Rational isogenies of prime degree

Philippe Michaud-Jacobs

University of Warwick

Triangle Groups, Belyi Uniformization, and Modularity

Bhaskaracharya Pratishthana, Pune, India

7th April 2022

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

For each p, such an elliptic curve does exist.

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

For each p, such an elliptic curve does exist.

Why is this an important theorem?

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

For each p, such an elliptic curve does exist.

Why is this an important theorem?

- Isogenies are important maps.

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

For each p, such an elliptic curve does exist.

Why is this an important theorem?

- Isogenies are important maps.
- It can be rephrased in terms of Galois representations.

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

For each p, such an elliptic curve does exist.

Why is this an important theorem?

- Isogenies are important maps.
- It can be rephrased in terms of Galois representations.
- It can be rephrased in terms of modular curves.

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

For each p, such an elliptic curve does exist.

Why is this an important theorem?

- Isogenies are important maps.
- It can be rephrased in terms of Galois representations.
- It can be rephrased in terms of modular curves.
- It is a crucial component in the modular method.

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

For each p, such an elliptic curve does exist.

Why is this an important theorem?

- Isogenies are important maps.
- It can be rephrased in terms of Galois representations.
- It can be rephrased in terms of modular curves.
- It is a crucial component in the modular method.
- Its proof introduced many important concepts.

Mazur's Theorem (1978)

Let $E/\mathbb{Q}$ be an elliptic curve. Let p be a prime such that E admits a rational p-isogeny. Then

$$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

For each p, such an elliptic curve does exist.

Why is this an important theorem?

- Isogenies are important maps.
- It can be rephrased in terms of Galois representations.
- It can be rephrased in terms of modular curves.
- It is a crucial component in the modular method.
- Its proof introduced many important concepts.

Aim: give an (accessible!) overview of the proof, following Mazur's paper: *Rational isogenies of prime degree*.

Isogenies

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$.

Isogenies

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$.

- An isogeny between elliptic curves is a non-constant morphism $\varphi : E_1 \to E_2$ that preserves the group structure.

Isogenies

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$.

- An isogeny between elliptic curves is a non-constant morphism $\varphi : E_1 \to E_2$ that preserves the group structure.
- The degree of an isogeny is the size of its kernel.

Isogenies

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$.

- An isogeny between elliptic curves is a non-constant morphism $\varphi : E_1 \to E_2$ that preserves the group structure.
- The degree of an isogeny is the size of its kernel. If φ has degree p, we say it is a p-isogeny.

Isogenies

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$.

- An isogeny between elliptic curves is a non-constant morphism $\varphi : E_1 \to E_2$ that preserves the group structure.
- The degree of an isogeny is the size of its kernel. If φ has degree p, we say it is a p-isogeny.
- An isogeny is rational if it can be expressed using rational functions with coefficients in $\mathbb{Q}$.

Isogenies

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$.

- An isogeny between elliptic curves is a non-constant morphism $\varphi : E_1 \to E_2$ that preserves the group structure.
- The degree of an isogeny is the size of its kernel. If φ has degree p, we say it is a p-isogeny.
- An isogeny is rational if it can be expressed using rational functions with coefficients in $\mathbb{Q}$.
  Equivalently, $\varphi^\sigma = \varphi$ for any $\sigma \in G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Isogenies

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$.

- An isogeny between elliptic curves is a non-constant morphism $\varphi : E_1 \to E_2$ that preserves the group structure.
- The degree of an isogeny is the size of its kernel. If φ has degree p, we say it is a p-isogeny.
- An isogeny is rational if it can be expressed using rational functions with coefficients in $\mathbb{Q}$.
  Equivalently, $\varphi^\sigma = \varphi$ for any $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Example.

$$E_1 : Y^2 = X^3 + aX^2 + bX, \quad E_2 : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X.$$

$$\varphi : (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right),$$

Isogenies

Let E_1, E_2 be elliptic curves over $\mathbb{Q}$.

- An isogeny between elliptic curves is a non-constant morphism $\varphi : E_1 \to E_2$ that preserves the group structure.
- The degree of an isogeny is the size of its kernel. If φ has degree p, we say it is a p-isogeny.
- An isogeny is rational if it can be expressed using rational functions with coefficients in $\mathbb{Q}$.
  Equivalently, $\varphi^\sigma = \varphi$ for any $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Example.

$$E_1 : Y^2 = X^3 + aX^2 + bX, \quad E_2 : Y^2 = X^3 - 2aX^2 + (a^2 - 4b)X.$$

$$\varphi : (x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right),$$

$\ker(\varphi) = \{0_{E_1}, (0,0)\}$, it is a rational 2-isogeny.

The mod p cyclotomic character

Let p be a prime and ζ_p a primitive p-th root of unity.

The mod p cyclotomic character

Let p be a prime and ζ_p a primitive p-th root of unity.

- For each $\sigma \in G_{\mathbb{Q}}$, we have

$$\zeta_p^{\sigma} = \zeta_p^{a_\sigma}$$

for some $a_\sigma \in \{1, \ldots, p-1\}$.

The mod p cyclotomic character

Let p be a prime and ζ_p a primitive p-th root of unity.

- For each $\sigma \in G_{\mathbb{Q}}$, we have

$$\zeta_p^{\sigma} = \zeta_p^{a_\sigma}$$

for some $a_\sigma \in \{1, \ldots, p-1\}$.

Define the mod p cyclotomic character

$$\begin{aligned} \chi_p : G_{\mathbb{Q}} &\to \mathbb{F}_p^{\times} \\ \sigma &\mapsto a_\sigma, \text{ where } \zeta_p^{\sigma} = \zeta_p^{a_\sigma}. \end{aligned}$$

The mod p cyclotomic character

Let p be a prime and ζ_p a primitive p-th root of unity.

- For each $\sigma \in G_{\mathbb{Q}}$, we have

$$\zeta_p^{\sigma} = \zeta_p^{a_\sigma}$$

for some $a_\sigma \in \{1, \ldots, p-1\}$.

Define the mod p cyclotomic character

$$\begin{aligned} \chi_p : G_{\mathbb{Q}} &\to \mathbb{F}_p^{\times} \\ \sigma &\mapsto a_\sigma, \text{ where } \zeta_p^{\sigma} = \zeta_p^{a_\sigma}. \end{aligned}$$

Let $q \neq p$ be a prime. Let σ_q denote a Frobenius element at q.

The mod p cyclotomic character

Let p be a prime and ζ_p a primitive p-th root of unity.

- For each $\sigma \in G_{\mathbb{Q}}$, we have

$$\zeta_p^{\sigma} = \zeta_p^{a_\sigma}$$

for some $a_\sigma \in \{1, \ldots, p-1\}$.

Define the mod p cyclotomic character

$$\begin{aligned} \chi_p : G_{\mathbb{Q}} &\to \mathbb{F}_p^{\times} \\ \sigma &\mapsto a_\sigma, \text{ where } \zeta_p^{\sigma} = \zeta_p^{a_\sigma}. \end{aligned}$$

Let $q \neq p$ be a prime. Let σ_q denote a Frobenius element at q. Then $\zeta_p^{\sigma_q} = \zeta_p^{q}$, so

$$\chi_p(\sigma_q) = q \pmod{p}.$$

The mod p Galois representation

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime.

The mod p Galois representation

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime.
The Galois group $G_{\mathbb{Q}}$ acts on $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

The mod p Galois representation

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime.
The Galois group $G_{\mathbb{Q}}$ acts on $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and gives rise to the mod p Galois representation of E:

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

The mod p Galois representation

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime.
The Galois group $G_{\mathbb{Q}}$ acts on $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and gives rise to the mod p Galois representation of E:

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

Fix a basis (R_1, R_2) of $E[p]$.

The mod p Galois representation

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime.
The Galois group $G_{\mathbb{Q}}$ acts on $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and gives rise to the mod p Galois representation of E:

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

Fix a basis (R_1, R_2) of $E[p]$. For $\sigma \in G_{\mathbb{Q}}$,

$$R_1^{\sigma} = aR_1 + bR_2$$
$$R_2^{\sigma} = cR_1 + dR_2.$$

The mod p Galois representation

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime.
The Galois group $G_{\mathbb{Q}}$ acts on $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and gives rise to the mod p Galois representation of E:

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

Fix a basis (R_1, R_2) of $E[p]$. For $\sigma \in G_{\mathbb{Q}}$,

$$R_1^{\sigma} = aR_1 + bR_2$$
$$R_2^{\sigma} = cR_1 + dR_2.$$

Then $\overline{\rho}_{E,p}(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

The mod p Galois representation

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime.
The Galois group $G_{\mathbb{Q}}$ acts on $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ and gives rise to the mod p Galois representation of E:

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

Fix a basis (R_1, R_2) of $E[p]$. For $\sigma \in G_{\mathbb{Q}}$,

$$R_1^{\sigma} = aR_1 + bR_2$$
$$R_2^{\sigma} = cR_1 + dR_2.$$

Then $\overline{\rho}_{E,p}(\sigma) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

- $\det(\overline{\rho}_{E,p}) = \chi_p$.

