : a \in k\}$ and for $a, b \in k$ we have $(t+at^2)(t+bt^2) = t^2 + (a+b)t^3 + abt^4 = t^2$ in A, which is not zero (for any (a,b)). So we deduce that the homomorphism $k[X,Y]/(XY) \to A/I$ mapping X and Y to t does not lift to A.

[There is an awful lot of freedom here – altogether the six solutions submitted and the solution in my notes give no fewer than five different isomorphism classes of quadruples (A, I, x, y) which solve the problem!]

2. [3 points] Let $c > 1$ be an integer coprime to 6, and let ${}_c\theta(z,\tau)$ be the meromorphic function defined for $z \in \mathbf{C}$ and $\tau \in \mathcal{H}$ by

$$ {}_c\theta(z,\tau) = q^{\frac{c^2-1}{12}} (-t)^{\frac{-c(c-1)}{2}} \gamma_q(t)^{c^2} \gamma_q(t^c)^{-1}, $$

where $q = e^{2\pi i z}$, $q = e^{2\pi i \tau}$, and

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

[Note that there was a typographical error in the question – sorry! The sign on the exponent of $-t$ was wrong. The correct formula is as above.]

Show that:

(a) ${}_c\theta(z,\tau)$ depends only on the class of z modulo $\mathbb{Z} + \mathbb{Z}\tau$;

Solution: *[by Pedro Lemos]* It is enough to prove that ${}_c\theta(z+1,\tau) = {}_c\theta(z+\tau,\tau) = {}_c\theta(z,\tau)$ for every $z \in \mathbb{C}$. That ${}_c\theta(z+1,\tau) = {}_c\theta(z,\tau)$ is obvious, as $t' = e^{2\pi i(z+1)} = e^{2\pi i z} = t$.

Now consider ${}_c\theta(z+\tau,\tau)$. Note that $t' = e^{2\pi i(z+\tau)} = qt$, where $t = e^{2\pi iz}$ and $q = e^{2\pi i\tau}$. We are going to prove that $\frac{{}_c\theta(z+\tau,\tau)}{{}_c\theta(z,\tau)} = 1$, thus proving our result. We are going to do this by looking at each factor of the definition of ${}_c\theta$. Firstly,

$$\left(\frac{-qt}{-t}\right)^{\frac{-c(c-1)}{2}} = q^{\frac{-c(c-1)}{2}}.$$

Also note that

$$\gamma_q(qt)^{c^2} = \left(\prod_{n\geq 0}(1-q^{n+1}t)\prod_{n\geq 1}(1-q^{n-1}t^{-1})\right)^{c^2}$$

and

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

Hence,

$$\frac{\gamma_q(qt)^{c^2}}{\gamma_q(t)^{c^2}} = \left(\frac{1-t^{-1}}{1-t}\right)^{c^2} = (-t)^{-c^2}$$

and

$$\begin{aligned}\frac{\gamma_q(q^ct^c)^{-1}}{\gamma_q(t^c)^{-1}} &= \frac{\prod_{0\leq n<c}(1-q^nt^c)}{\prod_{1-c\leq n<1}(1-q^nt^{-c})}\\ &= \prod_{0\leq n<c}\frac{1-q^nt^c}{1-q^{-n}t^{-c}}\\ &= q^{1+2+\cdots+(c-1)}t^{c+c+\cdots+c}\prod_{0\leq n<c}(-1)\\ &= (-1)^ct^{c^2}q^{\frac{c(c-1)}{2}}.\end{aligned}$$

Therefore,

$$\begin{aligned}\frac{{}_c\theta(z+\tau,\tau)}{{}_c\theta(z,\tau)} &= \frac{q^{\frac{c^2-1}{12}}}{q^{\frac{c^2-1}{12}}}\cdot\frac{(-qt)^{\frac{-c(c-1)}{2}}}{(-t)^{\frac{-c(c-1)}{2}}}\cdot\frac{\gamma_q(qt)^{c^2}}{\gamma_q(t)^{c^2}}\cdot\frac{\gamma_q(q^ct^c)^{-1}}{\gamma_q(t^c)^{-1}}\\ &= q^{-c(c-1)/2}\cdot(-t)^{c^2}\cdot(-1)^ct^{-c^2}q^{\frac{c(c-1)}{2}}\\ &= (-1)^{c+c^2}\\ &= 1\end{aligned}$$

(since $c + c^2$ is even!)

