# Modular Curves (TCC) Problem Sheet 2

David Loeffler

21st February 2014

This is the second 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 30; the number of marks available for each question is indicated.

Work should be submitted, on paper or by email, on or before Friday 7th March.

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

---

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 $C$.

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

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 $N$.

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 $\langle P, Q \rangle_{E[N]} = e^{2\pi i/N}$.

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 $R$.
   (b) The restriction of the functor from (a) to the subcategory $\underline{\mathbf{F}_5 - Alg}$ of $\mathbf{F}_5$-algebras.
   (c) The functor $\underline{Ring} \to \underline{Set}$ mapping $R$ to the set of cubes in $R$.
   (d) The functor $\underline{\mathbb{R} - Alg} \to \underline{Set}$ mapping $R$ to the set of all vector space homomorphisms $\mathbb{R}^2 \to R$.
   (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.

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

6. [2 points] (a) Let $\mathcal{F}$ be a representable functor $\underline{Ring} \to \underline{Set}$. Show that if $(R_i)_{i\geq 1}$ 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 $\mathcal{F}(R) = \varprojlim_n \mathcal{F}(R_n)$.

   (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.

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 $nP \neq 0$ but $nP_x = 0$ as a point on $E_x$ for every $x \in \operatorname{Spec} S$.

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

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 $(0, 0)$.

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.