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$.

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.
- The cusps are rational points: $\infty, 0 \in X_0(p)(\mathbb{Q})$.

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.
- The cusps are rational points: $\infty, 0 \in X_0(p)(\mathbb{Q})$.
- The j-map: $j : X_0(p) \to \mathbb{P}^1$. The poles of j are the cusps.

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.
- The cusps are rational points: $\infty, 0 \in X_0(p)(\mathbb{Q})$.
- The j-map: $j : X_0(p) \to \mathbb{P}^1$. The poles of j are the cusps.
- The Atkin–Lehner involution $w_p : X_0(p) \to X_0(p)$ swaps the cusps.

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.
- The cusps are rational points: $\infty, 0 \in X_0(p)(\mathbb{Q})$.
- The j-map: $j : X_0(p) \to \mathbb{P}^1$. The poles of j are the cusps.
- The Atkin–Lehner involution $w_p : X_0(p) \to X_0(p)$ swaps the cusps.
- $X_0(p)$ parametrises elliptic curves with p-isogenies:

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.
- The cusps are rational points: $\infty, 0 \in X_0(p)(\mathbb{Q})$.
- The j-map: $j : X_0(p) \to \mathbb{P}^1$. The poles of j are the cusps.
- The Atkin–Lehner involution $w_p : X_0(p) \to X_0(p)$ swaps the cusps.
- $X_0(p)$ parametrises elliptic curves with p-isogenies:

if $E/\mathbb{Q}$ is an elliptic curve with a rational p-isogeny, φ, then

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.
- The cusps are rational points: $\infty, 0 \in X_0(p)(\mathbb{Q})$.
- The j-map: $j : X_0(p) \to \mathbb{P}^1$. The poles of j are the cusps.
- The Atkin–Lehner involution $w_p : X_0(p) \to X_0(p)$ swaps the cusps.
- $X_0(p)$ parametrises elliptic curves with p-isogenies:

if $E/\mathbb{Q}$ is an elliptic curve with a rational p-isogeny, φ, then

$$(E, \varphi) \rightsquigarrow [(E, \varphi)] = x \in X_0(p)(\mathbb{Q}).$$

The modular curve $X_0(p)$

- As a Riemann surface, $Y_0(p) = \Gamma_0(p)\backslash\mathbb{H}$. By adding the cusps ∞, 0 we make it into a *compact* Riemann surface $X_0(p)$.
- $X_0(p)$ is an algebraic curve defined over $\mathbb{Q}$ and has good reduction at primes $q \neq p$.
- The cusps are rational points: $\infty, 0 \in X_0(p)(\mathbb{Q})$.
- The j-map: $j : X_0(p) \to \mathbb{P}^1$. The poles of j are the cusps.
- The Atkin–Lehner involution $w_p : X_0(p) \to X_0(p)$ swaps the cusps.
- $X_0(p)$ parametrises elliptic curves with p-isogenies:

if $E/\mathbb{Q}$ is an elliptic curve with a rational p-isogeny, φ, then

$$(E, \varphi) \rightsquigarrow [(E, \varphi)] = x \in X_0(p)(\mathbb{Q}).$$

Moreover, $j(x) = j(E)$.

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a rational p-isogeny, φ.

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a rational p-isogeny, φ.
- (ii) E has a rational subgroup of order p, $V_p = \langle R \rangle$.

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a rational p-isogeny, φ.
- (ii) E has a rational subgroup of order p, $V_p = \langle R \rangle$.
- (iii) $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is reducible, $\overline{\rho}_{E,p} \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix}\right)$.

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a rational p-isogeny, φ.
- (ii) E has a rational subgroup of order p, $V_p = \langle R \rangle$.
- (iii) $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is reducible, $\overline{\rho}_{E,p} \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix}\right)$.

(i) $\Longrightarrow$ (ii). Take $\ker(\varphi)$.

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a rational p-isogeny, φ.
- (ii) E has a rational subgroup of order p, $V_p = \langle R \rangle$.
- (iii) $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is reducible, $\overline{\rho}_{E,p} \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix}\right)$.

(i) $\Longrightarrow$ (ii). Take $\ker(\varphi)$.

(ii) $\Longrightarrow$ (i). Quotient by V_p.

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a rational p-isogeny, φ.
- (ii) E has a rational subgroup of order p, $V_p = \langle R \rangle$.
- (iii) $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is reducible, $\overline{\rho}_{E,p} \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix}\right)$.

(i) $\Longrightarrow$ (ii). Take $\ker(\varphi)$.

(ii) $\Longrightarrow$ (i). Quotient by V_p.

(ii) $\Longrightarrow$ (iii). V_p is a non-trivial proper $G_{\mathbb{Q}}$-submodule of $E[p]$.

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a rational p-isogeny, φ.
- (ii) E has a rational subgroup of order p, $V_p = \langle R \rangle$.
- (iii) $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is reducible, $\overline{\rho}_{E,p} \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix}\right)$.

(i) $\implies$ (ii). Take $\ker(\varphi)$.

(ii) $\implies$ (i). Quotient by V_p.

(ii) $\implies$ (iii). V_p is a non-trivial proper $G_{\mathbb{Q}}$-submodule of $E[p]$.

(iii) $\implies$ (ii). With the right choice of basis (R_1, R_2) of $E[p]$,

$$R_1^{\sigma} = \lambda(\sigma) R_1 \in \langle R_1 \rangle.$$

Equivalent formulations

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime. The following are equivalent:

- (i) E admits a rational p-isogeny, φ.
- (ii) E has a rational subgroup of order p, $V_p = \langle R \rangle$.
- (iii) $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is reducible, $\overline{\rho}_{E,p} \sim \left(\begin{smallmatrix} \lambda & * \\ 0 & \lambda' \end{smallmatrix}\right)$.

(i) $\implies$ (ii). Take $\ker(\varphi)$.

(ii) $\implies$ (i). Quotient by V_p.

(ii) $\implies$ (iii). V_p is a non-trivial proper $G_{\mathbb{Q}}$-submodule of $E[p]$.

(iii) $\implies$ (ii). With the right choice of basis (R_1, R_2) of $E[p]$,

$$R_1^{\sigma} = \lambda(\sigma) R_1 \in \langle R_1 \rangle.$$

So $\langle R_1 \rangle$ is a rational subgroup of order p.

Overview of the proof

Suppose (from now on) that $E/\mathbb{Q}$ has a rational p-isogeny and $p \geq 23$. We want to show $p \in \{37, 43, 67, 163\}$.

Overview of the proof

Suppose (from now on) that $E/\mathbb{Q}$ has a rational p-isogeny and $p \geq 23$. We want to show $p \in \{37, 43, 67, 163\}$.

Let $q \neq 2, p$ be a prime.

Overview of the proof

Suppose (from now on) that $E/\mathbb{Q}$ has a rational p-isogeny and $p \geq 23$. We want to show $p \in \{37, 43, 67, 163\}$.

Let $q \neq 2, p$ be a prime.

- Suppose E has potentially multiplicative reduction at q (meaning $v_q(j(E)) < 0$).

Overview of the proof

Suppose (from now on) that $E/\mathbb{Q}$ has a rational p-isogeny and $p \geq 23$. We want to show $p \in \{37, 43, 67, 163\}$.

Let $q \neq 2, p$ be a prime.

- Suppose E has potentially multiplicative reduction at q (meaning $v_q(j(E)) < 0$).

  We will construct the *Eisenstein quotient*, a rank 0 quotient of the Jacobian of $X_0(p)$, and use the theory of formal immersions to obtain a contradiction.

Overview of the proof

Suppose (from now on) that $E/\mathbb{Q}$ has a rational p-isogeny and $p \geq 23$. We want to show $p \in \{37, 43, 67, 163\}$.

Let $q \neq 2, p$ be a prime.

- Suppose E has potentially multiplicative reduction at q (meaning $v_q(j(E)) < 0$).

  We will construct the *Eisenstein quotient*, a rank 0 quotient of the Jacobian of $X_0(p)$, and use the theory of formal immersions to obtain a contradiction.
- So E has potentially good reduction at all $q \neq 2, p$ (meaning $v_q(j(E)) \geq 0$).