[Most of you got this one, but the calculation is unavoidably painful; Pedro's solution was the shortest.]

(b) for τ fixed, the divisor of ${}_c\theta(z,\tau)$ as a meromorphic function on $E_\tau = \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ is $c^2(0) - E_\tau[c]$;

Solution: *[by Lars Sektnan]* It suffices to prove that for each q, the function $\gamma_q(t)$ nas no poles and vanishes (to order 1) exactly at the ponts of $\exp(2\pi i(\mathbb{Z}+\tau\mathbb{Z}))$. For then $\gamma_q^{c^2}$ vanishes to order c^2 at the point of E_τ which is the image of 0, and $\gamma_q(t^c)^{-1}$ has a pole of order 1 at each point t such that $t = e^{2\pi iz}$ for some $z \in c^{-1}(\mathbb{Z}+\tau\mathbb{Z})$. Since $(-t)^{-c(c-1)}/2$ has no poles or zeroes for non-zero t, it would then follow that ${}_c\theta(z,\tau)$ has a zero at 0 of

order c^2-1 and simple pole at each nonzero c-torsion point of E_τ, i.e.

$$\operatorname{div}({}_c\theta(z,\tau)) = c^2(0) - E_\tau[c]$$

as required.
Now, $\gamma_q(t)$ vanishes if and only if $t = q^n$ or $t^{-1} = q^n$ for some $n \geq 0$, i.e. if and only if $t \in q^{\mathbb{Z}}$, hence if and only if $z \in \mathbb{Z} + \mathbb{Z}\tau$. Since no other terms in the product can vanish, the vanishing is to order 1 as required.
[Pretty much everyone got this, but one has to be a little careful to take account of the fact that $0 \in E[c]$ so the two terms in the sum of divisors $c^2(0) - E_\tau[c]$ are not disjoint.]

(c) for any N coprime to c we have

$$\prod_{\substack{y \in E_\tau \\ Ny = z}} {}_c\theta(y,\tau) = {}_c\theta(z,\tau).$$

Solution: *[Partial solution by Chris Birkbeck, slightly adapted]*
If $[N] : E_\tau \to E_\tau$ is the multiplication-by-N map, we see that $\{y \in E_\tau : Ny = z\} = [N]^{-1}(z) = \{\frac{z}{N} + x : x \in E_\tau[N]\}$. So

$$\prod_{\substack{y \in E_\tau \\ Ny = z}} {}_c\theta(y,\tau) = \prod_{0 \leq a,b < N} {}_c\theta\left(\frac{z}{N} + \frac{a}{N} + \frac{b}{N}\tau\right).$$

We claim that the following two formulae hold:

$$\prod_{0 \leq a < N} {}_c\theta\left(\frac{z}{N} + \frac{a}{N}, \tau\right) = {}_c\theta(z, N\tau), \tag{†}$$

$$\prod_{0 \leq b < N} {}_c\theta(z + b\tau, N\tau) = {}_c\theta(z,\tau). \tag{‡}$$

Combining these obviously gives the result.
We first prove (†). Note that $e^{2\pi i\left(\frac{z}{N} + \frac{a}{N}\right)} = t^{1/N}\zeta_N^a$, where $\zeta_N = e^{2\pi i/N}$.
Now, we have

$$\prod_{0 \leq a < N} \gamma_q\left(\zeta_N^a t^{1/N}\right) = \prod_{n \geq 0}\prod_a (1 - q^n t^{1/N}\zeta_N^a) \cdot \prod_{n \geq 1}\prod_a (1 - q^n t^{-1/N}\zeta_N^{-a}).$$

Using the polynomial identity $\prod_{0 \leq a < N}(1 - \zeta_N^a X) = 1 - X^N$, this is

$$\begin{aligned}\prod_{0 \leq a < N} \gamma_q\left(\zeta_N^a t^{1/N}\right) &= \prod_{n \geq 0}(1 - q^{nN}t)\prod_{n \geq 1}(1 - q^{nN}t^{-1}) \\ &= \gamma_{q^N}(t).\end{aligned}$$

