Rational Isogenies of Prime Degree

Tyler Genao

January 21, 2020

Theorem (Rational Isogenies of Prime Degree, Mazur 1978)

If $p \in \mathbb{Z}$ is a prime such that some elliptic curve over $\mathbb{Q}$ admits a $\mathbb{Q}$-rational p-isogeny, then
$p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$.

- Mazur proves this by showing $p \leq 17$, $p = 37$, or $\mathbb{Q}(\sqrt{-p})$ has class number one.
- Such examples of $\mathbb{Q}$-rational p-isogenies were already known. Examples include:
  1. Genus zero cases: $X_0(p)$ for $p = 2, 3, 5, 7, 13$.
  2. CM points defined over $\mathbb{Q}$: these are given by $p = 2, 3, 7, 11, 19, 43, 67, 163$.
- There are examples of rational $p = 17, 37$ isogenies, but they are neither of the genus zero case nor the CM case.

- Expanding on some examples of $\mathbb{Q}$-rational p-isogenies:
  1. Genus zero cases, e.g. $p = 2, 3, 5, 7, 13$: the modular curve $X_0(p)$ can always be defined over $\mathbb{Q}$. $X_0(p)$ also always has at least one $\mathbb{Q}$-rational point – namely, the cusp at infinity. Therefore, it must be isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$, and since it has finitely many cusps it will have infinitely many noncusps. We note that the noncusps will correspond (up to appropriate isomorphism) to an elliptic curve $E_{/\mathbb{Q}}$ with a $\mathbb{Q}$-rational p-isogeny.

- Expanding on some examples of $\mathbb{Q}$-rational p-isogenies: **2.** CM cases $p = 11, 19, 43, 67, 163$: by the theory of complex multiplication, one has for $K := \mathbb{Q}(\sqrt{-p})$ that any elliptic curve E with CM by $\mathcal{O}_K$ has a rational cyclic isogeny ϕ of degree p coming from the prime ideal $\mathfrak{P} := \sqrt{-p}\mathcal{O}_K$.

Proposition

Let K be a number field and $N > 0$ a squarefree integer. Let $\mathfrak{q} \subseteq \mathcal{O}_K$ be prime and above a prime $q \in \mathbb{Z}$, with ramification index

$$e_{\mathfrak{q}}(K/\mathbb{Q}) < q - 1.$$

Let $E_{/K}$ be an elliptic curve with a K-rational cyclic N-isogeny C_N. Let $x := (E, C_N) \in X_0(N)(K)$, and suppose there is an optimal quotient $\pi : J_0(N)^{\text{new}}_{/K} \twoheadrightarrow A_{/K}$ such that $\pi(x)$ has finite order in $A(K)$. Then E has potentially good reduction at $\mathfrak{q}$.

Corollary ($K = \mathbb{Q}$)

Let $K = \mathbb{Q}$ and $N > 0$ a squarefree integer. Let $q \in \mathbb{Z}$ be an odd prime, so its ramification index

$$e_q(K/\mathbb{Q}) = 1 < q - 1.$$

Let $E_{/\mathbb{Q}}$ be an elliptic curve with a $\mathbb{Q}$-rational cyclic N-isogeny C_N. Let $x := (E, C_N) \in X_0(N)(\mathbb{Q})$. Since there is an optimal quotient $\pi : J_0(N)^{\text{new}}_{/\mathbb{Q}} \twoheadrightarrow A_{/\mathbb{Q}}$ (the Eisenstein quotient) with finite Mordell-Weil group, E has potentially good reduction at q.

- If $E_{/\mathbb{Q}}$ has a rational p-isogeny for $p \geq 5$, then E has in fact **good reduction** at all odd primes $\neq p$.
- To see this, note that multiplicative reduction is impossible since it is preserved under base change, which contradicts potentially good reduction.
- On the other hand, additive reduction is impossible since the Tamagawa number is at most 4, whereas our generator for the isogeny is of prime order > 4.

- With the previous proposition, one can reprove Mazur's theorem:

Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$. Then one has the torsion subgroup

$$E_{\text{tors}}(\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/N\mathbb{Z}, & \text{for some } N = 1, 2, \ldots, 10, 12; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, & \text{for some } N = 1, 2, 3, 4 \end{cases}.$$

- Prove by assuming potentially good reduction at $q = 3$, and work through cases for reduction.