Overview of the proof

Suppose (from now on) that $E/\mathbb{Q}$ has a rational p-isogeny and $p \geq 23$. We want to show $p \in \{37, 43, 67, 163\}$.

Let $q \neq 2, p$ be a prime.

- Suppose E has potentially multiplicative reduction at q (meaning $v_q(j(E)) < 0$).

  We will construct the *Eisenstein quotient*, a rank 0 quotient of the Jacobian of $X_0(p)$, and use the theory of formal immersions to obtain a contradiction.

- So E has potentially good reduction at all $q \neq 2, p$ (meaning $v_q(j(E)) \geq 0$).

  We will study the mod p Galois representation of E and the *isogeny character* to prove that $p = 37$ or that $\mathbb{Q}(\sqrt{-p})$ has class number 1 (so $p = 43, 67$, or 163).

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.
Suppose $q \neq 2, p$ is a prime of potentially multiplicative reduction for E.

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.
Suppose $q \neq 2, p$ is a prime of potentially multiplicative reduction for E.

- $(E, \varphi) \rightsquigarrow x \in X_0(p)(\mathbb{Q}) \backslash \{0, \infty\}$.

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.
Suppose $q \neq 2, p$ is a prime of potentially multiplicative reduction for E.

- $(E, \varphi) \rightsquigarrow x \in X_0(p)(\mathbb{Q}) \backslash \{0, \infty\}$.
- We have $v_q(j(x)) = v_q(j(E)) < 0$.

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.
Suppose $q \neq 2, p$ is a prime of potentially multiplicative reduction for E.

- $(E, \varphi) \rightsquigarrow x \in X_0(p)(\mathbb{Q}) \backslash \{0, \infty\}$.
- We have $v_q(j(x)) = v_q(j(E)) < 0$.
- So $\tilde{x} = \tilde{0}$ or $\tilde{\infty} \in X_0(p)(\mathbb{F}_q)$.

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.
Suppose $q \neq 2, p$ is a prime of potentially multiplicative reduction for E.

- $(E, \varphi) \rightsquigarrow x \in X_0(p)(\mathbb{Q}) \backslash \{0, \infty\}$.
- We have $v_q(j(x)) = v_q(j(E)) < 0$.
- So $\tilde{x} = \tilde{0}$ or $\tilde{\infty} \in X_0(p)(\mathbb{F}_q)$.
- By replacing x by $w_p(x)$ if necessary, we may assume that $\tilde{x} = \tilde{\infty} \pmod{q}$.

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.
Suppose $q \neq 2, p$ is a prime of potentially multiplicative reduction for E.

- $(E, \varphi) \rightsquigarrow x \in X_0(p)(\mathbb{Q}) \backslash \{0, \infty\}$.
- We have $v_q(j(x)) = v_q(j(E)) < 0$.
- So $\tilde{x} = \tilde{0}$ or $\tilde{\infty} \in X_0(p)(\mathbb{F}_q)$.
- By replacing x by $w_p(x)$ if necessary, we may assume that $\tilde{x} = \tilde{\infty} \pmod{q}$.

  We will now **forget about** E and just focus on x.

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.
Suppose $q \neq 2, p$ is a prime of potentially multiplicative reduction for E.

- $(E, \varphi) \rightsquigarrow x \in X_0(p)(\mathbb{Q}) \backslash \{0, \infty\}$.
- We have $v_q(j(x)) = v_q(j(E)) < 0$.
- So $\tilde{x} = \tilde{0}$ or $\tilde{\infty} \in X_0(p)(\mathbb{F}_q)$.
- By replacing x by $w_p(x)$ if necessary, we may assume that $\tilde{x} = \tilde{\infty} \pmod{q}$.

  We will now **forget about** E and just focus on x.
- So $\tilde{x} = \tilde{\infty} \pmod{q}$.

A prime of potentially multiplicative reduction

$E/\mathbb{Q}$ has a rational p-isogeny, φ, and $p \geq 23$.
Suppose $q \neq 2, p$ is a prime of potentially multiplicative reduction for E.

- $(E, \varphi) \rightsquigarrow x \in X_0(p)(\mathbb{Q}) \backslash \{0, \infty\}$.
- We have $v_q(j(x)) = v_q(j(E)) < 0$.
- So $\tilde{x} = \tilde{0}$ or $\tilde{\infty} \in X_0(p)(\mathbb{F}_q)$.
- By replacing x by $w_p(x)$ if necessary, we may assume that $\tilde{x} = \tilde{\infty} \pmod{q}$.

  We will now **forget about** E and just focus on x.
- So $\tilde{x} = \tilde{\infty} \pmod{q}$.

Our aim is to show that $x = \infty$, which would be a contradiction.

The Jacobian $J_0(p)$

Write $J_0(p)$ for the Jacobian of $X_0(p)$.

The Jacobian $J_0(p)$

Write $J_0(p)$ for the Jacobian of $X_0(p)$.
We have the Abel–Jacobi map with basepoint ∞:

$$\begin{aligned} \iota : X_0(p)(\mathbb{Q}) &\hookrightarrow J_0(p)(\mathbb{Q}) \\ y &\mapsto [y - \infty] \end{aligned}$$

The Jacobian $J_0(p)$

Write $J_0(p)$ for the Jacobian of $X_0(p)$.
We have the Abel–Jacobi map with basepoint ∞:

$$\begin{aligned} \iota : X_0(p)(\mathbb{Q}) &\hookrightarrow J_0(p)(\mathbb{Q}) \\ y &\mapsto [y - \infty] \end{aligned}$$

So

$$\begin{aligned} X_0(p)(\mathbb{Q}) \hookrightarrow J_0(p)(\mathbb{Q}) &\to J_0(p)(\mathbb{F}_q) \\ x \mapsto [x - \infty] \quad &\mapsto [\tilde{x} - \tilde{\infty}] = [0] \end{aligned}$$

The Jacobian $J_0(p)$

Write $J_0(p)$ for the Jacobian of $X_0(p)$.
We have the Abel–Jacobi map with basepoint ∞:

$$\begin{aligned} \iota : X_0(p)(\mathbb{Q}) &\hookrightarrow J_0(p)(\mathbb{Q}) \\ y &\mapsto [y - \infty] \end{aligned}$$

So

$$\begin{aligned} X_0(p)(\mathbb{Q}) \hookrightarrow J_0(p)(\mathbb{Q}) &\to J_0(p)(\mathbb{F}_q) \\ x \mapsto [x - \infty] \quad &\mapsto [\tilde{x} - \tilde{\infty}] = [0] \end{aligned}$$

An optimal quotient of $J_0(p)$ is an abelian variety A such that the kernel of the quotient map $J_0(p) \to A$ is an abelian variety.

A rank 0 quotient

Key Result

Let A be any non-trivial optimal quotient of $J_0(p)$.

A rank 0 quotient

Key Result

Let A be any non-trivial optimal quotient of $J_0(p)$. Then

$$\theta : X_0(p) \to J_0(p) \to A$$

A rank 0 quotient

Key Result

Let A be any non-trivial optimal quotient of $J_0(p)$. Then

$$\theta : X_0(p) \to J_0(p) \to A$$

is a formal immersion at ∞ (over $\mathbb{Q}$ and mod q).

A rank 0 quotient

Key Result

Let A be any non-trivial optimal quotient of $J_0(p)$. Then

$$\theta : X_0(p) \to J_0(p) \to A$$

is a formal immersion at ∞ (over $\mathbb{Q}$ and mod q).

Consequence. If $\theta(x) - \theta(\infty) = 0 \in A(\mathbb{Q})$ then $x = \infty$.

A rank 0 quotient

Key Result

Let A be any non-trivial optimal quotient of $J_0(p)$. Then

$$\theta : X_0(p) \to J_0(p) \to A$$

is a formal immersion at ∞ (over $\mathbb{Q}$ and mod q).

Consequence. If $\theta(x) - \theta(\infty) = 0 \in A(\mathbb{Q})$ then $x = \infty$.

We only know that $\mathrm{red}\,(\theta(x) - \theta(\infty)) = \tilde{0} \in A(\mathbb{F}_q)$.

A rank 0 quotient

Key Result

Let A be any non-trivial optimal quotient of $J_0(p)$. Then

$$\theta : X_0(p) \to J_0(p) \to A$$

is a formal immersion at ∞ (over $\mathbb{Q}$ and mod q).

Consequence. If $\theta(x) - \theta(\infty) = 0 \in A(\mathbb{Q})$ then $x = \infty$.

We only know that $\mathrm{red}\,(\theta(x) - \theta(\infty)) = \tilde{0} \in A(\mathbb{F}_q)$.
But if $A(\mathbb{Q})$ has rank 0, then by injectivity of torsion,
$\theta(x) - \theta(\infty) = 0 \in A(\mathbb{Q})$.