Moreover, for any c coprime to N, raising to the c-th power permutes the roots of unity of order N, so we have

$$\prod_{0 \leq a < N} \gamma_q\left(\zeta_N^{ac} t^{c/N}\right) = \gamma_{q^N}(t^c).$$

It follows that

$$\prod_{0 \leq a < N} {}_c\theta\left(\frac{z}{N} + \frac{a}{N}, \tau\right) = {}_c\theta(z, N\tau).$$

We now consider (‡). We calculate first the quantity

$$\prod_{0\le b<N} \gamma_{q^N}(q^b t) = \prod_b \prod_{n\ge 0} (1-q^{nN+b}t) \prod_{n\ge 1}(1-q^{nN-b}t^{-1}).$$

As n varies over integers ≥ 0 and b varies over $\{0,\dots,N-1\}$, the quantity $nN+b$ varies over all integers ≥ 0; and as n varies over integers ≥ 1 and b varies, the quantity $nN-b$ varies over integers ≥ 1. so we deduce

$$\prod_{0\le b<N} \gamma_{q^N}(q^b t) = \gamma_q(t).$$

[The evaluation of the term $\prod_{0\le b<N} \gamma_{q^N}(q^{bc}t^c)$ is more complicated, but proceeds along similar lines. The idea is to use the identity $\gamma_q(qt) = (-t)^{-1}\gamma_q(t)$ and induction to write

$$\gamma_{q^N}(q^{bc}t^c) = P_{b,c,N}(q,t)^{-1}\gamma_{q^N}(q^v t^c),$$

where $P_{b,c,N}(q,t)$ is some polynomial in q,t depending on b,c,N, and $v = N(bc/N - \lfloor bc/N \rfloor)$ is the reduction of bc modulo N. As the b's vary, the v's run over $\{0,..,N-1\}$ and we get

$$\prod_{0\le b<N} \gamma_{q^N}(q^{bc}t^c) = \gamma_q(t^c)\prod_b P_{b,c,N}(q,t)^{-1},$$

and then one shows that the product on the right simplifies down to a product of a power of q and a power of $-t$. Nobody did this, sadly!
As I set this question without doing it myself first, and it turned out to be significantly more difficult than I had expected, I gave all of you the mark for free.]

3. For integers c, N with $(c, 6N) = 1$ let ${}_c g_N(\tau)$ be the meromorphic function on $Y_1(N)$ defined by

$${}_c g_N(\tau) = {}_c\theta(1/N, \tau).$$

(a) [1 point] Show that the q-expansion coefficients of ${}_c g_N$ lie in $\mathbb{Z}[\zeta_N]$, and satisfy

$$a_n({}_c g_N)^\sigma = a_n\left(\langle \chi(\sigma)\rangle\, {}_c g_N\right)$$

for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$, where χ is the mod N cyclotomic character and $\langle d\rangle$ is the diamond operator.

Solution: *[by Chris Birkbeck]* We have

$${}_c g_N(\tau) = q^{\frac{c^2-1}{12}}(-\zeta_N)^{\frac{-c(c-1)}{2}} \prod_{n\ge 0}\left((1-q^n\zeta_N)^{c^2}\sum_{k\ge 0} q^{nk}\zeta_N^{ck}\right)\prod_{n\ge 1}\left((1-q^n\zeta_N^{-1})^{c^2}\sum_{k\ge 0} q^{nk}\zeta_N^{-ck}\right)$$

which clearly lies in $\mathbb{Z}[\zeta_N][[q]]$.
Next we want $a_n({}_c g_N)^\sigma = a_n(\langle\chi(\sigma)\rangle {}_c g_N)$ for $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Now, σ acts on $\mathbb{Q}(\zeta_N)$ by $\zeta_N \mapsto \zeta_N^d$ where $d = \chi(\sigma)$.
By the above se see that $a_n({}_c g_N)^\sigma$ will just be $a_n({}_c g_N)$ with all ζ_N replaced by ζ_N^d. As $\langle d\rangle {}_c g_N = \langle d\rangle {}_c\theta(1/N,\tau) = {}_c\theta(d/N,\tau)$, we obtain the desired result.