- Let $C_p \leq E_{/K}$ be a K-rational p-isogeny. Then we have a mod$-p$ Galois representation

$$\rho_{E,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$$

given by

$$\rho_{E,p}(G_K) = \begin{bmatrix} r & * \\ 0 & \frac{\chi_p}{r} \end{bmatrix}$$

where $\chi_p : G_K \to \mathbb{F}_p^\times$ is the mod p cyclotomic character.

- $r : G_K \to \mathbb{F}_p^\times$ is called the *isogeny character* of C_p.

- Assume that $p \in \mathbb{Z}$ is inert in K. Then one has the factorization

$$r = \alpha \cdot \chi_p^k$$

for some unramified character α at $p\mathcal{O}_K$ and $0 \leq k < p$.

Proposition

If E also has potentially good reduction at $p\mathcal{O}_K$, then α^{2t} is unramified everywhere, where

$$t := \begin{cases} 6 & if\ p \equiv 1 \pmod{12} \\ 2 & if\ p \equiv 5 \pmod{12} \\ 3 & if\ p \equiv 7 \pmod{12} \\ 1 & if\ p \equiv 11 \pmod{12} \end{cases}$$

and k must satisfy

$$k \mod \frac{p-1}{2} = \begin{cases} 0, 1 \\ \frac{1}{2} \\ \frac{1}{3}, \frac{2}{3} \end{cases}.$$

Furthermore, when $K = \mathbb{Q}$ one has the order of α divides 12.

- From here on out, we will assume that K is a number field, $E_{/K}$ an elliptic curve with a K-rational p-isogeny where $p \in \mathbb{Z}_{\geq 5}$ is inert in K, and $\mathfrak{Q} \subseteq \mathcal{O}_K$ a prime ideal of characteristic $\neq p$, such that E has potentially good reduction at $p\mathcal{O}_K$ and $\mathfrak{Q}$. We note that E must have good reduction at $\mathfrak{Q}$.
- Mazur shows that C_p descends to a $k(\mathfrak{Q})$-rational p-isogeny on $\tilde{E}_{/k(\mathfrak{Q})}$, with an isogeny character $b_{\mathfrak{Q}} \cdot \chi_p^k$ where $b_{\mathfrak{Q}}$ is an unramified character of order dividing 12. Here, $k(\mathfrak{Q}) := \mathcal{O}_K/\mathfrak{Q}$.

- The mod-p Galois representation for $\tilde{E}_{k(\mathfrak{Q})}$ is then

$$\rho_{\tilde{E},p} = \begin{bmatrix} b_{\mathfrak{Q}}\chi_p^k & * \\ 0 & b_{\mathfrak{Q}}^{-1}\chi_p^{1-k} \end{bmatrix}.$$

- Taking the trace gives

$$\mathrm{Tr}(\rho_{\tilde{E},p}) \equiv b_{\mathfrak{Q}}\chi_p^k + b_{\mathfrak{Q}}^{-1}\chi_p^{1-k} \pmod{p}.$$

- The image on the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{Q}}$, which generates $\mathrm{Gal}(\overline{k(\mathfrak{Q})}/k(\mathfrak{Q}))$, is then

$$\mathrm{Tr}(\rho_{\tilde{E},p}(\mathrm{Frob}_{\mathfrak{Q}})) \equiv b_{\mathfrak{Q}}(\mathrm{Frob}_{\mathfrak{Q}})q_0^k + b_{\mathfrak{Q}}(\mathrm{Frob}_{\mathfrak{Q}})^{-1}q_0^{1-k} \pmod{p}$$

where $q_0 := \#|k(\mathfrak{Q})|$.

- Let us look at the case $E_{/\mathbb{Q}}$, $q_0 = q \in \mathbb{Z}$:

$$\mathrm{Tr}(\rho_{\tilde{E},p}(\mathrm{Frob}_q)) \equiv b_q(\mathrm{Frob}_q)q_0^k + b_q(\mathrm{Frob}_q)^{-1}q_0^{1-k} \pmod{p}.$$

- Then the LHS of the congruence is the trace of Frobenius of $\tilde{E}_{/\mathbb{F}_q}$.
- Passing to the extension $\mathbb{F}_{q^{12}}/\mathbb{F}_q$, we get $q_0 = q^{12}$. Noting that b_q has order dividing 12, we conclude the following fact about the trace of Frobenius computed relative to $\mathbb{F}_{q^{12}}$.

