RATIONAL ISOGENIES OF PRIME DEGREE

TYLER GENAO

1. Introduction

These notes follow the seminal 1978 paper "Rational Isogenies of Prime Degree" [Maz78]. In it, Mazur classifies all (elliptic curve) $\mathbb{Q}$-rational p-isogenies for prime p; such a classificaition is equivalent to determining for which prime p the modular curve $Y_0(p)$ has a rational point. This is part of a larger study of rational cyclic N-isogenies for positive integers N. At the time, the only such examples were those in Table 1 of [Maz78].

The main result of Mazur's paper is the following:

Theorem 1. [Maz78] *If $p \in \mathbb{Z}$ is prime such that some elliptic curve over $\mathbb{Q}$ admits a $\mathbb{Q}$-rational p-isogeny, then $p \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}$.*

This theorem reduces the problem of determining for which N one has $Y_0(N)(\mathbb{Q}) \neq \emptyset$ to the handful of integers $N = 39, 65, 91, 125, 169$, cf. Mazur's comments on p. 131 [Maz78]. Kenku studies this handful of N in a series of papers, culminating in [Ken81]. The conclusion is that the beginning table in [Maz78] is the complete list of N for which $X_0(N)$ has a rational noncuspidal point.

2. Rational points on elliptic curves

In proving the main result on $\mathbb{Q}$-rational prime isogenies, Mazur also proves a result on the torsion structure of an elliptic curve over $\mathbb{Q}$, see Theorem 4.1 [Maz78]. At the time, this result was also recently proven by Mazur in his previous paper on Eisenstein ideals [Maz77].

Theorem 2 (Mazur's Theorem [Maz77], [Maz78])**.** *Let E be an elliptic curve defined over $\mathbb{Q}$. Then one has the torsion subgroup*

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

Moreover, each possible group is the $\mathbb{Q}$-torsion subgroup of some $E_{/\mathbb{Q}}$.

This theorem was first "officially" conjectured by Ogg in [Ogg75]. That these were the only possible torsion structures was based in part on the following arguments. First, it was clear that that for any $E_{/\mathbb{Q}}$, $E(\mathbb{Q})$ is either cyclic or the product of a cyclic group with $\mathbb{Z}/2\mathbb{Z}$[1], and so the main problem was to find all possible orders for a rational

[1] By properties of the Weil pairing, if $E_{/K}$ is an elliptic curve with $E[N] \subseteq E(K)$, then the N'th roots of unity $\mu_N \subseteq K$. In particular, an $E_{/\mathbb{Q}}$ can only have $E[N] \subseteq E(\mathbb{Q})$ for $N = 1, 2$. Now, since the torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ is finite abelian, it is a product of finite cyclics. If a product

torsion point on an elliptic curve. For families of examples, see the table on p. 217 in [Kub76].

It was known by Serre and others in 1971 (cf. [Ogg75], or [DR73]) that the noncuspidal points of the modular curve $X_0(N)$ form an affine curve $Y_0(N)$, and that the points of $Y_0(N)(\mathbb{Q})$ parametrize elliptic curves $E_{/\mathbb{Q}}$ with a rational[2] cyclic[3] subgroup of order N, up to a certain type of isomorphism. Similarly the noncuspidal points of the modular curve $X_1(N)$ form an affine curve $Y_1(N)$, whose rational points parametrize $E_{/\mathbb{Q}}$ with a $\mathbb{Q}$-rational point of order N up to isomorphism. In particular, if an elliptic curve $E_{/\mathbb{Q}}$ has a $\mathbb{Q}$-rational point P of order N, then the curve gives rise to rational noncuspidal points $(E, P) \in X_1(N)$ and $(E, \langle P \rangle) \in X_0(N)$.

