Explicit Arithmetic for Modular Curves

Exercises

(A) Let E/K be an elliptic curve and suppose E has a K-rational 3-isogeny. Show that there is a quadratic twist E' that has a point of order 3.

(B) Let K be a field complete with respect to a non-archimedean valuation $|\cdot|$ (e.g. $K = \mathbb{Q}_p$). Let $q \in K^*$ satisfy $|q| < 1$. Let E_q be the Tate elliptic curve with parameter q (for this exercise you don't need to know what that is). Tate showed that there is an analytic isomorphism

$$\phi \; : \; E_q(\overline{K}) \to \overline{K}^*/q^{\mathbb{Z}}$$

that respects the action of $G_K = \mathrm{Gal}(\overline{K}/K)$. Use this to show that

$$\overline{\rho}_{E,N} \sim \begin{pmatrix} \chi_N & * \\ 0 & 1 \end{pmatrix}.$$

You can probably look up the answer to this; it is for example given in Chapter 2, Section 9 of the course notes. But it is extremely beneficial to do it on your own.

(C) Let p be a prime. Let $\mathrm{PGL}_2(\mathbb{F}_p)$ be the quotient of $\mathrm{GL}_2(\mathbb{F}_p)$ by the subgroup consisting of scalar matrices $\{\alpha I_2 : \alpha \in \mathbb{F}_p^\times\}$. Let E be an elliptic curve over $\mathbb{Q}$, and let $\mathbb{P}\overline{\rho}_{E,p}$ denote the composition

$$G_{\mathbb{Q}} \xrightarrow{\overline{\rho}_{E,p}} \mathrm{GL}_2(\mathbb{F}_p) \to \mathrm{PGL}_2(\mathbb{F}_p).$$

Now let $p \geq 7$ be a prime of potentially multiplicative reduction for E. Show that the image of $\mathbb{P}\overline{\rho}_{E,p}$ is not isomorphic to A_4, S_4, A_5. (**Hint:** E has potentially multiplicative reduction at p means that $E/\mathbb{Q}_p$ is a quadratic twist of a Tate curve. You may suppose that $\chi_p : G_p \to (\mathbb{Z}/p\mathbb{Z})^*$ is surjective, where $G_p = \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ is the decomposition subgroup of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$).