Modular Curves (TCC) Problem Sheet 2 – Solutions

David Loeffler

10th March 2014

---

1. [2 points] Let C be the curve in $\mathbb{A}^2/\mathbb{Q}$ defined by the classical modular polynomial $\Phi_2(X, Y)$ of level 2. Show that $(-3375, -3375)$ is a singular point of C.

> **Solution:** From lecture notes, we have
>
> $$\Phi_N(X,Y) = X^3 + Y^3 - X^2Y^2 + 1488XY(X+Y) - 162000(X^2+Y^2) + 40773375XY + 8748000000(X+Y) - 157464000000000.$$
>
> With the aid of a computer (or by hand) we find that $\Phi(-3375, -3375) = \frac{\partial\Phi}{\partial X}(-3375, -3375) = 0$. By symmetry this forces $\frac{\partial\Phi}{\partial Y}$ also to vanish, so $(-3375, -3375)$ is a singular point.

2. [3 points] Let f be the modular function of level $\Gamma_0(2)$ given by $\Delta(2z)/\Delta(z)$, where $\Delta(z)$ is the unique normalized weight 12 cusp form of level $\mathrm{SL}_2(\mathbb{Z})$.

   (a) Show that f gives an isomorphism of algebraic varieties over $\mathbb{Q}$ between $X_0(2)$ and $\mathbb{P}^1$.

   > **Solution:** We first check the statement over $\mathbf{C}$. Both $\Delta(z)$ and $\Delta(2z)$ are non-vanishing on $\mathcal{H}$, hence so is f, and the q-expansion of f is $q + \dots$ so f has a simple zero at ∞. Because a principal divisor has degree 0, it must have a simple pole at 0 and thus defines a degree 1 map to $\mathbb{P}^1$, hence an isomorphism.
   > Now we note that f obviously has q-expansion in $\mathbb{Q}[[q]]$, so it lies in $\mathbb{Q}(X_0(N))$. So it defines a map $X_0(N) \to \mathbf{P}^1$ over $\mathbb{Q}$ which is an isomorphism over $\mathbb{C}$, hence an isomorphism over $\mathbb{Q}$.

   (b) Describe the preimage in $X_0(2)$ of the point $(-3375, -3375)$ of C. (You may assume the following formulae:
   $$j(z) = \frac{(1+2^8 f)^3}{f}, \quad j(2z) = \frac{(1+2^4 f)^3)}{f^2}.)$$

   > **Solution:** Solving for $\frac{(1+2^8f)^3}{f} = -3375$, $\frac{(1+2^4f)^3)}{f^2} = -3375$ we obtain the simultaneous equations $(f+1/4096)(f^2+47/4096f+1/4096) = 0$, $(f+1)(f^2+47/4096f+1/4096) = 0$. So the preimage of $(-3375, -3375)$ in $X_0(2)$ is the $\mathbb{Q}$-scheme $\operatorname{Spec}\mathbb{Q}[f]/(f^2+47/4096f+1/4096)$, which is a complicated way of writing $\operatorname{Spec}\mathbb{Q}(\sqrt{-7})$. (Over $\mathbb{C}$ this is two points, interchanged by the Galois action.)

3. [4 points] Check the the following assertions from the lectures:

   (a) The map $\tau \mapsto (\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), \frac{1}{N}\mathbb{Z})$ gives a bijection between $\Gamma_0(N)\backslash\mathcal{H}$ and the set of equivalence classes of pairs (E, C), where E is an elliptic curve over $\mathbb{C}$ and C is a cyclic subgroup of E of order N.

(b) The map $\tau \mapsto (\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), \frac{1}{N})$ gives a bijection between $\Gamma_1(N)\backslash\mathcal{H}$ and the set of equivalence classes of pairs (E, P), where E is an elliptic curve over $\mathbb{C}$ and P is a point of E of exact order N.

Solution: We know that every elliptic curve over $\mathbb{C}$ is isomorphic to $E_\tau := \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$, for some $\tau \in \mathcal{H}$; and E_τ is isomorphic to $E_{\tau'}$ if and only if τ and τ' are in the same $\mathrm{SL}_2(\mathbb{Z})$-orbit, in which case any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mapping τ to τ' gives an isomorphism $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau') \to \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ via $z \mapsto (c\tau+d)z$ on $\mathbb{C}$.