Through explicit formulas, the genus of the curve $X_1(N)$ was known to equal 0 for exactly $N = 1, 2, \ldots, 10, 12$, and since $X_1(N)$ always has a $\mathbb{Q}$-rational point (the cusp at infinity), it follows that for such $N \neq 11 \leq 12$ one has $X_1(N) \cong \mathbb{P}^1_{\mathbb{Q}}$. One may conclude that for such N there are **infinitely** many nonisomorphic elliptic curves defined over $\mathbb{Q}$ with a $\mathbb{Q}$-rational point of order N. In particular, there are *many* examples of elliptic curves over $\mathbb{Q}$ with $\mathbb{Q}$-rational points of an order $1, 2, \ldots, 10, 12$.

Around 1975, one also knew that for $N < 151$ and $N \neq 1, 2, \ldots, 10, 12$ there did not exist $\mathbb{Q}$-rational points of order N on *any* elliptic curve $E_{/\mathbb{Q}}$. Thus one might have conjectured that $\mathbb{Q}$-rational points of order $1, 2, \ldots, 10, 12$ were the only possibilities. If one could show this, then one would see that the only possible torsion subgroups for $E_{/\mathbb{Q}}$ are those appearing in Theorem 2. Coupling this with explicit examples of such torsion subgroups in [Kub76], one would then prove Mazur's Theorem.

3. Examples of rational points on $Y_0(N)$

At the time of [Ogg75], one only knew that $Y_0(N) := X_0(N) \smallsetminus \{\text{cusps}\}$ had a $\mathbb{Q}$-rational point for $N = 1 - 19, 21, 25, 27, 37, 43, 67, 163$. Some examples are as such:

- When $X_0(N)$ has genus zero, i.e., when $N \in [1, 10] \cup \{12, 13, 16, 18, 25\}$. As mentioned earlier, such genus zero cases will always have infinitely many rational points since they are guaranteed at least one: the cusp at infinity.
- Positive integers N such that there is an imaginary quadratic field K and an order $\mathcal{O} \subseteq K$ of class number one with $\sqrt{-N} \in \mathcal{O}$. Some examples include $N \in \{11, 19, 43, 67, 163\}$.

Let us examine the second set of examples and how one produces rational cyclic isogenies through them. We begin with a review of the theory of *complex multiplication*, often called *CM*. For a proper reference on the theory of complex multiplication by $\mathcal{O}_K$, see [Sil94].

$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \subseteq E_{\text{tors}}(\mathbb{Q})$, then from $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \subseteq E[p]$ and $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ this implies $E[p] \subseteq E(\mathbb{Q})$, and thus $\mu_p \subseteq \mathbb{Q}$, whence $p = 2$.

[2] Here, rational means "fixed under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$", as in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ takes the cyclic subgroup to itself. We note that a K-rational subgroup of an $E_{/K}$ is "equivalent data" to a K-rational isogeny from E.

[3] Call an isogeny $\phi : E \to E'$ *cyclic* if its kernel is cyclic.

Denote by $[f, \Delta_K]$ the imaginary quadratic order in $\mathbb{Q}(\sqrt{\Delta_K})$ of conductor f; its discriminant is then $f^2\Delta_K$. Let $\mathcal{O}$ be an order with class number $h_{\mathcal{O}} = 1$, i.e., let

$$\begin{aligned}\mathcal{O} \in \{&[1, -3], [2, -3], [3, -3], [1, -4], [2, -4], [1, -7], [2, -7], [1, -8], [1, -11],\\ &[1, -19], [1, -43], [1, -67], [1, -163]\}.\end{aligned}$$