[Lots of you found this difficult, perhaps because you didn't spot the key identity

$$\langle d\rangle {}_c g_N(\tau) = {}_c\theta(d/N,\tau).$$

(b) [2 points] Show that ${}_cg_N$ generates $\mathbb{Q}(Y_1(N))$ as a field extension of $\mathbb{Q}(Y_0(N))$.

Solution: *[based on an idea by Pedro Lemos]* We know that for $N \geq 3$, we have $[\mathbb{Q}(Y_1(N)) : \mathbb{Q}(Y_0(N))] = [\Gamma_0(N) : \pm\Gamma_1(N)] = \phi(N)/2$. So it suffices to show that the subfield generated by ${}_cg_N$ has this degree over $\mathbb{Q}(Y_0(N))$.
I claim that if $u, v \in (\mathbb{Z}/N\mathbb{Z})^\times$, then $\langle u\rangle {}_cg_N = \langle v\rangle {}_cg_N$ if and only if $u = \pm v$. It is clear that this condition is sufficient.
Using part (c), we have

$$\operatorname{dlog}({}_cg_N) = -2\pi i(c^2 - \langle c\rangle)F_{1,N}^{(2)}\mathrm{d}z.$$

Let χ be a character of $(\mathbb{Z}/N\mathbb{Z})^\times$. Then we find that

$$\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times} \chi(d)^{-1}\langle d\rangle \operatorname{dlog}({}_cg_N) = -2\pi i(c^2 - \chi(c)) \sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times} \chi(d)^{-1}F_{d,N}^{(2)}$$

and the linear term of this is

$$-2\pi i(c^2 - \chi(c))(1 + \chi(-1))\tau(\chi, \zeta_N^c)$$

where $\tau(\chi, \zeta_N^c)$ is the Gauss sum, which is non-zero. Hence there is no character χ with $\chi(-1) = 1$ such that this sum is zero; equivalently, the stabilizer of $\operatorname{dlog}({}_cg_N)$ in $(\mathbb{Z}/N\mathbb{Z})^\times$ is ± 1.

(c) [2 points] Show that we have an equality of differentials

$$\operatorname{dlog}({}_cg_N) = -2\pi i\left(c^2F_{1,N}^{(2)} - F_{c,N}^{(2)}\right)\mathrm{d}z,$$

where $F_{b,N}^{(2)}$, for non-zero $b \in \mathbb{Z}/N\mathbb{Z}$, is the weight 2 Eisenstein series

$$F_{b,N}^{(2)}(q) = \frac{-1}{12} + \sum_{n\geq 1}\left(\sum_{d|n}\frac{n}{d}(\zeta_N^{bd} + \zeta_N^{-bd})\right)q^n.$$

Solution: *[by Pedro Lemos, edited for space]*
Let us apply logarithmic differentiation to ${}_cg_N$. We get *[using the identity* $\operatorname{dlog} AB = \operatorname{dlog} A + \operatorname{dlog} B$*, extended to infinite products by uniform convergence – DL]*

$$\frac{\operatorname{dlog}{}_cg_N(\tau)}{\mathrm{d}\,\tau} =$$
$$2\pi i\left(\frac{c^2-1}{12} + \sum_{n\geq 1}\left(\frac{n\zeta_N^c}{1-\zeta_N^c q^n} + \frac{n\zeta_N^{-c}}{1-\zeta_N^{-c}q^n}\right)q^n - c^2\sum_{n\geq 1}\left(\frac{n\zeta_N}{1-\zeta_N q^n} + \frac{n\zeta_N^{-1}}{1-\zeta_N^{-1}q^n}\right)q^n\right)$$

Since $|q| < 1$, this is equal to $-2\pi i(c^2H_1(\tau) - H_c(\tau))$ where

$$\begin{aligned} H_c(\tau) &= \frac{-1}{12} + \sum_{n\geq 1} n\zeta_N^c q^n\left(\zeta_N^c\sum_{j=0}^{\infty}\zeta_N^{jc}q^{jn} + \zeta_N^{-c}\sum_{j\geq 0}\zeta_N^{-jc}q^{jn}\right) \\ &= \frac{-1}{12} + \sum_{n\geq 1} n\left(\sum_{j=1}^{\infty}\zeta_N^{jc}q^{jn} + \sum_{j\geq 1}\zeta_N^{-jc}q^{jn}\right). \end{aligned}$$