Corollary

With notation as in this section, one has

1. $b_q(\mathrm{Frob}_q)q^k + b_q(\mathrm{Frob}_q)^{-1}q^{1-k}$ *is congruent mod* p *to the trace of Frobenius of some elliptic curve* $E'_{/\mathbb{F}_q}$;
2. $q^{12k} + q^{12-12k}$ *is congruent mod* p *to the trace of Frobenius of some elliptic curve* $E'_{/\mathbb{F}_q}$ *computed over* $\mathbb{F}_{q^{12}}$.

Theorem (Rational isogenies of prime degree)

For $p = 11$ or $p \geq 17$, if there is an elliptic curve $E_{/\mathbb{Q}}$ with a rational p-isogeny then $p = 11, 17, 19, 37, 43, 67, 163$.

- The rest of the slides will outline the proof of this theorem.

- Suppose $E_{/\mathbb{Q}}$ is an elliptic curve with a rational p-isogeny, $p = 11$ or $p \geq 17$. Then E has good reduction at all odd primes q. We also have an isogeny character $r = b_q \cdot \chi_p^k \bmod q$, as before; k is constrained to three cases mod $\frac{p-1}{2}$.
- Apply such cases to the congruence

$$\mathrm{Tr}(\rho_{\tilde{E},p}(\mathrm{Frob}_q)) \equiv q^{12k} + q^{12-12k} \pmod{p}$$

for small q. We also compute all possible traces of Frobenius over $\mathbb{F}_{q^{12}}$ for elliptic curves defined over $\mathbb{F}_q$, and check which p satisfy at least one congruence.
- We do this for each of the cases $k \equiv 0 \pmod{p-1}, 3k \equiv 1 \pmod{p-1}, 2k \equiv 1 + \frac{p-1}{2} \pmod{p-1}$.

Here is an example of the proof for $k \equiv 0 \pmod{p-1}$:

- We start with $q = 3$. A computer check tells us that the possible traces of Frobenius for $E_{/\mathbb{F}_3}$ computed over $\mathbb{F}_{3^{12}}$ are $658, -1358, 1458$. We then check the congruence

$$658, -1358, 1458 \equiv 1 + 3^{12} \pmod{p}$$

  and find this is satisfied when $p = 2, 3, 5, 7, 13, 19, 37, 97$.
- We know $Y_0(p)(\mathbb{Q}) \neq \emptyset$ when $p = 2, 3, 5, 7, 13, 19, 37$. $p = 97$ is suspicious.

- We repeat the calculations with $q = 5$: in particular, we check for which p at least one congruence

$$31250, 23506, -25774, -28334 \equiv 1 + 5^{12} \pmod{p}$$

holds. We find that $p = 2, 3, 5, 7, 13, 17, 31, 37, 61, 157, 229$, which lacks $p = 97$. We conclude there are no rational cyclic 97-isogenies.

- Unfortunately, the previous argument does not work in the third case $2k \equiv 1 + \frac{p-1}{2} \pmod{p-1}$. We get 231 possible primes p when checking $q = 3$, and 3368 possible primes p when checking $q = 5$.
- Using basic algebraic number theory, Mazur argues that in this case one must have that $\mathbb{Q}(\sqrt{-p})$ has class number one, and thus $p = 11, 19, 43, 67, 163$, which we have examples of rational p-isogenies for.

- First, he shows that all odd primes $q < \frac{p}{4}$ are inert in $K := \mathbb{Q}(\sqrt{-p})$.
- The Minkowski constant

$$M_K := \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\Delta_K|} = \frac{2\sqrt{p}}{\pi}$$

  is less than $\frac{p}{4}$, so with the previous fact any ideal in K of odd norm $< \frac{p}{4}$ is principal.
- Finally, he considers the case where 2 is not inert in K, and shows that primes above 2 are principal.

Thank you!