Explicitly Computing

$\bar{\mathbb{Q}} \subseteq \mathbb{C}$, $z \mapsto \bar{z}$

$E/\mathbb{Q}$ elliptic curve

ℓ any prime

$$\bar{\rho}_{E,\ell} \quad \rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell)$$

$\mathbb{F}_\ell$-vs $\mathbb{F}_\ell$-alg

$\dim_{\mathbb{F}_\ell} E[\ell] = 2$

$\#E[\ell] = \ell^2$

$\#\mathrm{Aut}(E[\ell]) = \#GL_2(\mathbb{F}_\ell) = (\ell^2-1)(\ell^2-\ell)$

$\ell = 5$: $(\ell^2-1)(\ell^2-\ell) = 24 \cdot 20 = 480$

$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$

Theorem: $\mathbb{F}_\ell[x] \ni \mathrm{charpoly}(\rho_{E,\ell}(\mathrm{Frob}_p)) = x^2 - a_p(E)x + p$

$\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

$a_p(E) = p + 1 - \#E(\mathbb{F}_p)$

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\rho_{E,\ell}} & GL_2(\mathbb{F}_\ell) \\ & \searrow \quad \nearrow & \\ & \mathrm{Gal}(K/\mathbb{Q}) & \end{array}$$

K / $\mathbb{Q}$ number field

$K = \mathbb{Q}(x(P), y(P) : P \in E(\bar{\mathbb{Q}})[\ell])$

Galois extension.

$|a_p| \le 2\sqrt{p}$

$p=2$.

$\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})$ $\qquad$ $R_p = \mathfrak{P} \cdot (\text{other primes})$

$\mathfrak{P} \cap \mathbb{Z}$

$\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(K/\mathbb{Q})$

$p \in \mathbb{Z}$ prime unramified in K (if $p \nmid \ell \cdot \Delta_E$ then $p \mid \Delta_K$)

$\mathrm{Frob}_{\mathfrak{P}} \longleftrightarrow \mathfrak{P} \subset R = \mathcal{O}_K$.

$\mathbb{F}_{\mathfrak{P}} := R/\mathfrak{P}$

$$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \xrightarrow{\cong} \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p) \to 1$$

($I_{\mathfrak{P}}$: $\to 1$ by unramified)

$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{P}) \subseteq \mathfrak{P}\}$

$\langle \mathrm{Frob}_{\mathfrak{P}} \rangle$

$(x \mapsto x^p)$

Explicitly Computing

$\overline{\mathbb{Q}} \subseteq \mathbb{C}$, $z \mapsto \bar{z}$

$\rho_{E,\ell} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(E[\ell]) \cong GL_2(\mathbb{F}_\ell)$

$\ell = 5$.

$E = 11a$. $\quad \Delta = 5^3$

$\#E[5] = 25 = 1 + 12 + 12$.

$E[5] =$

$K = \mathbb{Q}(E[5])$

$\mathbb{Q}(\zeta_5) \subseteq K$, $[K : \mathbb{Q}(\zeta_5)] = 4$, G_4

$K = \mathbb{Q}[x]/(x^4 - x^3 + x^2 - x + 1)$, G_4

$E_K(K)_{tor} \cong \mathbb{Z}/5 \oplus \mathbb{Z}/5$.

$\Delta_K = 5^3$

$\mathbb{Q}(\zeta_\ell) \subseteq \mathbb{Q}(E[\ell])$ — cont. finitely often

$p=2$.

$\rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{P}})$

$R_p = \mathfrak{P} \cdot (\text{other primes})$

$\mathfrak{P} \cap \mathbb{Z}$

$\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(K/\mathbb{Q})$

$2 \neq p \in \mathbb{Z}$ prime unramified in K. (if $p \nmid \ell \cdot \Delta_E$ then $p \mid \Delta_K$)

$\mathrm{Frob}_{\mathfrak{P}} \longleftrightarrow \mathfrak{P} \subset R = \mathcal{O}_K$.

$\mathbb{F}_{\mathfrak{P}} := R/\mathfrak{P}$

$1 \to I_{\mathfrak{P}} \to D_{\mathfrak{P}} \xrightarrow{\cong} \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p) \to 1$

$I_{\mathfrak{P}}$ acts by 1

$\begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$

$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{P}) \subseteq \mathfrak{P}\}$

$\langle \mathrm{Frob}_{\mathfrak{P}} \rangle$

$(x \mapsto x^p)$