Collecting terms according to the value of $m = in$ we have

$$H_c(\tau) = \frac{-1}{12} + \sum_{m \geq 1} \left(\sum_{j|m} \frac{m}{j} (\zeta_N^{cj} + \zeta_N^{-cj}) \right) q^m = F_{c,N}^{(2)}(q).$$

4. [1 point] Let X be a quasiprojective S-scheme, for S some scheme, equipped with a finite group G acting on X by S-scheme automorphisms. Is the functor $\underline{Sch/S} \to \underline{Sets}$ defined by

$$Y \mapsto \{\text{homs of } S\text{-schemes } Y \to X \text{ commuting with } G\text{-action}\}$$

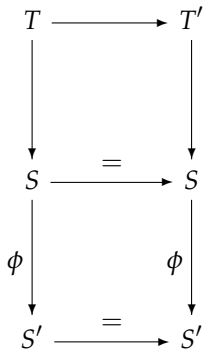
representable?

Solution: *[by Andrea Petracci]* Yes: it is represented by the closed subscheme X^G of fixed points for the G-action.

[Andrea went on to give a careful proof of the existence of this subscheme, with a reference to a 1992 paper by Edixhoven.]

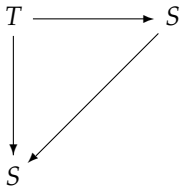
5. Recall that, for S a scheme, $\underline{Sch/S}$ denotes the "slice category" whose objects are pairs consisting of a scheme T and a morphism of schemes $T \to S$ (and whose morphisms are the obvious ones: morphisms of schemes $T \to U$ commuting with the morphism to S). There is a natural "forgetful functor" $\underline{Sch/S} \to \underline{Sch}$.
   (a) [1 point] Show that for any two schemes S, T, there is a canonical bijection between the following two sets:
   - morphisms of schemes $S \to S'$;
   - functors $\underline{Sch/S} \to \underline{Sch/S'}$ commuting with the forgetful map to $\underline{Sch}$.

Solution: *[by Lars Sektnan]*
If we are given a morphism $\phi : S \to S'$, we get a functor $\mathcal{F}_\phi : \underline{Sch/S} \to \underline{Sch/S'}$ by sending an object $T \to S$ of $\underline{Sch/S}$ to the object $T \to S'$ of $\underline{Sch/S'}$ obtained by composing $T \to S$ with the morphism ϕ. From the commutative diagram



we see how to define $\mathcal{F}_\phi$ on morphisms, so $\mathcal{F}_\phi$ is a functor. Since the underlying scheme of $T \to S$ and $T \to S'$ is T in both cases, $\mathcal{F}_\phi$ commutes with the forgetful functor to $\underline{Sch}$.
Conversely, given a functor $\mathcal{F} : \underline{Sch/S} \to \underline{Sch/S'}$ we get a morphism $S \to S'$ by considering $\mathcal{F}$ applied to the S-scheme S (with the identity morphism $S \to S$) *[i.e. the terminal object of $\underline{Sch/S}$ – DL.]* This gives a morphism $\phi_{\mathcal{F}} : S \to S'$.
To see that the two maps thus constructed are inverse to each other, let ϕ be a morphism $S \to S'$. Then $\mathcal{F}_\phi(S \to S)$ is the object $S \to S'$ given by composing id_S with ϕ, so $\phi_{F_\phi} = \phi$.

Conversely, let $\mathcal{F}$ be a functor $\underline{Sch/S} \to \underline{Sch/S'}$ commuting with the forgetful map. We get a morphism $\phi_{\mathcal{F}} : S \to S'$. Let $T \to S$ be a scheme over S. We must show that $\mathcal{F}(T \to S) = \mathcal{F}_{\phi_{\mathcal{F}}}(T \to S)$, where $\mathcal{F}_{\phi_{\mathcal{F}}}(T \to S)$ is the S'-scheme T given by composing $T \to S$ with $\phi_{\mathcal{F}}$. But the diagram



gives a morphism $(T \to S) \to (S \to S)$ in $\underline{Sch}/S$, so we must have a morphism $\mathcal{F}(T \to S) \to \mathcal{F}(S \to S)$ in $\underline{Sch/S'}$ (since $\mathcal{F}$ is a functor), so $\mathcal{F}_{\phi_{\mathcal{F}}} = \mathcal{F}$.