(a) Firstly, we see that the map $E_{\gamma\tau} \to E_\tau$ given by γ sends $1/N$ to $\frac{(c\tau+d)}{N}$ mod $\mathbb{Z}+\mathbb{Z}\tau$; this is in $\frac{1}{N}\mathbb{Z}$ modulo $\mathbb{Z}+\mathbb{Z}\tau$ if and only if $\gamma \in \Gamma_0(N)$. So the map is well-defined and injective.

Now we check surjectivity. Let E be an elliptic curve and C a cyclic subgroup of order N. We know that E is $\mathbb{C}/\Lambda$ for some lattice Λ, and, using the Smith normal form for abelian groups, we can find a basis u, v of Λ as a $\mathbb{Z}$-module such that the image of v/N generates C. At least one of v/u and $-v/u$ is in $\mathcal{H}$ and this gives the surjectivity of the map.

(b) The proof that the map is well-defined and injective is similar to (a) with the very minor change that the image of $1/N$ is $1/N$ modulo $\mathbb{Z}+\mathbb{Z}\tau$ if and only if $\gamma \in \Gamma_1(N)$. For the surjectivity we proceed exactly as before.

4. [3 points] Let E be an elliptic curve over $\mathbb{C}$, and $N > 1$. The *Weil pairing* is a perfect pairing $E[N] \times E[N] \to \mu_N$ (the exact definition is not relevant for this question, but it is given in Silverman's elliptic curves book). You may assume the following fact: if $E = \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$, then $\langle \tau/N, 1/N \rangle_{E[N]} = e^{2\pi i/N}$.

Using this, prove that the map $\tau \mapsto (\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), \frac{\tau}{N}, \frac{1}{N})$ gives a bijection between $\Gamma(N)\backslash\mathcal{H}$ and the set of equivalence classes of triples (E, P, Q) with E an elliptic curve over $\mathbb{C}$ and P, Q two points of order N on E with $\langle P, Q \rangle_{E[N]} = e^{2\pi i/N}$.

Solution: We proceed as before to see that $E_{\gamma\tau} \to E_\tau$ sends $1/N$ to $\frac{c\tau+d}{N}$ and τ/N to $\frac{a\tau+b}{N}$ modulo $\mathbb{Z}+\mathbb{Z}\tau$. This shows that the map is injective (and well-defined).

For surjectivity we must be a little more crafty. Given a triple (E, P, Q), we may assume without loss of generality that $E = E_\tau$ for some τ. We have $P, Q = \frac{a\tau+b}{N}, \frac{c\tau+d}{N}$ for some $a, b, c, d \in \mathbb{Z}/N\mathbb{Z}$, and since $\langle P, Q \rangle = e^{2\pi i/N}$, we know that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. It is a known result that $\mathrm{SL}_2(\mathbb{Z})$ surjects onto $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so so we can choose some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mod N. Then the map $E_{\gamma\tau} \to E_\tau$ sends $(\tau/N, 1/N)$ to P, Q, and hence $(E, P, Q) \sim (E_{\tau'}, \tau'/N, 1/N)$ where $\tau' = \gamma\tau$.

5. [6 points] For each of the following functors $\mathcal{F} : \mathcal{C} \to \underline{Set}$, either write down an object X of $\mathcal{C}$ and an element of $\mathcal{F}(X)$ which represent $\mathcal{F}$, or prove that $\mathcal{F}$ is not representable.

(a) The functor $\underline{Ring} \to \underline{Set}$ mapping a ring R to the set of cube roots of 1 in R.

Solution: This is represented by $(\mathbb{Z}[T]/(T^3-1), T)$.

(b) The restriction of the functor from (a) to the subcategory $\underline{\mathbf{F}_5 - Alg}$ of $\mathbf{F}_5$-algebras.

Solution: This is represented by $(\mathbf{F}_5[T]/(T^3-1), T)$.