A rank 0 quotient

Key Result

Let A be any non-trivial optimal quotient of $J_0(p)$. Then

$$\theta : X_0(p) \to J_0(p) \to A$$

is a formal immersion at ∞ (over $\mathbb{Q}$ and mod q).

Consequence. If $\theta(x) - \theta(\infty) = 0 \in A(\mathbb{Q})$ then $x = \infty$.

We only know that $\mathrm{red}\,(\theta(x) - \theta(\infty)) = \tilde{0} \in A(\mathbb{F}_q)$.
But if $A(\mathbb{Q})$ has rank 0, then by injectivity of torsion,
$\theta(x) - \theta(\infty) = 0 \in A(\mathbb{Q})$. So $x = \infty$.

A rank 0 quotient

Key Result

Let A be any non-trivial optimal quotient of $J_0(p)$. Then

$$\theta : X_0(p) \to J_0(p) \to A$$

is a formal immersion at ∞ (over $\mathbb{Q}$ and mod q).

Consequence. If $\theta(x) - \theta(\infty) = 0 \in A(\mathbb{Q})$ then $x = \infty$.

We only know that $\mathrm{red}\,(\theta(x) - \theta(\infty)) = \tilde{0} \in A(\mathbb{F}_q)$.
But if $A(\mathbb{Q})$ has rank 0, then by injectivity of torsion,
$\theta(x) - \theta(\infty) = 0 \in A(\mathbb{Q})$. So $x = \infty$.

So we want to find a non-trivial optimal quotient of $J_0(p)$ that has rank 0.

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

It means that the pullback map

$$\theta^* : \hat{\mathcal{O}}_{A,\theta(\infty)} \longrightarrow \hat{\mathcal{O}}_{X_0(p),\infty}$$

is surjective.

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

It means that the pullback map

$$\theta^* : \hat{\mathcal{O}}_{A,\theta(\infty)} \longrightarrow \hat{\mathcal{O}}_{X_0(p),\infty}$$

is surjective. *But what does this mean?*

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

It means that the pullback map

$$\theta^* : \hat{\mathcal{O}}_{A,\theta(\infty)} \longrightarrow \hat{\mathcal{O}}_{X_0(p),\infty}$$

is surjective. *But what does this mean?*

- $\mathcal{O}_{X_0(p),\infty}$ is the local ring of ratios of functions f/g with $g(\infty) \neq 0$.

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

It means that the pullback map

$$\theta^* : \hat{\mathcal{O}}_{A,\theta(\infty)} \longrightarrow \hat{\mathcal{O}}_{X_0(p),\infty}$$

is surjective. *But what does this mean?*

- $\mathcal{O}_{X_0(p),\infty}$ is the local ring of ratios of functions f/g with $g(\infty) \neq 0$.
- If π is a uniformiser (π vanishes once at ∞) then we can think of $\hat{\mathcal{O}}_{X_0(p),\infty}$ as power series in π: say $a_0 + a_1\pi + a_2\pi^2 + \ldots$.

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

It means that the pullback map

$$\theta^* : \hat{\mathcal{O}}_{A,\theta(\infty)} \longrightarrow \hat{\mathcal{O}}_{X_0(p),\infty}$$

is surjective. *But what does this mean?*

- $\mathcal{O}_{X_0(p),\infty}$ is the local ring of ratios of functions f/g with $g(\infty) \neq 0$.
- If π is a uniformiser (π vanishes once at ∞) then we can think of $\hat{\mathcal{O}}_{X_0(p),\infty}$ as power series in π: say $a_0 + a_1\pi + a_2\pi^2 + \ldots$.
- Let u be a uniformiser at $\theta(\infty)$.

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

It means that the pullback map

$$\theta^* : \hat{\mathcal{O}}_{A,\theta(\infty)} \longrightarrow \hat{\mathcal{O}}_{X_0(p),\infty}$$

is surjective. *But what does this mean?*

- $\mathcal{O}_{X_0(p),\infty}$ is the local ring of ratios of functions f/g with $g(\infty) \neq 0$.
- If π is a uniformiser (π vanishes once at ∞) then we can think of $\hat{\mathcal{O}}_{X_0(p),\infty}$ as power series in π: say $a_0 + a_1\pi + a_2\pi^2 + \dots$.
- Let u be a uniformiser at $\theta(\infty)$. Then

$$(\theta^*(u))(\infty) = u(\theta(\infty)) = 0.$$

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

It means that the pullback map

$$\theta^* : \hat{\mathcal{O}}_{A,\theta(\infty)} \longrightarrow \hat{\mathcal{O}}_{X_0(p),\infty}$$

is surjective. *But what does this mean?*

- $\mathcal{O}_{X_0(p),\infty}$ is the local ring of ratios of functions f/g with $g(\infty) \neq 0$.
- If π is a uniformiser (π vanishes once at ∞) then we can think of $\hat{\mathcal{O}}_{X_0(p),\infty}$ as power series in π: say $a_0 + a_1\pi + a_2\pi^2 + \dots$.
- Let u be a uniformiser at $\theta(\infty)$. Then

$$(\theta^*(u))(\infty) = u(\theta(\infty)) = 0.$$

So $\theta^*(u) = a_1\pi + a_2\pi^2 + \dots$.

Defining formal immersions

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 1

What does it mean to be a formal immersion at ∞?

It means that the pullback map

$$\theta^* : \hat{\mathcal{O}}_{A,\theta(\infty)} \longrightarrow \hat{\mathcal{O}}_{X_0(p),\infty}$$

is surjective. *But what does this mean?*

- $\mathcal{O}_{X_0(p),\infty}$ is the local ring of ratios of functions f/g with $g(\infty) \neq 0$.
- If π is a uniformiser (π vanishes once at ∞) then we can think of $\hat{\mathcal{O}}_{X_0(p),\infty}$ as power series in π: say $a_0 + a_1\pi + a_2\pi^2 + \ldots$.
- Let u be a uniformiser at $\theta(\infty)$. Then

$$(\theta^*(u))(\infty) = u(\theta(\infty)) = 0.$$

So $\theta^*(u) = a_1\pi + a_2\pi^2 + \ldots$. We need $a_1 \neq 0$ for θ^* to be surjective.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞,

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞, then $\theta^*(u) = a_1\pi + a_2\pi^2 + \ldots$. We need $a_1 \neq 0$.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞, then $\theta^*(u) = a_1\pi + a_2\pi^2 + \ldots$. We need $a_1 \neq 0$.
- Write $\underline{q} = e^{2\pi i\tau}$.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞, then $\theta^*(u) = a_1\pi + a_2\pi^2 + \ldots$. We need $a_1 \neq 0$.
- Write $q = e^{2\pi i\tau}$. The q-expansion principle says that we can identify π with q.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞, then $\theta^*(u) = a_1\pi + a_2\pi^2 + \ldots$. We need $a_1 \neq 0$.
- Write $\underline{q} = e^{2\pi i\tau}$. The $\underline{q}$-expansion principle says that we can identify π with $\underline{q}$.
- So $\theta^*(u) = a_1\underline{q} + a_2\underline{q}^2 + \ldots$.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞, then $\theta^*(u) = a_1\pi + a_2\pi^2 + \dots$. We need $a_1 \neq 0$.
- Write $\underline{q} = e^{2\pi i\tau}$. The $\underline{q}$-expansion principle says that we can identify π with $\underline{q}$.
- So $\theta^*(u) = a_1\underline{q} + a_2\underline{q}^2 + \dots$. We still need $a_1 \neq 0$.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞, then $\theta^*(u) = a_1\pi + a_2\pi^2 + \ldots$. We need $a_1 \neq 0$.
- Write $\underline{q} = e^{2\pi i\tau}$. The $\underline{q}$-expansion principle says that we can identify π with $\underline{q}$.
- So $\theta^*(u) = a_1\underline{q} + a_2\underline{q}^2 + \ldots$. We still need $a_1 \neq 0$.
- This looks like the Fourier expansion of a cuspform $f \in S_2(\Gamma_0(p))$.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞, then $\theta^*(u) = a_1\pi + a_2\pi^2 + \ldots$. We need $a_1 \neq 0$.
- Write $\underline{q} = e^{2\pi i\tau}$. The $\underline{q}$-expansion principle says that we can identify π with $\underline{q}$.
- So $\theta^*(u) = a_1\underline{q} + a_2\underline{q}^2 + \ldots$. We still need $a_1 \neq 0$.
- This looks like the Fourier expansion of a cuspform $f \in S_2(\Gamma_0(p))$. We have $f = a_1\underline{q} + a_2\underline{q}^2 + \ldots$ with $a_1 \neq 0$.