Let $I \subseteq \mathcal{O}$ be an invertible ideal, and write its factorization as $I = \prod_{\mathfrak{P}\subseteq\mathcal{O}} \mathfrak{P}^{a_{\mathfrak{P}}}$; necessarily each $\mathfrak{P}$ dividing I is also invertible in $\mathcal{O}$. By Theorems and Corollaries 3.8, 3.9, and 3.12 in [Con], one has that $\mathfrak{P}\mathcal{O}_K$ is also prime with $\mathcal{O}/\mathfrak{P} \cong \mathcal{O}_K/\mathfrak{P}\mathcal{O}_K$, along with a prime factorization $I\mathcal{O}_K = \prod_{\mathfrak{P}|I} \mathfrak{P}^{a_{\mathfrak{P}}}\mathcal{O}_K$. Then the Chinese Remainder Theorem gives us

$$\mathcal{O}/I \cong \bigoplus_{\mathfrak{P}|I} \mathcal{O}/\mathfrak{P}_p^{a_{\mathfrak{P}}} \cong \bigoplus_{\mathfrak{P}|I} \mathcal{O}_K/\mathfrak{P}^{a_{\mathfrak{P}}}\mathcal{O}_K.$$

Assuming that each factor $\mathcal{O}_K/\mathfrak{P}^{a_{\mathfrak{P}}}\mathcal{O}_K$ in this direct sum is additively cyclic and of order coprime to the others, their direct sum $\mathcal{O}/I$ will also be additively cyclic.

Next, recall that there exists an elliptic curve $E_{/\mathbb{Q}}$ with CM by $\mathcal{O}$, and that there is a particular normalized isomorphism $\mathcal{O} \cong_{[\cdot]} \mathrm{End}(E)$. Then any endomorphism $\phi \in \mathrm{End}(E)$ may be written as $\phi = [\alpha]$ for a unique element $\alpha \in \mathcal{O}$, and will have degree equal to the field norm $N_{K/\mathbb{Q}}(\alpha)$. One also has that any invertible ideal $I \subseteq \mathcal{O}$ determines an elliptic curve isogeny $[I] : E \to E/E[I]$ of degree $N(I) := \#|\mathcal{O}/I|$. For invertible ideals $I \subseteq \mathcal{O}$, one has for the isogeny $[I]$ of E that $E[I] := \ker[I] \cong_{\mathcal{O}} (\mathcal{O}/I, +)$. The conclusion is that $[I]$ is a *cyclic* isogeny if $\mathcal{O}/I$ is additively cyclic.

Let us discuss rationality of the isogeny $[I]$. Recall that $[I]$ is always defined over $K(j(E))$, the Hilbert class field of K. In particular, since we are assuming $h_{\mathcal{O}} = 1$ it follows that $K(j(E)) = K$, and so $[I]$ is defined over K. To check if $[I]$ is $\mathbb{Q}$-rational, we must check that $[I]$ is unaffected by complex conjugation. We note that $[I]_E^\sigma = [I^\sigma]_{E^\sigma} = [I^\sigma]_E$. In particular, if the conjugate $\overline{I} = I$ then we may conclude that the isogeny $[I]$ is $\mathbb{Q}$-rational.

Now we may illustrate some examples of rational CM points on $Y_0(N)$. Let us assume that $\mathcal{O}$ is a class number one order with $\sqrt{-N} \in \mathcal{O}$. For example, we may take

$$\begin{aligned}\mathcal{O} := \mathcal{O}_K := \mathbb{Z}[\sqrt{-2}], \mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right],\\ \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right], \mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right].\end{aligned}$$

In each case, one has that N is prime. Let $E_{/\mathbb{Q}}$ be an elliptic curve with CM by $\mathcal{O}$. Let $\mathfrak{P} := \sqrt{-N}\mathcal{O}$ be the prime in $\mathcal{O}$ above N. It follows that $\mathcal{O}/\mathfrak{P}$ is cyclic of order N. Furthermore, since $\mathfrak{P} = \overline{\mathfrak{P}}$ we conclude that $[\sqrt{-N}]$ is a $\mathbb{Q}$-rational N-isogeny, whence $(E, [\sqrt{-N}]) \in Y_0(N)(\mathbb{Q})$.