(c) The functor $\underline{Ring} \to \underline{Set}$ mapping R to the set of cubes in R.

Solution: This is not representable. If it were represented by (S, α) for some α, then we would have $\alpha = \beta^3$ for some $\beta \in R$. Now consider the ring $S' = \mathbb{C}[T]$ with the cube T^3. Then there would have to be a unique homomorphism $\phi : S \to S'$ mapping α to T^3, which would therefore have to send β to one of $\{T, e^{2\pi i/3}T, e^{-2\pi i/3}T\}$. But then ϕ cannot be the same as $\sigma \circ \phi$, where σ is the automorphism given by $T \mapsto e^{2\pi i/3}T$, so we get a contradiction.

(d) The functor $\underline{\mathbb{R} - Alg} \to \underline{Set}$ mapping R to the set of all vector space homomorphisms $\mathbb{R}^2 \to R$.

Solution: This functor is the same as (i.e. is naturally isomorphic to) the functor mapping R to the set of ordered pairs of elements of R, which is represented by $\mathbb{R}[X, Y]$.

(e) The functor from the category $\underline{Top}$ of all topological spaces to $\underline{Set}$ which maps a topological space T to the set of its points.

Solution: Represented by the unique one-point space.

(f) The contravariant functor $\underline{Top} \to \underline{Sets}$ which maps a topological space T to the set of open subsets of T.

Solution: Represented by the two-point space $\{x_1, x_2\}$ with the topology for which the open sets are $\{\varnothing, \{x_1\}, \{x_1, x_2\}\}$.

6. [2 points] (a) Let $\mathcal{F}$ be a representable functor $\underline{Ring} \to \underline{Set}$. Show that if $(R_i)_{i \ge 1}$ is a projective system of rings (i.e. a collection of rings R_i and morphisms $R_{i+1} \to R_i$) and $R = \varprojlim R_n$, then $\mathcal{F}(R) = \varprojlim_n \mathcal{F}(R_n)$.

Solution: It suffices to show that if S is any ring then there is a bijection $\hom(S, \varprojlim_i R_i) \to \varprojlim_i \hom(S, R_i)$. Depending on your taste, this is either an elementary exercise, or is the definition of the projective limit.

(b) Hence show that the functor $\underline{Ring} \to \underline{Set}$ mapping a ring R to the set of roots of unity in R is not representable.

Solution: Fix a prime p and consider the rings $R_i = \mathbb{Z}/p^i$. Since R_i is finite, every invertible element of R_i is a root of unity, so if $\mathcal{F}$ is this functor then $\varprojlim_i \mathcal{F}(R_i) = \varprojlim_i R_i^\times = \mathbb{Z}_p^\times$. But $p+1$ is an element of $\mathbb{Z}_p^\times$ which is not a root of unity in $\mathbb{Z}_p$, so $\mathcal{F}(\mathbb{Z}_p) \ne \mathbb{Z}_p^\times$.

7. [3 points] Give an example of a scheme S, an elliptic curve E/S, an integer $N > 1$, and a section $P \in E(S)$ such that $nP \ne 0$ but $nP_x = 0$ as a point on E_x for every $x \in S$.

Solution: There were many nice solutions to this question. For instance, take $S = \operatorname{Spec} k[t]/t^2$ for k a field (of characteristic not 2 or 3), E the curve $y^2 = x^3 - 1$, and P the section $(1, t)$. The scheme S has only one point (corresponding to the ideal (t)) and the reduction modulo t is just the order 2 point $(1, 0)$ of $y^2 = x^3 - 1$ over k; but $-P$ is the section $(1, -t)$ which is not equal to P as an element of $E(S)$.

(This kind of pathology is specific to non-reduced schemes, and conversely more or less any non-reduced scheme will work! Other nice examples that were submitted included an example of an elliptic curve over $\mathbb{Z}/49$ and a point whose reduction modulo 7 had order 4.)

8. [2 points] Let R be a local ring. Show that every elliptic curve over $\operatorname{Spec} R$ has a Weierstrass equation.