Relation to newforms

We have $\theta : X_0(p) \to A$ is a formal immersion at ∞.

Question 2

Why is θ a formal immersion at ∞?

- If u is a uniformiser at $\theta(\infty)$ and π is a uniformiser at ∞, then $\theta^*(u) = a_1\pi + a_2\pi^2 + \ldots$. We need $a_1 \neq 0$.
- Write $\underline{q} = e^{2\pi i\tau}$. The $\underline{q}$-expansion principle says that we can identify π with $\underline{q}$.
- So $\theta^*(u) = a_1\underline{q} + a_2\underline{q}^2 + \ldots$. We still need $a_1 \neq 0$.
- This looks like the Fourier expansion of a cuspform $f \in S_2(\Gamma_0(p))$. We have $f = a_1\underline{q} + a_2\underline{q}^2 + \ldots$ with $a_1 \neq 0$.
- Since A is an optimal quotient of $J_0(p)$, there is a cuspform f attached to A, and we can use this to prove that $a_1 \neq 0$.

The Eisenstein quotient

We construct a non-trivial, rank 0, optimal quotient of $J_0(p)$.

The Eisenstein quotient

We construct a non-trivial, rank 0, optimal quotient of $J_0(p)$.

- For each prime $\ell \neq p$ we have a Hecke operator T_ℓ acting on $J_0(p)$.

The Eisenstein quotient

We construct a non-trivial, rank 0, optimal quotient of $J_0(p)$.

- For each prime $\ell \neq p$ we have a Hecke operator T_ℓ acting on $J_0(p)$.
- The Hecke algebra is the $\mathbb{Z}$-algebra generated by all the Hecke operators T_ℓ **and** the Atkin–Lehner involution w_p.

The Eisenstein quotient

We construct a non-trivial, rank 0, optimal quotient of $J_0(p)$.

- For each prime $\ell \neq p$ we have a Hecke operator T_ℓ acting on $J_0(p)$.
- The Hecke algebra is the $\mathbb{Z}$-algebra generated by all the Hecke operators T_ℓ **and** the Atkin–Lehner involution w_p.
- We define the Eisenstein ideal to be

$$\mathbb{I} = \langle w_p + 1, T_\ell - \ell - 1 \ : \ \ell \neq p \rangle.$$

The Eisenstein quotient

We construct a non-trivial, rank 0, optimal quotient of $J_0(p)$.

- For each prime $\ell \neq p$ we have a Hecke operator T_ℓ acting on $J_0(p)$.
- The Hecke algebra is the $\mathbb{Z}$-algebra generated by all the Hecke operators T_ℓ **and** the Atkin–Lehner involution w_p.
- We define the Eisenstein ideal to be

$$\mathbb{I} = \langle w_p + 1, T_\ell - \ell - 1 \ : \ \ell \neq p \rangle.$$

The Eisenstein quotient

We define the Eisenstein quotient to be

$$J_e(p) = \frac{J_0(p)}{\left(\bigcap_{k\geq 1} \mathbb{I}^k\right) J_0(p)}.$$

The Eisenstein quotient

We construct a non-trivial, rank 0, optimal quotient of $J_0(p)$.

- For each prime $\ell \neq p$ we have a Hecke operator T_ℓ acting on $J_0(p)$.
- The Hecke algebra is the $\mathbb{Z}$-algebra generated by all the Hecke operators T_ℓ **and** the Atkin–Lehner involution w_p.
- We define the Eisenstein ideal to be

$$\mathbb{I} = \langle w_p + 1, T_\ell - \ell - 1 \ : \ \ell \neq p \rangle.$$

The Eisenstein quotient

We define the Eisenstein quotient to be

$$J_e(p) = \frac{J_0(p)}{\left(\bigcap_{k\geq 1} \mathbb{I}^k\right) J_0(p)}.$$

We have $J_e(p)(\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}$, where n is the numerator of $(p-1)/12$.

We're halfway there!

The isogeny character

Know. All primes $q \neq 2, p$ are of potentially good reduction for E.

The isogeny character

Know. All primes $q \neq 2, p$ are of potentially good reduction for E.

Recall, $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is **reducible**,

The isogeny character

Know. All primes $q \neq 2, p$ are of potentially good reduction for E.

Recall, $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is **reducible**, so

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix},$$

The isogeny character

Know. All primes $q \neq 2, p$ are of potentially good reduction for E.

Recall, $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is **reducible**, so

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix},$$

and $\lambda' = \chi_p/\lambda$ since $\det(\overline{\rho}_{E,p}) = \chi_p$.

The isogeny character

Know. All primes $q \neq 2, p$ are of potentially good reduction for E.

Recall, $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is **reducible**, so

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix},$$

and $\lambda' = \chi_p/\lambda$ since $\det(\overline{\rho}_{E,p}) = \chi_p$.

The isogeny character

The character $\lambda : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ is called the isogeny character of (E, φ).

The isogeny character

Know. All primes $q \neq 2, p$ are of potentially good reduction for E.

Recall, $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is **reducible**, so

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix},$$

and $\lambda' = \chi_p/\lambda$ since $\det(\overline{\rho}_{E,p}) = \chi_p$.

The isogeny character

The character $\lambda : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ is called the isogeny character of (E, φ).

- λ tells us how $G_{\mathbb{Q}}$ acts on $V_p = \ker(\varphi)$:

The isogeny character

Know. All primes $q \neq 2, p$ are of potentially good reduction for E.

Recall, $\overline{\rho}_{E,p} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is **reducible**, so

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix},$$

and $\lambda' = \chi_p/\lambda$ since $\det(\overline{\rho}_{E,p}) = \chi_p$.

The isogeny character

The character $\lambda : G_{\mathbb{Q}} \to \mathbb{F}_p^{\times}$ is called the isogeny character of (E, φ).

- λ tells us how $G_{\mathbb{Q}}$ acts on $V_p = \ker(\varphi)$: if $V_p = \langle R \rangle$, then for $\sigma \in G_{\mathbb{Q}}$,

$$R^{\sigma} = \lambda(\sigma) R.$$

Relating λ^{12} to χ_p

Fact

$\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$.

Relating λ^{12} to χ_p

Fact

$\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Relating λ^{12} to χ_p

Fact

$\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$. We call s the isogeny signature.

Relating λ^{12} to χ_p

Fact

$\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$. We call s the isogeny signature.

Why?

Relating λ^{12} to χ_p

Fact

$\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$. We call s the isogeny signature.

Why?

- View $E/\mathbb{Q}_q$.

Relating λ^{12} to χ_p

Fact

$\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$. We call s the isogeny signature.

Why?

- View $E/\mathbb{Q}_q$.
- E attains a good reduction at a totally ramified extension $K_q/\mathbb{Q}_q$ of degree dividing 12.

Relating λ^{12} to χ_p

Fact

$\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$. We call s the isogeny signature.

Why?

- View $E/\mathbb{Q}_q$.
- E attains a good reduction at a totally ramified extension $K_q/\mathbb{Q}_q$ of degree dividing 12.
- The fact comes from a careful study of how I_q' acts on $E[p]$, where I_q' is the inertia group of K_q.

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Why is this fact useful?

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Why is this fact useful?

Let $\sigma_q \in G_{\mathbb{Q}}$ be a Frobenius element at q.

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Why is this fact useful?

Let $\sigma_q \in G_{\mathbb{Q}}$ be a Frobenius element at q.

- $\lambda(\sigma_q)^{12} = \chi_p(\sigma_q)^s = q^s \pmod p$.

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Why is this fact useful?

Let $\sigma_q \in G_{\mathbb{Q}}$ be a Frobenius element at q.

- $\lambda(\sigma_q)^{12} = \chi_p(\sigma_q)^s = q^s \pmod p$.

So $\lambda(\sigma_q)$ is a root, mod p, of the polynomial $X^{12} - q^s$.

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Why is this fact useful?

Let $\sigma_q \in G_{\mathbb{Q}}$ be a Frobenius element at q.

- $\lambda(\sigma_q)^{12} = \chi_p(\sigma_q)^s = q^s \pmod p$.

  So $\lambda(\sigma_q)$ is a root, mod p, of the polynomial $X^{12} - q^s$.
- $\overline{\rho}_{E,p}(\sigma_q) = \begin{pmatrix} \lambda(\sigma_q) & * \\ 0 & \lambda'(\sigma_q) \end{pmatrix}$.

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Why is this fact useful?

Let $\sigma_q \in G_{\mathbb{Q}}$ be a Frobenius element at q.