Our construction of rational points on $Y_0(N)$ is a special case of a study on Heegner points. Say that the pair (N, Δ), where $\Delta := f^2\Delta_K$ is a discriminant of an imaginary quadratic order in some $K = \mathbb{Q}(\sqrt{\Delta_K})$, satisfies the *Heegner hypothesis* if every prime $p \mid N$ either splits in $\mathcal{O}_K$, or ramifies in $\mathcal{O}_K$ with $p^2 \nmid N$. In such a case, one can show there must exist an invertible ideal $I \subseteq \mathcal{O} := \mathcal{O}(\Delta)$ of norm N with $\mathcal{O}/I$ cyclic; consequently, one gets an H-rational cyclic N-isogeny, where $H := K(j(E))$ is the

Hilbert class field of K. In our examples above we chose an explicit endomorphism ring $\mathcal{O}$ and ideal I, and showed that $\ker[I]$ is not just H-rational but in fact $\mathbb{Q}$-rational.

Remark. We should emphasize that our examples of rational points on $Y_0(N)$ were *CM points*, i.e., induced by a CM elliptic curve. It is a general philosophy that most modular curves X will have $X(\mathbb{Q})$ consist only of cusps and CM points.

As mentioned earlier, Kenku in [Ken81] concludes that $Y_0(N)(\mathbb{Q}) \neq \emptyset$ precisely when $N \in [1, 10] \cup [12, 19] \cup \{21, 25, 27, 37, 43, 67, 163\}$. What Mazur shows in [Maz78] is the equivalent statement for prime N:

Theorem 3. *If $Y_0(p)(\mathbb{Q}) \neq \emptyset$, then $p = 2, 3, 4, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163$.*

A bit of justification for these primes: that $Y_0(p)(\mathbb{Q}) \neq \emptyset$ for $p \in \{2, 3, 5, 7, 13\}$ follows from the curve $X_0(p)$ having genus zero. For $p \in \{11, 19, 43, 67, 163\}$ one has $Y_0(p)(\mathbb{Q}) \neq \emptyset$ by our discussion on CM above. But for $p = 17, 37$, the verification is a bit different: according to the remarks on isogenies on pp. 78-80 in [BK75], there is a $\mathbb{Q}$-rational 17-isogeny between the two elliptic curves

$$E_1 : y^2 + xy + y = x^3 - 3041x + 64278$$

and

$$E_2 : y^2 + xy + y = x^3 - 190891x - 36002922;$$

this fact was supplied by Vélu. For $p = 37$, one can show that the curve

$$E : y^2 + xy + y = x^3 + x^2 - 8x + 6$$

has a $\mathbb{Q}$-rational 37-isogeny to another curve, and that these two curves give rise to the only two rational points on $Y_0(37)$.[4]

Over the course of these notes we will prove Theorem 3 – which is equivalent to Theorem 1 – and in the process also prove Mazur's Theorem.

4. The algebraic geometry: optimal quotients and potentially good reduction

Recall that for an abelian variety $A_{/K}$, one calls another variety $X_{/K}$ a *quotient* of A if there exists a surjective K-morphism $A \twoheadrightarrow X$. One calls this quotient *optimal* if its kernel is a connected subgroup scheme, i.e., an abelian subvariety.

We let $A_{/K}$ be an abelian variety over e.g. a number field K with ring of integers $\mathcal{O}_K$. Suppose $\mathfrak{p} \subseteq \mathcal{O}_K$ is a prime ideal. Then the fiber/reduction of A mod $\mathfrak{p}$ might not be an abelian variety. For example, if $E_{/\mathbb{Q}}$ is an elliptic curve, then for any prime p dividing the discriminant $\Delta_{E_{/\mathbb{Q}}}$ the reduction of E mod p will not be an elliptic curve; it will have a singularity, and instead its group of nonsingular points will be isomorphic to either $(\mathbb{F}_p, +)$ or $(\mathbb{F}_p^\times, \cdot)$ – the cases of additive and multiplicative reduction, respectively. for the completion $K_\mathfrak{p}$ of K at $\mathfrak{p}$, to say E has bad reduction at $\mathfrak{p}$ is to say that $E_{/K_\mathfrak{p}}$ also