> **Solution:** If R is a local ring and $\{U_i\}_{i\in I}$ is an open cover of $\operatorname{Spec} R$, then at least one of the U_i must contain the point corresponding to the unique maximal ideal of R; but this forces U_i to be the whole of $\operatorname{Spec} R$, since every nonempty closed subset of $\operatorname{Spec} R$ contains this point. Since we know there is an open cover over which E has a Weierstrass equation, we conclude that actually E has a Weierstrass equation over R.

9. [2 points] Let E be the elliptic curve over $\mathbb{Z}[1/(2\times 37)]$ defined by $y^2 = x^3 - 16x + 16$, and P the point $(0,4)$. Find $\alpha, \beta \in \mathbb{Q}$ and an isomorphism between E and the Tate-normal-form elliptic curve $E(\alpha,\beta)$ that maps P to $(0,0)$.

> **Solution:** Let (X,Y) be coordinates on $Y^2 = X^3 - 16X + 16$. First we kill the constant term by a translation sending $(0,4)$ to $(0,0)$: let $(X_1,Y_1) = (X, Y-4)$; then
>
> $$(Y_1+4)^2 = X_1^3 - 16X_1 + 16 \Leftrightarrow Y_1^2 + 8Y_1 = X_1^3 - 16X_1.$$
>
> Now we kill the linear term in X by a shear transformation: let $(X_2,Y_2) = (X_1, Y_1 + 2X_1)$; then
>
> $$(Y_2 - 2X_2)^2 + 8(Y_2 - 2X_2) = X_2^3 - 16X_2 \Leftrightarrow Y_2^2 - 4X_2Y_2 + 8Y_2 = X_2^3 - 4X_2^2.$$
>
> Now we scale to make the coefficients of Y and X^2 equal: we set $(X_3,Y_3) = (X_2/4, -Y_2/8)$; then
>
> $$64Y_3^2 + 128X_3Y_3 - 64Y_3 = 64X_3^3 - 64X_3^2 \Rightarrow Y_3^2 + 2X_3Y_3 - Y_3 = X_3^3 - X_3^2.$$
>
> This is in Tate normal form with $\alpha = 2$ and $\beta = -1$, and combining the transformations we have
>
> $$(X_3,Y_3) = (X/4, (4-Y-2X)/8).$$
>
> So the transformation $(X,Y) \mapsto (X/4,(4-Y-2X)/8)$ gives an isomorphism from E to the Tate normal form curve $E(2,-1)$; the inverse is given by $(X,Y) \mapsto (4X, 4-8X-8Y)$.

[I took off a mark for anyone who didn't give an explicit formula for either the morphism $E \to E(2,-1)$, or its inverse $E(2,-1) \to E$.]

10. [3 points] Find an equation for $Y_1(6)$ (as a $\mathbb{Z}[1/6]$-scheme), and the universal pair (E,P) over it.

> **Solution:** Recall the formulae for the multiples of $P = (0:0:1)$ on the universal Tate-normal-form curve $E(A,B)$ over $S = \operatorname{Spec} \mathbb{Z}[A,B,\Delta(A,B)^{-1}]$. We have
>
> $$3P = (1-A : A-B-1 : 1), \quad -3P = (1-A, (A-1)^2, 1).$$
>
> So the subscheme of S where $6P = 0$ is given by $A - B - 1 = (A-1)^2$ or $B = -(A-1)(A-2)$. Since 6 has no proper divisors > 3, this is also the locus where P has exact order 6. Hence we have
>
> $$\begin{aligned} Y_1(6) &= \operatorname{Spec} \mathbb{Z}[\tfrac{1}{6}, A, \Delta(A, -(A-1)(A-2))^{-1}] \\ &= \operatorname{Spec} \mathbb{Z}[\tfrac{1}{6}, A, (A-1)^{-1}, (A-2)^{-1}, (9A-10)^{-1}] \end{aligned}$$
>
> (since $\Delta(A, -(A-1)(A-2)) = (A-1)^6(A-2)^3(9A-10)$), and the universal elliptic curve over $Y_1(6)$ is given by $E(A, -(A-1)(A-2))$.