- $\lambda(\sigma_q)^{12} = \chi_p(\sigma_q)^s = q^s \pmod p$.

  So $\lambda(\sigma_q)$ is a root, mod p, of the polynomial $X^{12} - q^s$.
- $\overline{\rho}_{E,p}(\sigma_q) = \begin{pmatrix} \lambda(\sigma_q) & * \\ 0 & \lambda'(\sigma_q) \end{pmatrix}$. So $\lambda(\sigma_q)$ is a root, mod p, of the characteristic polynomial of $\overline{\rho}_{E,p}(\sigma_q)$.

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Why is this fact useful?

Let $\sigma_q \in G_{\mathbb{Q}}$ be a Frobenius element at q.

- $\lambda(\sigma_q)^{12} = \chi_p(\sigma_q)^s = q^s \pmod p$.

  So $\lambda(\sigma_q)$ is a root, mod p, of the polynomial $X^{12} - q^s$.
- $\overline{\rho}_{E,p}(\sigma_q) = \begin{pmatrix} \lambda(\sigma_q) & * \\ 0 & \lambda'(\sigma_q) \end{pmatrix}$. So $\lambda(\sigma_q)$ is a root, mod p, of the characteristic polynomial of $\overline{\rho}_{E,p}(\sigma_q)$. This is

$$X^2 - \mathrm{Tr}(\overline{\rho}_{E,p}(\sigma_q))X + \det(\overline{\rho}_{E,p}(\sigma_q)) = X^2 - a_q(E)X + q,$$

A root of two polynomials

Fact: $\lambda^{12} = \chi_p^s$ for some $s \in \{0, 4, 6, 8, 12\}$. Moreover, if $s = 6$, then $p \equiv 3 \pmod 4$.

Why is this fact useful?

Let $\sigma_q \in G_{\mathbb{Q}}$ be a Frobenius element at q.

- $\lambda(\sigma_q)^{12} = \chi_p(\sigma_q)^s = q^s \pmod p$.

  So $\lambda(\sigma_q)$ is a root, mod p, of the polynomial $X^{12} - q^s$.

- $\overline{\rho}_{E,p}(\sigma_q) = \begin{pmatrix} \lambda(\sigma_q) & * \\ 0 & \lambda'(\sigma_q) \end{pmatrix}$. So $\lambda(\sigma_q)$ is a root, mod p, of the characteristic polynomial of $\overline{\rho}_{E,p}(\sigma_q)$. This is

$$X^2 - \mathrm{Tr}(\overline{\rho}_{E,p}(\sigma_q))X + \det(\overline{\rho}_{E,p}(\sigma_q)) = X^2 - a_q(E)X + q,$$

  where $a_q(E)$ denotes the *trace of Frobenius* (which is independent of p).

A criterion

- $\lambda(\sigma_q)$ is a root, mod p, of $X^{12} - q^s$ and $X^2 - a_q(E)X + q$.

A criterion

- $\lambda(\sigma_q)$ is a root, mod p, of $X^{12} - q^s$ and $X^2 - a_q(E)X + q$. So

$$p \mid \mathrm{Res}\left(X^{12} - q^s, X^2 - a_q(E)X + q\right).$$

A criterion

- $\lambda(\sigma_q)$ is a root, mod p, of $X^{12} - q^s$ and $X^2 - a_q(E)X + q$. So

$$p \mid \mathrm{Res}\left(X^{12} - q^s, X^2 - a_q(E)X + q\right).$$

Problem. We don't know what $a_q(E)$ is...

A criterion

- $\lambda(\sigma_q)$ is a root, mod p, of $X^{12} - q^s$ and $X^2 - a_q(E)X + q$. So

$$p \mid \mathrm{Res}\left(X^{12} - q^s, X^2 - a_q(E)X + q\right).$$

Problem. We don't know what $a_q(E)$ is... ☹

A criterion

- $\lambda(\sigma_q)$ is a root, mod p, of $X^{12} - q^s$ and $X^2 - a_q(E)X + q$. So

$$p \mid \mathrm{Res}\left(X^{12} - q^s, X^2 - a_q(E)X + q\right).$$

Problem. We don't know what $a_q(E)$ is... ☹

Solution. We know $a_q(E) \in \mathbb{Z}$ and (by the Hasse–Weil bounds)

$$-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}.$$

A criterion

- $\lambda(\sigma_q)$ is a root, mod p, of $X^{12} - q^s$ and $X^2 - a_q(E)X + q$. So

$$p \mid \mathrm{Res}\left(X^{12} - q^s, X^2 - a_q(E)X + q\right).$$

Problem. We don't know what $a_q(E)$ is... ☹

Solution. We know $a_q(E) \in \mathbb{Z}$ and (by the Hasse–Weil bounds)

$$-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}. \quad ☺$$

A criterion

- $\lambda(\sigma_q)$ is a root, mod p, of $X^{12} - q^s$ and $X^2 - a_q(E)X + q$. So

$$p \mid \mathrm{Res}\left(X^{12} - q^s, X^2 - a_q(E)X + q\right).$$

Problem. We don't know what $a_q(E)$ is... ☹

Solution. We know $a_q(E) \in \mathbb{Z}$ and (by the Hasse–Weil bounds)

$$-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}. \quad ☺$$

So

$$p \mid R_{q,s} := \mathrm{lcm}_{-2\sqrt{q} \leq a \leq 2\sqrt{q}} \left(\mathrm{Res}\left(X^{12} - q^s, X^2 - aX + q\right)\right).$$

A criterion

- $\lambda(\sigma_q)$ is a root, mod p, of $X^{12} - q^s$ and $X^2 - a_q(E)X + q$. So

$$p \mid \mathrm{Res}\left(X^{12} - q^s, X^2 - a_q(E)X + q\right).$$

Problem. We don't know what $a_q(E)$ is... ☹
Solution. We know $a_q(E) \in \mathbb{Z}$ and (by the Hasse–Weil bounds)

$$-2\sqrt{q} \leq a_q(E) \leq 2\sqrt{q}. \quad ☺$$

So

$$p \mid R_{q,s} := \mathrm{lcm}_{-2\sqrt{q} \leq a \leq 2\sqrt{q}} \left(\mathrm{Res}\left(X^{12} - q^s, X^2 - aX + q\right)\right).$$

We can compute $R_{q,s}$ and it only depends on q and s.

Some computations

If $s = 0$ or 12.

Some computations

If $s = 0$ or 12. Let $q = 3$.

Some computations

If $s = 0$ or 12. Let $q = 3$. Then

$$R_{3,0} = R_{3,12} = 8131531262400 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 97$$

Some computations

If $s = 0$ or 12. Let $q = 3$. Then

$$R_{3,0} = R_{3,12} = 8131531262400 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 97$$

37 is in our list, but not 97.

Some computations

If $s = 0$ or 12. Let $q = 3$. Then

$$R_{3,0} = R_{3,12} = 8131531262400 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 97$$

37 is in our list, but not 97. To eliminate 97, we use $q = 5$:

Some computations

If $s = 0$ or 12. Let $q = 3$. Then

$$R_{3,0} = R_{3,12} = 8131531262400 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 97$$

37 is in our list, but not 97. To eliminate 97, we use $q = 5$:

$$\begin{aligned} R_{5,0} = R_{5,12} &= 17072929032886039622400 \\ &= 2^8 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 17 \cdot 31^2 \cdot 37 \cdot 61 \cdot 157 \cdot 229 \end{aligned}$$

Some computations

If $s = 0$ or 12. Let $q = 3$. Then

$$R_{3,0} = R_{3,12} = 8131531262400 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 97$$

37 is in our list, but not 97. To eliminate 97, we use $q = 5$:

$$\begin{aligned} R_{5,0} = R_{5,12} &= 170729290328860396224 00 \\ &= 2^8 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 17 \cdot 31^2 \cdot 37 \cdot 61 \cdot 157 \cdot 229 \end{aligned}$$

If $s = 4$ or 8.

Some computations

If $s = 0$ or 12. Let $q = 3$. Then

$$R_{3,0} = R_{3,12} = 8131531262400 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 97$$

37 is in our list, but not 97. To eliminate 97, we use $q = 5$:

$$\begin{aligned} R_{5,0} = R_{5,12} &= 17072929032886039622400 \\ &= 2^8 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 17 \cdot 31^2 \cdot 37 \cdot 61 \cdot 157 \cdot 229 \end{aligned}$$

If $s = 4$ or 8. Let $q = 3$.