[4] The curve $X_0(37)$ is unique in that it is the only hyperelliptic modular curve of the form $X_0(N)$, and it has a hyperelliptic involution *not* induced by an automorphism of the upper half plane; see p. 450 [Ogg74]. This involution swaps the two rational cusps with the two rational noncuspidal points. These two rational non-cusps are called *exceptional*, as they are exceptions to the general philosophy: they are neither CM points nor cusp points.

has bad reduction at $\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$. We say that $E_{/K}$ has *potentially good reduction at* $\mathfrak{p}$ if there is a finite extension $L/K_\mathfrak{p}$ of local fields such that $E_{K_\mathfrak{p}}$ has good reduction at all primes in $\mathcal{O}_L$ above $\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$. Observe then that the reduction at $\mathfrak{p}$ has to be additive if E has both potentially good reduction and bad reduction at $\mathfrak{p}$, since good and multiplicative reduction are preserved under finite extensions $L/K_\mathfrak{p}$; cf. the Semistable Reduction Theorem, p. 197 [Sil09].

Let $p \geq 5$ be prime, and consider the Jacobian $J_0(p)$ of the modular curve $X_0(p)$; it has a particular quotient $J_0(N)^{\text{new}}$ which fits into an exact sequence

$$0 \to J_0(N)_{\text{old}/\mathbb{Q}} \to J_0(N)_{/\mathbb{Q}} \to J_0(N)^{\text{new}}_{/\mathbb{Q}} \to 0.$$

The abelian subvariety $J_0(N)_{\text{old}/\mathbb{Q}} \leq J_0(N)_{/\mathbb{Q}}$ is defined on p. 138 [Maz78]. Mazur shows the following result about potential good reduction, contingent on the existence of some particular quotient of $J_0(N)^{\text{new}}_{/\mathbb{Q}}$.

Proposition 4 (Corollary 4.3 [Maz78])**.** *Let K be a number field and $N > 0$ a squarefree integer. Let $\mathfrak{q} \subseteq \mathcal{O}_K$ be a prime ideal, say above $q \in \mathbb{Z}$, 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 $f : J_0(N)^{\text{new}}_K \twoheadrightarrow A_K$ such that $f(x)$ has finite order in $A(K)$. Then E has potentially good reduction at $\mathfrak{q}$.

Detailed in [Maz77], there is a specific quotient of $J_0(p)_{/\mathbb{Q}}$ for $p \geq 5$ called the *Eisenstein quotient* which satisfies the above assumption. Denoted $\tilde{J}$, the Eisenstein quotient is also an optimal quotient of $J_0(p)^{\text{new}}$ and its Mordell-Weil group $\tilde{J}(\mathbb{Q})$ is finite. In particular, finiteness of $\tilde{J}(\mathbb{Q})$ implies that the image of any $\mathbb{Q}$-rational point in $J_0(p)$ under this quotient is finite. Furthermore, one has for any prime $q > 2$ that its ramification index is trivially $e_q(\mathbb{Q}/\mathbb{Q}) = 1 < q-1$. Therefore, any noncuspidal rational point $(E, C_p) \in X_0(p)(\mathbb{Q})$ with $p \geq 5$ is such that E has potentially good reduction at q. We summarize this as the following proposition – this is the version we will use in the rest of the paper.

Proposition 5 (Corollary 4.4 [Maz78])**.** *Let $p \geq 5$ be prime. Then any elliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational p-isogeny has potentially good reduction at all primes $q > 2$.*

5. A proof of Mazur's Theorem

Let $E_{/\mathbb{Q}}$ be an elliptic curve with a rational point $P \in E(\mathbb{Q})$ of finite order. By [Kub76], to prove Mazur's Theorem it suffices to show that P cannot have prime order $p \geq 23$. Kubert's justification is as such: for an elliptic curve $E_{/\mathbb{Q}}$, say its $\mathbb{Q}$-torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ is *parametrizable* if the pair $(E, E_{\text{tors}}(\mathbb{Q}))$ is a $\mathbb{Q}$-rational "point" on some modular curve $X(\Gamma)$ of genus zero which parametrizes such torsion structure. For example, if $E_{\text{tors}}(\mathbb{Q})$ is cyclic, then $E_{/\mathbb{Q}}$ is parametrizable $\Leftrightarrow$ $(E, E_{\text{tors}}(\mathbb{Q})) \in X_0(N)$ for some N with $\text{genus}(X_0(N)) = 0$.