[This was, amazingly, the only complete solution! The other five of you all gave the two constructions $\mathcal{F} \mapsto \phi_{\mathcal{F}}$ and $\phi \mapsto \mathcal{F}_{\phi}$ but either did not bother to check that they were inverse to each other, or attempted the check but did so wrongly.]

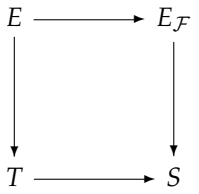
(b) [1 point] Show that for any scheme S there is a canonical bijection between

- elliptic curves over S,
- functors $\underline{Sch/S} \to \underline{Ell/\mathbb{Z}}$ commuting with the forgetful map to $\underline{Sch}$.

Solution: Let E be a an elliptic curve over S. We define a functor $\mathcal{F}_E : \underline{Sch/S} \to \underline{Ell/\mathbb{Z}}$ as follows. If $T \to S$ is an object of $\underline{Sch/S}$, we define $\mathcal{F}_E(T)$ to be the fibre product $E \times_S T$ with its natural map to T. (Since the fibre of $E \times_S T$ over $t \in T$ is the fibre of E over $f(T) \in S$, this is indeed an elliptic curve). If $T \to T'$ is a morphism of S-schemes, then this gives a morphism $E \times_S T \to E \times_S T'$, and we have $(E \times_S T') \times'_T T = (E \times_S T)$, so we obtain a morphism in $\underline{Ell/\mathbb{Z}}$.

Conversely, if $\mathcal{F} : \underline{Sch/S} \to \underline{Ell/\mathbb{Z}}$ is a functor, then $\mathcal{F}(S \to S)$ is an object of $\underline{Ell/\mathbb{Z}}$, and if $\mathcal{F}$ commutes with the forgetful functor, the base scheme of this elliptic curve must be S itself. So we obtain an elliptic curve $E_{\mathcal{F}}$ over S.

I claim that the maps $\mathcal{F} \to E_{\mathcal{F}}$ and $E \to \mathcal{F}_E$ are mutually inverse. Firstly, the image of $S \to S$ under $\mathcal{F}_E$ is the elliptic curve $E \times_S S = E$ over S, so $E_{\mathcal{F}_E} = E$. On the other hand, given $\mathcal{F}$ and an object $T \to S$ of $\underline{Sch}/S$, the image of the canonical morphism $(T \to S) \to (S \to S)$ of S-schemes is a morphism in $\underline{Ell}/\mathbb{Z}$ from $\mathcal{F}(T \to S)$ to $\mathcal{E}_F/S$, i.e. a diagram



where $E \to T = \mathcal{F}(T \to S)$. The definition of morphisms in the category $\underline{Ell}/\mathbb{Z}$ now implies that $E = E_{\mathcal{F}} \times_S T$ and hence $\mathcal{F}_{E_{\mathcal{F}}} = \mathcal{F}$.

[Not a single one of you did the final check correctly! You should be ashamed of yourselves.]

(* This justifies thinking of $\underline{Ell/\mathbb{Z}}$ as *the category of S'-schemes, for a non-existent S' representing the functor $S \to \{$elliptic curves over $S\}$*. Can you construct a similar category which is "the universal elliptic curve over $\underline{Ell/\mathbb{Z}}$"? *)

Solution: See the excellent article *What Is... A Stack?* in the Notices of the AMS. The correct choice is to let $\mathcal{C}$ be the category whose objects are triples of a base scheme S, an elliptic curve E/S and a section $S \to E$.

6. Let $\mathcal{P}$ be a moduli problem on $\underline{Ell}/R$, for some ring R, and let $\widetilde{\mathcal{P}}$ be the associated contravariant functor $\underline{Sch}/R \to \underline{Sets}$.