Some computations

If $s = 0$ or 12. Let $q = 3$. Then

$$R_{3,0} = R_{3,12} = 8131531262400 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 97$$

37 is in our list, but not 97. To eliminate 97, we use $q = 5$:

$$\begin{aligned} R_{5,0} = R_{5,12} &= 17072929032886039622400 \\ &= 2^8 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 17 \cdot 31^2 \cdot 37 \cdot 61 \cdot 157 \cdot 229 \end{aligned}$$

If $s = 4$ or 8. Let $q = 3$. Then

$$R_{3,4} = R_{3,8} = 9815256000 = 2^6 \cdot 3^8 \cdot 5^3 \cdot 11 \cdot 17.$$

Some computations

If $s = 0$ or 12. Let $q = 3$. Then

$$R_{3,0} = R_{3,12} = 8131531262400 = 2^6 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 19 \cdot 37 \cdot 97$$

37 is in our list, but not 97. To eliminate 97, we use $q = 5$:

$$\begin{aligned} R_{5,0} = R_{5,12} &= 170729290328860396224 00 \\ &= 2^8 \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 17 \cdot 31^2 \cdot 37 \cdot 61 \cdot 157 \cdot 229 \end{aligned}$$

If $s = 4$ or 8. Let $q = 3$. Then

$$R_{3,4} = R_{3,8} = 9815256000 = 2^6 \cdot 3^8 \cdot 5^3 \cdot 11 \cdot 17.$$

Conclusion: If $s \in \{0, 4, 8, 12\}$, then $p = 37$ (since $p \geq 23$).

The case $s = 6$

If $s = 6$ then

The case $s = 6$

If $s = 6$ then

$$R_{q,6} = 0 \text{ for any prime } q.$$

The case $s = 6$

If $s = 6$ then

$$R_{q,6} = 0 \text{ for any prime } q.$$

This tells us *nothing* about p...

The case $s = 6$

If $s = 6$ then

$$R_{q,6} = 0 \text{ for any prime } q.$$

This tells us *nothing* about p...

Why? If $a = a_q(E) = 0$ then we are considering the polynomials

$$X^{12} - q^6 \quad \text{and} \quad X^2 + q.$$

The case $s = 6$

If $s = 6$ then

$$R_{q,6} = 0 \text{ for any prime } q.$$

This tells us *nothing* about p...

Why? If $a = a_q(E) = 0$ then we are considering the polynomials

$$X^{12} - q^6 \quad \text{and} \quad X^2 + q.$$

These share the roots $\pm\sqrt{-q}$, so their resultant is always 0.

The case $s = 6$

If $s = 6$ then

$$R_{q,6} = 0 \text{ for any prime } q.$$

This tells us *nothing* about p...

Why? If $a = a_q(E) = 0$ then we are considering the polynomials

$$X^{12} - q^6 \quad \text{and} \quad X^2 + q.$$

These share the roots $\pm\sqrt{-q}$, so their resultant is always 0.

We need a different argument...

Relating λ to χ_p

Suppose $s = 6$, so $\lambda^{12} = \chi_p^6$. Recall that $p \equiv 3 \pmod 4$.

Relating λ to χ_p

Suppose $s = 6$, so $\lambda^{12} = \chi_p^6$. Recall that $p \equiv 3 \pmod 4$.

Define $\psi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ by $\psi = \lambda \chi_p^{-\frac{p+1}{4}}$.

Relating λ to χ_p

Suppose $s = 6$, so $\lambda^{12} = \chi_p^6$. Recall that $p \equiv 3 \pmod 4$.

Define $\psi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ by $\psi = \lambda \chi_p^{-\frac{p+1}{4}}$. Then

$$\psi^{12} = \frac{\lambda^{12}}{\chi_p^{3(p+1)}} = \frac{\lambda^{12}}{\chi_p^{3(p-1)}\chi_p^6} = \frac{\lambda^{12}}{\chi_p^6} = 1.$$

Relating λ to χ_p

Suppose $s = 6$, so $\lambda^{12} = \chi_p^6$. Recall that $p \equiv 3 \pmod 4$.

Define $\psi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ by $\psi = \lambda \chi_p^{-\frac{p+1}{4}}$. Then

$$\psi^{12} = \frac{\lambda^{12}}{\chi_p^{3(p+1)}} = \frac{\lambda^{12}}{\chi_p^{3(p-1)}\chi_p^6} = \frac{\lambda^{12}}{\chi_p^6} = 1.$$

Also $\psi^{p-1} = 1$.

Relating λ to χ_p

Suppose $s = 6$, so $\lambda^{12} = \chi_p^6$. Recall that $p \equiv 3 \pmod 4$.

Define $\psi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ by $\psi = \lambda \chi_p^{-\frac{p+1}{4}}$. Then

$$\psi^{12} = \frac{\lambda^{12}}{\chi_p^{3(p+1)}} = \frac{\lambda^{12}}{\chi_p^{3(p-1)}\chi_p^6} = \frac{\lambda^{12}}{\chi_p^6} = 1.$$

Also $\psi^{p-1} = 1$. So $\psi^{\gcd(12,p-1)} = 1$,

Relating λ to χ_p

Suppose $s = 6$, so $\lambda^{12} = \chi_p^6$. Recall that $p \equiv 3 \pmod 4$.

Define $\psi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ by $\psi = \lambda \chi_p^{-\frac{p+1}{4}}$. Then

$$\psi^{12} = \frac{\lambda^{12}}{\chi_p^{3(p+1)}} = \frac{\lambda^{12}}{\chi_p^{3(p-1)}\chi_p^6} = \frac{\lambda^{12}}{\chi_p^6} = 1.$$

Also $\psi^{p-1} = 1$. So $\psi^{\gcd(12,p-1)} = 1$, so $\psi^6 = 1$.

Relating λ to χ_p

Suppose $s = 6$, so $\lambda^{12} = \chi_p^6$. Recall that $p \equiv 3 \pmod 4$.

Define $\psi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ by $\psi = \lambda \chi_p^{-\frac{p+1}{4}}$. Then

$$\psi^{12} = \frac{\lambda^{12}}{\chi_p^{3(p+1)}} = \frac{\lambda^{12}}{\chi_p^{3(p-1)}\chi_p^6} = \frac{\lambda^{12}}{\chi_p^6} = 1.$$

Also $\psi^{p-1} = 1$. So $\psi^{\gcd(12,p-1)} = 1$, so $\psi^6 = 1$.

Next,

$$\lambda^2(\sigma_q) = \psi^2(\sigma_q)\chi_p(\sigma_q)^{\frac{p+1}{2}} = \psi^2(\sigma_q) q^{\frac{p+1}{2}} \pmod p.$$

The link to $\mathbb{Q}(\sqrt{-p})$

Claim

If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.

The link to $\mathbb{Q}(\sqrt{-p})$

Claim

If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.

Proof. Suppose not.

The link to $\mathbb{Q}(\sqrt{-p})$

Claim

If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.

Proof. Suppose not.

- Then $\left(\frac{q}{p}\right) = 1$. So $q^{\frac{p+1}{2}} = q \pmod{p}$.

The link to $\mathbb{Q}(\sqrt{-p})$

Claim

If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.

Proof. Suppose not.

- Then $\left(\frac{q}{p}\right) = 1$. So $q^{\frac{p+1}{2}} = q \pmod{p}$.
- So

$$\lambda^2(\sigma_q) = \psi^2(\sigma_q) q^{\frac{p+1}{2}} = q \cdot \psi^2(\sigma_q) \pmod{p}.$$

The link to $\mathbb{Q}(\sqrt{-p})$

Claim

If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.

Proof. Suppose not.

- Then $\left(\frac{q}{p}\right) = 1$. So $q^{\frac{p+1}{2}} = q \pmod{p}$.
- So
$$\lambda^2(\sigma_q) = \psi^2(\sigma_q) q^{\frac{p+1}{2}} = q \cdot \psi^2(\sigma_q) \pmod{p}.$$
- Then
$$(\lambda')^2(\sigma_q) = \chi_p^2(\sigma_q)\lambda^{-2}(\sigma_q) = q \cdot \psi^{-2}(\sigma_q) \pmod{p}.$$

The link to $\mathbb{Q}(\sqrt{-p})$

Claim

If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.

Proof. Suppose not.

- Then $\left(\frac{q}{p}\right) = 1$. So $q^{\frac{p+1}{2}} = q \pmod{p}$.
- So
$$\lambda^2(\sigma_q) = \psi^2(\sigma_q) q^{\frac{p+1}{2}} = q \cdot \psi^2(\sigma_q) \pmod{p}.$$
- Then
$$(\lambda')^2(\sigma_q) = \chi_p^2(\sigma_q)\lambda^{-2}(\sigma_q) = q \cdot \psi^{-2}(\sigma_q) \pmod{p}.$$
- So
$$\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}.$$

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

- The LHS

$$= (\lambda(\sigma_q) + \lambda'(\sigma_q))^2 - 2(\lambda\lambda')(\sigma_q) = a_q(E)^2 - 2q \pmod{p}.$$

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

- The LHS

$$= (\lambda(\sigma_q) + \lambda'(\sigma_q))^2 - 2(\lambda\lambda')(\sigma_q) = a_q(E)^2 - 2q \pmod{p}.$$

- On the RHS: $\psi^6 = 1$.