Kubert proves (Main result 1 [Kub76]) that if $E_{\text{tors}}(\mathbb{Q})$ is **not** parametrizable, then there is a prime $p \mid \#|E_{\text{tors}}(\mathbb{Q})|$ with $p \geq 23$; in particular, by Cauchy's Theorem one must have a $\mathbb{Q}$-rational point of prime order ≥ 23. Therefore, to prove Mazur's

Theorem it suffices to show that any elliptic curve over $\mathbb{Q}$ does not have a $\mathbb{Q}$-rational p-point for $p \geq 23$, and to note that the parametrizable torsion subgroups are precisely those 15 cases we already know (e.g. p. 217 [Kub76]).

We will now prove Mazur's Theorem. Our proof will actually show that no rational point may have order $p = 11$ or $p \geq 17$.

Remark. Our proof here is essentially Mazur's proof from [Maz78], except rewritten to cite results from [Sil09].

Proof of Mazur's Theorem. For the sake of contradiction, suppose there exists an elliptic curve $E_{/\mathbb{Q}}$ with a rational point $P \in E(\mathbb{Q})$ of some order $p = 11, 17, 23, \ldots$. By Proposition 5, E must have potentially good reduction at $q = 3$. We will now show that all possible reductions of E mod 3 (good, multiplicative and split) cannot happen.

1. E has good reduction at 3: then the set $\tilde{E}(\mathbb{F}_3)$ of nonsingular points mod 3 is an elliptic curve over $\mathbb{F}_3$. Thus, we apply the Hasse-Weil bounds to deduce that $|\#|\tilde{E}(\mathbb{F}_3)| - 3 - 1| \leq 2\sqrt{3}$, and so $\#|\tilde{E}(\mathbb{F}_3)| \leq 7$. On the other hand, Since E has nonsingular reduction mod 3, we have by Prop. 3.1.b ch. 7 [Sil09] $E(\mathbb{Q})[p] \hookrightarrow \tilde{E}(\mathbb{F}_3)$. In particular, a prime order $p \geq 11$ point $P \in E(\mathbb{Q})[p]$ embeds into an order ≤ 7 group.
2. E has multiplicative reduction at 3: by the Semistable Reduction Theorem (Prop. 5.4 ch. 7 [Sil09]), since $E_{/\mathbb{Q}_3}$ has multiplicative reduction, for any finite extension $K/\mathbb{Q}_3$ $E_{/K}$ will also have multiplicative reduction. This contradicts that E has potentially good reduction at 3.
3. E has additive reduction at 3: by Thm. 6.1 ch.7 [Sil09] one has $[E(\mathbb{Q}_3) : E_0(\mathbb{Q}_3)] \leq 4$, where $E_0(\mathbb{Q}_3)$ is the set of points in $E(\mathbb{Q}_3)$ which reduce to a nonsingular point mod 3.[5] If we let $i := [E(\mathbb{Q}_3) : E_0(\mathbb{Q}_3)]$, then since $P \in E(\mathbb{Q}_3)$ this forces iP to be nonsingular mod 3. In particular, we have the reduction $\widetilde{iP} \in \tilde{E}(\mathbb{F}_3)$, where $\tilde{E}(\mathbb{F}_3) \cong (\mathbb{F}_3, +)$ (as per additive reduction). This forces the order of the reduction $\#|\widetilde{iP}| \mid 3$. On the other hand, the order of iP in $E(\mathbb{Q}_3)$ is p, whence the order $\#|\widetilde{iP}| \mid (p, 3) = 1$. This implies that $iP \in E_1(\mathbb{Q}_3)$, where $E_1(\mathbb{Q}_3)$ is the set of points of $E(\mathbb{Q}_3)$ in the kernel of the reduction map. This is impossible, as $E_1(\mathbb{Q}_3)$ has no nontrivial p-torsion (Prop 3.1.a ch. 7 [Sil09]).