   (a) [2 points] Show that

   $$(\mathcal{P} \text{ is representable}) \Leftrightarrow (\mathcal{P} \text{ is rigid and } \widetilde{\mathcal{P}} \text{ is representable}).$$

   Solution: *[by Diletta Martinelli, somewhat condensed]*
   Firstly, we show the "⇒" direction. Let's assume that $\mathcal{P}$ is represented by an elliptic curve E_0/S_0 together with some universal $\alpha_0 \in \mathcal{P}(E_0/S_0)$. Then, for any $E'/S' \in \mathrm{Obj}(\underline{Ell}/R)$ and $\alpha' \in \mathcal{P}(E'/S')$, there is a unique way to find a morphism $\phi : S' \to S_0$ and an isomorphism $\iota : E' \cong E_0 \times_{(S_0,\phi)} S'$ such that the pullback of α_0 is α'.
   We want to prove that $\widetilde{\mathcal{P}}$ is represented by the object S_0 and the element $(E_0, \alpha) \in \widetilde{\mathcal{P}}(S_0)$. But for each R-scheme S' and each $(E'/S', \alpha) \in \widetilde{\mathcal{P}}(S_0)$, we can interpret E'/S' as an object of $\underline{Ell}/R$ and α as an element of $\mathcal{P}(E'/S')$, so there is a unique pair (ϕ, ι) as above; in particular, there is a unique $\phi : S' \to S_0$ such that $(E'/S', \alpha')$ is isomorphic to the pullback of $(E_0/S_0, \alpha_0)$. Thus $\widetilde{\mathcal{P}}$ is representable. Moreover, since ι is also unique, $\mathrm{Aut}(E'/S')$ must act without fixed points on $\mathcal{P}(E'/S')$, so $\mathcal{P}$ is rigid.
   Conversely, if $S_0, (E_0, \alpha_0)$ represents $\widetilde{\mathcal{P}}$ and $\mathcal{P}$ is rigid, then for every $E/S \in \mathrm{Obj}(\underline{Ell}/R)$ and each $\alpha \in \mathcal{P}(E/S)$, there exists a unique morphism $\phi : S \to S_0$ such that $(E/S, \alpha)$ is isomorphic to the pullback of $(E_0/S_0, \alpha_0)$. By the rigidity of $\mathcal{P}$, this isomorphism $(E/S, \alpha) \cong (E_0/S_0, \alpha_0)$ is unique, so we have a unique morphism $E/S \to E_0/S_0$ in $\underline{Ell}/R$ for which the pullback of α_0 is α; that is, $(E_0/S_0, \alpha_0)$ represents $\mathcal{P}$.

   (b) [2 points] Assume that there exists an elliptic curve E_0 over $\operatorname{Spec} R$. Let $\mathcal{P}$ be the following (rather pathological) moduli problem:

   $$\mathcal{P}(E/S) = \begin{cases} \text{the set with one element,} & \text{if } E \text{ is isomorphic over } S \text{ to } E_0 \times_R S \\ \varnothing, & \text{otherwise.} \end{cases}$$

   Show that $\mathcal{P}$ is not rigid, but $\widetilde{\mathcal{P}}$ is representable (by $\operatorname{Spec} R$ itself). [*This counterexample is due to Ofer Gabber and is in section A.4 of Katz–Mazur.*]

   Solution: *Look in Katz–Mazur, which should be in any decent departmental library.*

[As pointed out by Andrea Petracci, these statements are not at all specific to the category Ell $/R$*: they work whenever you have two categories $\mathcal{C}$, $\mathcal{D}$ with a functor $p : \mathcal{C} \to \mathcal{D}$ satisfying two straightforward axioms. The technical term for this is that* Ell $/R$ *is a "category fibred in groupoids over* Sch $/R$*".]*

7. Recall the series $X(u,q), Y(u,q)$ defined in the section on the Tate curve.

   (a) [2 points] Verify that we have

   $$\frac{\frac{\mathrm{d}}{\mathrm{d}u}X(u,q)}{2Y(u,q) + X(u,q)} = \frac{1}{u}.$$

   Solution: *[Everybody got this right, so I won't bother to type out the argument.]*

   (b) [1 point] Why do the projective coordinates

   $$((1-u)^3X(u,q) : (1-u)^3Y(u,q) : (1-u)^3)$$

   not define a morphism of schemes over $R = \mathbb{Z}[[q]]$ from $\mathbf{G}_m/R$ to $\mathrm{Tate}(q)$? *[Hint: Convince yourself that $\mathbb{Z}[u][[q]]$ is not the same ring as $\mathbb{Z}[[q]][u]$.]*