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

- The LHS

$$= (\lambda(\sigma_q) + \lambda'(\sigma_q))^2 - 2(\lambda\lambda')(\sigma_q) = a_q(E)^2 - 2q \pmod{p}.$$

- On the RHS: $\psi^6 = 1$. So $\psi^2(\sigma_q)$ is a third root of unity.

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

- The LHS

$$= (\lambda(\sigma_q) + \lambda'(\sigma_q))^2 - 2(\lambda\lambda')(\sigma_q) = a_q(E)^2 - 2q \pmod{p}.$$

- On the RHS: $\psi^6 = 1$. So $\psi^2(\sigma_q)$ is a third root of unity. So

$$\psi^2(\sigma_q) + \psi^{-2}(\sigma_q) = 2 \text{ or } -1 \pmod{p}.$$

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

- The LHS

$$= (\lambda(\sigma_q) + \lambda'(\sigma_q))^2 - 2(\lambda\lambda')(\sigma_q) = a_q(E)^2 - 2q \pmod{p}.$$

- On the RHS: $\psi^6 = 1$. So $\psi^2(\sigma_q)$ is a third root of unity. So

$$\psi^2(\sigma_q) + \psi^{-2}(\sigma_q) = 2 \text{ or } -1 \pmod{p}.$$

- So $a_q(E)^2 = q$ or $4q \pmod{p}$.

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

- The LHS

$$= (\lambda(\sigma_q) + \lambda'(\sigma_q))^2 - 2(\lambda\lambda')(\sigma_q) = a_q(E)^2 - 2q \pmod{p}.$$

- On the RHS: $\psi^6 = 1$. So $\psi^2(\sigma_q)$ is a third root of unity. So

$$\psi^2(\sigma_q) + \psi^{-2}(\sigma_q) = 2 \text{ or } -1 \pmod{p}.$$

- So $a_q(E)^2 = q$ or $4q \pmod{p}$.
- But since $0 \leq a_q(E)^2 < 4q$,

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

- The LHS

$$= (\lambda(\sigma_q) + \lambda'(\sigma_q))^2 - 2(\lambda\lambda')(\sigma_q) = a_q(E)^2 - 2q \pmod{p}.$$

- On the RHS: $\psi^6 = 1$. So $\psi^2(\sigma_q)$ is a third root of unity. So

$$\psi^2(\sigma_q) + \psi^{-2}(\sigma_q) = 2 \text{ or } -1 \pmod{p}.$$

- So $a_q(E)^2 = q$ or $4q \pmod{p}$.
- But since $0 \leq a_q(E)^2 < 4q$,

$$-4q < a_q(E)^2 - 4q < 4q \quad \text{and} \quad -q \leq a_q(E)^2 - q < 3q.$$

Proof of claim continued

We have $\lambda^2(\sigma_q) + (\lambda')^2(\sigma_q) = q \cdot \left(\psi^2(\sigma_q) + \psi^{-2}(\sigma_q)\right) \pmod{p}$.

- The LHS

$$= (\lambda(\sigma_q) + \lambda'(\sigma_q))^2 - 2(\lambda\lambda')(\sigma_q) = a_q(E)^2 - 2q \pmod{p}.$$

- On the RHS: $\psi^6 = 1$. So $\psi^2(\sigma_q)$ is a third root of unity. So

$$\psi^2(\sigma_q) + \psi^{-2}(\sigma_q) = 2 \text{ or } -1 \pmod{p}.$$

- So $a_q(E)^2 = q$ or $4q \pmod{p}$.
- But since $0 \leq a_q(E)^2 < 4q$,

$$-4q < a_q(E)^2 - 4q < 4q \quad \text{and} \quad -q \leq a_q(E)^2 - q < 3q.$$

- A contradiction, since $4q < p$ by assumption.

Extending to $q = 2$

Know. If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.

Extending to $q = 2$

Know. If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.
Consequence. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $2 < \mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Extending to $q = 2$

Know. If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.

Consequence. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $2 < \mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Fact: this is also true if $\mathrm{Norm}(\mathfrak{q}) = 2$.

Extending to $q = 2$

Know. If $2 < q < p/4$ then q is inert in $\mathbb{Q}(\sqrt{-p})$.
Consequence. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $2 < \mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.
Fact: this is also true if $\mathrm{Norm}(\mathfrak{q}) = 2$.

Recall $p \equiv 3 \pmod 4$, so $\Delta_{\mathbb{Q}(\sqrt{-p})} = -p$, and $\mathcal{O}_{\mathbb{Q}(\sqrt{-p})} = \mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$

- If $\mathrm{Norm}(\mathfrak{q}) = 2$ then 2 splits in $\mathbb{Q}(\sqrt{-p})$ and $p \equiv -1$ or $7 \pmod{16}$.
- Suppose $p = -1 + 16t$. Define

$$\alpha = \frac{3 + \sqrt{-p}}{2} \in \mathcal{O}_{\mathbb{Q}(\sqrt{-p})}.$$

- Then $\mathrm{Norm}(\alpha) = 2(1 + 2t)$.
- So $\langle \alpha \rangle = \mathfrak{c}_2 \cdot \mathfrak{b}$ for some $\mathfrak{c}_2 \mid 2$ and an odd ideal $\mathfrak{b}$ satisfying $\mathrm{Norm}(\mathfrak{b}) = 1 + 2t < p/4$.
- So $\mathfrak{b}$ is principal. So $\mathfrak{c}_2$ is principal.

Completing the proof

Know. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $\mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Completing the proof

Know. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $\mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Minkowski's Theorem says that the class group of $\mathbb{Q}(\sqrt{-p})$ is generated by the prime ideals of norm $< M_{\mathbb{Q}(\sqrt{-p})}$,

Completing the proof

Know. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $\mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Minkowski's Theorem says that the class group of $\mathbb{Q}(\sqrt{-p})$ is generated by the prime ideals of norm $< M_{\mathbb{Q}(\sqrt{-p})}$, where

$$M_{\mathbb{Q}(\sqrt{-p})} = \frac{2\sqrt{p}}{\pi} < p/4.$$

Completing the proof

Know. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $\mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Minkowski's Theorem says that the class group of $\mathbb{Q}(\sqrt{-p})$ is generated by the prime ideals of norm $< M_{\mathbb{Q}(\sqrt{-p})}$, where

$$M_{\mathbb{Q}(\sqrt{-p})} = \frac{2\sqrt{p}}{\pi} < p/4.$$

So all generators of the class group are principal ideals.

Completing the proof

Know. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $\mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Minkowski's Theorem says that the class group of $\mathbb{Q}(\sqrt{-p})$ is generated by the prime ideals of norm $< M_{\mathbb{Q}(\sqrt{-p})}$, where

$$M_{\mathbb{Q}(\sqrt{-p})} = \frac{2\sqrt{p}}{\pi} < p/4.$$

So all generators of the class group are principal ideals.

So $\mathbb{Q}(\sqrt{-p})$ has class number 1.

Completing the proof

Know. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $\mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Minkowski's Theorem says that the class group of $\mathbb{Q}(\sqrt{-p})$ is generated by the prime ideals of norm $< M_{\mathbb{Q}(\sqrt{-p})}$, where

$$M_{\mathbb{Q}(\sqrt{-p})} = \frac{2\sqrt{p}}{\pi} < p/4.$$

So all generators of the class group are principal ideals.

So $\mathbb{Q}(\sqrt{-p})$ has class number 1. So $p = 43, 67$, or 163, since $p \geq 23$ by assumption.

Completing the proof

Know. If $\mathfrak{q}$ is a prime of $\mathbb{Q}(\sqrt{-p})$ and $\mathrm{Norm}(\mathfrak{q}) < p/4$, then $\mathfrak{q}$ is principal.

Minkowski's Theorem says that the class group of $\mathbb{Q}(\sqrt{-p})$ is generated by the prime ideals of norm $< M_{\mathbb{Q}(\sqrt{-p})}$, where

$$M_{\mathbb{Q}(\sqrt{-p})} = \frac{2\sqrt{p}}{\pi} < p/4.$$

So all generators of the class group are principal ideals.

So $\mathbb{Q}(\sqrt{-p})$ has class number 1. So $p = 43, 67$, or 163, since $p \geq 23$ by assumption.