□

The next three sections will focus on the proof of the main theorem on rational isogenies of prime degree; these sections will correspond to §5, §6 and §7 in [Maz78].

6. Prime isogenies I: isogeny characters

Let $E_{/K}$ be an elliptic curve over a number field. Let $N > 0$ be an integer, and let $\phi : E \to E'$ be a cyclic K-rational N-isogeny; recall this is equivalent to having a cyclic subgroup $C_N \subseteq E$ of order N which is G_K-rational, with $G_K := \mathrm{Aut}(\overline{K}/K)$

[5] For a local field K and an elliptic curve $E_{/K}$, we call the index $[E_0(K) : E(K)]$ the *Tamagawa number* of E.

the absolute Galois group of K. Fixing a generator P of C_N, one defines the **isogeny character** of ϕ as

$$r : G_K \to (\mathbb{Z}/N\mathbb{Z})^\times \tag{1}$$

by $r(\sigma) := n$ where $\sigma(P) = nP$. Note that the isogeny character is independent of choice of generator for C_N. The isogeny character naturally appears as a factor of the determinant of the mod-N Galois representation of $E_{/K}$:

$$\rho_{E,N} = \begin{bmatrix} r & * \\ 0 & \frac{\chi_N}{r} \end{bmatrix}$$

where $\chi_N : G_K \to (\mathbb{Z}/N\mathbb{Z})^\times$ is the mod-N cyclotomic character of K.[6]

Let us assume $N = p$ is prime with p inert in $\mathcal{O}_K$. Then by class field theory, one has for some unique $0 \leq k < p-1$ a factorization

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

where $\chi_p : G_K \to \mathbb{F}_p^\times$ is the mod p cyclotomic character and $\alpha : G_K \to \mathbb{F}_p^\times$ is some unramified character at $p\mathcal{O}_K$.[7]

Now we also assume that $p \geq 5$. Following Table (5.1) [Maz78], let us set

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

Mazur in Lemma 5.3 [Maz78] shows that α^{2t} is unramified everywhere. In fact, he shows more under an additional assumption of potentially good reduction; this assumption will automatically hold when $K = \mathbb{Q}$ once we assume the existence of an isogeny, see Proposition 5.

Proposition 6 (Proposition 5.1, Lemma 5.3 [Maz78]). *Let K be a number field, and let $E_{/K}$ be an elliptic curve with a K-rational p-isogeny where $p \geq 5$ remains prime in K. If E has potentially good reduction at p, then one has the factorization $r = \alpha \cdot \chi_p^k$, where α^{2t} is unramified everywhere and*

$$k \mod \frac{p-1}{2} = \begin{cases} 0, 1 \\ \frac{1}{2} \text{ (only possible if } p \equiv 3 \pmod 4) \\ \frac{1}{3}, \frac{2}{3} \text{ (only possible if } p \equiv 5 \pmod 6) \end{cases}.$$

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

[6] Recall that for a field K, the *mod-N cyclotomic character* of K is the homomorphism $\chi_N : G_K \to (\mathbb{Z}/N\mathbb{Z})^\times$ such that $\forall \sigma \in G_K, \sigma(\zeta_N) = \zeta_N^{\chi_N(\sigma)}$.

[7] A character $\alpha : G_K \to \mathbb{F}_p^\times$ is *unramified* at $\mathfrak{P} \subseteq \mathcal{O}_K$ if $\alpha(I_\mathfrak{P}) = 1$, where the *inertia subgroup* $I_\mathfrak{P} := \{\sigma \in G_K \mid \sigma \equiv \text{id} \bmod \mathfrak{P}\}$. So an unramified character α at $\mathfrak{P}$ will descend to a homomorphism $\alpha : G_K/I_\mathfrak{P} \to \mathbb{F}_p^\times$.