Solution: *[by Andrea Petracci]*
The elements $(1-u)^3X, (1-u)^3Y, (1-u)$ lie in $\mathbb{Z}[u,u^{-1}][[q]]$ and satisfy the defining equation

$$y^2z + xyz = x^3 + a_4xz + a_6z^3$$

of the Tate curve; so they define a morphism $\operatorname{Spec}\mathbb{Z}[u,u^{-1}][[q]] \to \operatorname{Tate}(q)$ over $\operatorname{Spec}\mathbb{Z}[[q]]$, and we have a commutative diagram

$$\begin{array}{ccc} \operatorname{Spec}\mathbb{Z}[u,u^{-1}][[q]] & \longrightarrow & \operatorname{Tate}(q) \\ \downarrow & & \downarrow \\ \operatorname{Spec}\mathbb{Z}[[q]][u,u^{-1}] & \longrightarrow & \operatorname{Spec}\mathbb{Z}[[q]]. \end{array}$$

Notice that $\operatorname{Spec}\mathbb{Z}[[q]][u,u^{-1}] = \mathbb{G}_m/\mathbb{Z}[[q]]$. So the question is whether we can find a diagonal arrow $\operatorname{Spec}\mathbb{Z}[[q]][u,u^{-1}] \to \operatorname{Tate}(q)$ making the diagram commute.
The answer is no, since $(1-u)^3X$ does not lie in $\mathbb{Z}[[q]][u,u^{-1}]$ as it has terms of arbitrarily high degree in u.

(c) (*) If you know about formal schemes, convince yourself that this formula *does* define a morphism of formal schemes over R from $\widehat{\mathbf{G}_m}$ to the formal completion of $\operatorname{Tate}(q)$ at infinity, and the pullback of the invariant differential $\frac{dX}{2Y+X}$ on $\operatorname{Tate}(q)$ is the invariant differential $\frac{du}{u}$ on $\widehat{\mathbf{G}_m}$. *[Hint: Convince yourself that $\mathbb{Z}[[u]][[q]]$* ***is*** *the same ring as $\mathbb{Z}[[q]][[u]]$.]*

8. [4 points] List the eight cusps of $Y(3)$, and the action of $\operatorname{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ on them.

Solution: Recall that the cusps of $Y(3)$ are given by $\Gamma(3)$-level structures on the Tate curve $\operatorname{Tate}(q)$ over the $\mathbb{Z}[1/3]$-algebra $\mathbb{Z}((r)) \otimes \mathbb{Z}[\zeta, 1/3]$, where $r = q^{1/3}$ and $\zeta = \zeta_3$, modulo the automorphisms given by multiplication by -1 on the curve and by $r \mapsto \zeta_3^a r$, $a = 0, 1, -1$. Note that there are $(3^2-1)(3^2-3) = 48$ choices of $\Gamma(3)$-level structures over this large ring, and the group acting has order 6, so this gives us 8 cusps:

$$\begin{aligned} S_1 &= \{(r,\zeta),(r\zeta,\zeta),(r\zeta^{-1},\zeta),(r^{-1},\zeta^{-1}),(r^{-1}\zeta,\zeta^{-1}),(r^{-1}\zeta^{-1},\zeta^{-1})\} \\ S_2 &= \{(r,\zeta^{-1}),(r\zeta,\zeta^{-1}),(r\zeta^{-1},\zeta^{-1}),(r^{-1},\zeta),(r^{-1}\zeta,\zeta),(r^{-1}\zeta,\zeta)\} \\ S_3 &= \{(r,r\zeta),(r\zeta,r\zeta^{-1}),(r\zeta^{-1},r),(r^{-1},r^{-1}\zeta^{-1}),(r^{-1}\zeta^{-1},r^{-1}\zeta),(r^{-1}\zeta,r^{-1})\} \\ S_4 &= \{(r,r^{-1}\zeta),(r\zeta,r^{-1}),(r\zeta^{-1},r^{-1}\zeta^{-1}),(r^{-1},r\zeta),(r^{-1}\zeta,r),(r^{-1}\zeta,r\zeta)\} \end{aligned}$$

and T_1, T_2, T_3, T_4 which are the images of these under the involution that swaps the two vectors in the basis of the 3-torsion. The action of Galois is now given by swapping S_1 with S_2, T_1 wtih T_2, S_3 with T_3 and S_4 with T_4.