Integrality of the j–invariant of elliptic curves with complex multiplication

Francesc Gispert

10th April 2019

Lemma

- Let K be a p–adic field with normalized valuation $v_K \colon K^\times \to \mathbb{Z}$.
- Let E/K be an elliptic curve with $v_K(j(E)) < 0$.
- Take a prime $\ell \notin \{ 2, p \}$ such that and $\ell \nmid v_K(j(E))$.

- There exist σ in the inertia subgroup I_K of G_K and a basis (P_1, P_2) of $E[\ell]$ such that

$$\begin{pmatrix} P_1^\sigma & P_2^\sigma \end{pmatrix} = \begin{pmatrix} P_1 & P_2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Proof

- Since $j(E) \notin \mathcal{O}_K$, we have a G_K–equivariant isomorphism

$$E(\overline{K}) \cong \overline{K}^\times / q^{\mathbb{Z}}$$

  for some $q \in K^\times$ with $v_K(q) > 0$.

- In particular, $E[\ell]$ corresponds to

$$\zeta_\ell^i \cdot (q^{1/\ell})^j \quad \text{for } 0 \leq i, j < \ell,$$

  where

  - ζ_ℓ is a fixed primitive ℓ–th root of 1 and
  - $q^{1/\ell}$ is a fixed ℓ–th root of q.

Proof

- The condition $\ell \nmid v_K(j(E))$ is preserved under finite extensions L/K with $\ell \nmid [L:K]$ because

$$v_L|_K = e(L/K) v_K.$$

- Up to replacing K with a quadratic extension of K, we may assume that $E \cong E_q$ over K.
- Up to replacing K with $K(\zeta_\ell)$, we may assume that $\zeta_\ell \in K$.

Proof

- Recall that $v_K(q) > 0$ and

$$j(E) = j(E_q) = \frac{1}{q} + 744 + 196884q + \cdots.$$

- Therefore, $v_K(j(E)) = v_K\left(\frac{1}{q}\right) = -v_K(q)$.
- Now $\ell \nmid v_K(q)$, whence $K\left(q^{1/\ell}\right)/K$ is totally ramified of degree ℓ.

Proof

- Choose $\overline{\sigma} \in G_{K(q^{1/\ell})/K}$ such that

$$\left(q^{1/\ell}\right)^{\overline{\sigma}} = \zeta_\ell \cdot q^{1/\ell}.$$

- Since $K\left(q^{1/\ell}\right)/K$ is totally ramified, there exists a lift $\sigma \in G_K$ such that $\sigma|_{K^{\mathrm{ur}}} = \mathrm{id}_{K^{\mathrm{ur}}}$. That is, $\sigma \in I_K$.
- By construction,

$$\zeta_\ell^\sigma = \zeta_\ell \quad \text{and} \quad \left(q^{1/\ell}\right)^\sigma = \zeta_\ell \cdot q^{1/\ell}. \qquad \square$$

Theorem

- Let K be a number field.
- Let E/K be an elliptic curve with $j(E) \notin \mathcal{O}_K$.

- Then $\mathrm{End}(E) = \mathbb{Z}$.

Proof (Serre)

- Let $\psi \in \mathrm{End}(E)$. We want to prove that $\psi \in \mathbb{Z}$.
- Up to replacing K with a finite extension, we may assume that $\psi \in \mathrm{End}_K(E)$.
- Recall:

$$(X - \psi)(X - \widehat{\psi}) = X^2 - \tau X + \delta,$$

  where
  - $\delta = \psi\widehat{\psi} = \deg(\psi) \in \mathbb{Z}$ and
  - $\tau = \psi + \widehat{\psi} = 1 + \deg(\psi) - \deg(1 - \psi) \in \mathbb{Z}$.
- Key idea: we want $\tau = 2\psi$.

Proof (Serre)

- Pick a prime $\mathfrak{p}$ of $\mathcal{O}_K$ such that $v_{\mathfrak{p}}(j(E)) < 0$.
- Fix an embedding

$$\begin{array}{ccc} \overline{K} & \hookrightarrow & \overline{K}_{\mathfrak{p}} \\ | & & | \\ K & \hookrightarrow & K_{\mathfrak{p}} \end{array}$$

  and identify $G_{K_{\mathfrak{p}}}$ with the corresponding decomposition subgroup of G_K.

Proof (Serre)

- We write $E/K_{\mathfrak{p}}$ for the base change of E/K under $K \hookrightarrow K_{\mathfrak{p}}$ (abuse of notation).
- For every *large enough* prime number ℓ, the lemma yields $\sigma_\ell \in G_K$ such that, under $\rho_\ell \colon G_K \to \mathrm{End}(\mathrm{T}_\ell(E))$,

$$\rho_\ell(\sigma_\ell) \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mod \ell$$

  in terms of an appropriate basis (P_ℓ, Q_ℓ) of $\mathrm{T}_\ell(E)$.
- Note: $\sigma_\ell \in I_{K_{\mathfrak{p}}} \subseteq G_{K_{\mathfrak{p}}} \subset G_K$ and $E[\ell] \subset E(\overline{K}) \subset E(\overline{K}_{\mathfrak{p}})$.

Proof (Serre)

- Let ψ_ℓ be the image of ψ under $\mathrm{End}_K(E) \hookrightarrow \mathrm{End}_K(\mathrm{T}_\ell(E))$.
- In terms of the basis (P_ℓ, Q_ℓ),

$$\psi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{for some } a, b, c, d \in \mathbb{Z}_\ell.$$

- Recall: $\delta = \det(\psi_\ell)$ and $\tau = \mathrm{tr}(\psi_\ell)$.

Proof (Serre)

- As ψ_ℓ is defined over K, ψ_ℓ and $\rho_\ell(\sigma_\ell)$ commute:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mod \ell.$$

- A straight-forward calculation shows that
  - $c \equiv 0 \mod \ell$ and
  - $a \equiv d \mod \ell$.
- In particular, $\tau = a + d \equiv 2a \equiv 2d \mod \ell$.

Proof (Serre)

- Therefore,

$$\tau - 2\psi_\ell = \begin{pmatrix} \tau & 0 \\ 0 & \tau \end{pmatrix} - \begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix} \equiv \begin{pmatrix} 0 & -2b \\ 0 & 0 \end{pmatrix} \mod \ell$$

  and so

$$\deg(\tau - 2\psi) = \det(\tau - 2\psi_\ell) \equiv 0 \mod \ell.$$

- But this congruence holds for infinitely many primes ℓ, so

$$\deg(\tau - 2\psi) = 0.$$

Proof (Serre)

- All in all,

$$\psi = \frac{\tau}{2} \in \frac{1}{2}\mathbb{Z} \subset \mathbb{Q}.$$

- But $\mathrm{End}(E)$ is either $\mathbb{Z}$ or an order in a quadratic imaginary field (as $\mathrm{char}(K) = 0$).
- Thus, ψ must be integral over $\mathbb{Z}$.
- This can happen only if $\psi \in \mathbb{Z}$. $\square$

References

Silverman, J. H. (1994). *Advanced topics in the arithmetic of elliptic curves*. Graduate texts in mathematics 151. New York, NY, USA: Springer-Verlag. Chap. V.6, pp. 445–448.