7. Prime isogenies II: congruences from a p-isogeny

Important Remark. For the rest of these notes, let us assume that K is a number field, $p \geq 5$ is a prime which remains prime in K, and $\mathfrak{Q} \subseteq \mathcal{O}_K$ is a prime with residue characteristic $q \neq p$. We also assume that we have a K-rational p-isogeny (E, C_p) such that E has potentially good reduction both at $\mathfrak{Q}$ and at $p\mathcal{O}_K$. It can be shown that $E_{/K}$ **must have good reduction at $\mathfrak{Q}$,** using similar arguments as those in the proof of Mazur's theorem.

Remark. For $K = \mathbb{Q}$, the assumptions in the above remark are true for a $\mathbb{Q}$-rational p-isogeny (E, C_p) when $p \geq 5$ – in particular, E will have good reduction at all primes $q > 2$; see Proposition 5.

For our elliptic curve (E, C_p), let $\tilde{E}_{/k_{\mathfrak{Q}}}$ denote the reduction of E mod $\mathfrak{Q}$. Since $\mathrm{char}(\mathfrak{Q}) \neq p$ we have the p-torsion of the reduction $\tilde{E}[p] \cong \mathbb{F}_p^2$. One can show that our K-rational p-isogeny C_p descends to a $k_{\mathfrak{Q}}$-rational p-isogeny $\tilde{C_p}$ of $\tilde{E}$, and that its isogeny character is $b_{\mathfrak{Q}}\tilde{\chi}_p^k$, where $\tilde{\chi}_p : \mathrm{Gal}(\overline{k_{\mathfrak{Q}}}/k_{\mathfrak{Q}}) \to \mathbb{F}_p^\times$ is the mod-p cyclotomic character for residue field $k_{\mathfrak{Q}}$, $k \in \mathbb{Z}$ is as in Table 2, and $b_{\mathfrak{Q}}$ is an unramified character.

Let us consider the mod-p Galois representation of $\tilde{E}_{/k_{\mathfrak{Q}}}$:

$$\rho_{\tilde{E},p} = \begin{bmatrix} b_{\mathfrak{Q}}\tilde{\chi}_p^k & * \\ 0 & b_{\mathfrak{Q}}^{-1}\tilde{\chi}_p^{1-k} \end{bmatrix} \in \mathrm{GL}_2(\mathbb{F}_p).$$

Taking the trace of this representation gives

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

Since $\mathrm{Gal}(\overline{k_{\mathfrak{Q}}}/k_{\mathfrak{Q}})$ is infinite cyclic and generated by the Frobenius automorphism $\mathrm{Frob}_{\mathfrak{Q}} := \mathrm{Frob}_q^{f(\mathfrak{Q}|q)}$,[8] the character $\tilde{\chi}_p : \mathrm{Gal}(\overline{k_{\mathfrak{Q}}}/k_{\mathfrak{Q}}) \to \mathbb{F}_p^\times$ is completely determined by its image on $\mathrm{Frob}_{\mathfrak{Q}}$. By definition, $\mathrm{Frob}_{\mathfrak{Q}}$ takes elements α to α^{q_0}, where $q_0 := \#|k_{\mathfrak{Q}}|$. We thus have $\tilde{\chi}_p(\mathrm{Frob}_{\mathfrak{Q}}) = q_0$, and so the image of the trace of Frobenius

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

Furthermore, for the field extension $\mathbb{F}_{q_0^v}/k_{\mathfrak{Q}}$ of degree equal to the order of the character $b_{\mathfrak{Q}}$ – say v – one can show that $\tilde{E}_{/\mathbb{F}_{q_0^v}}$ has trace of Frobenius $q_0^{vk} + q_0^{v-vk} \pmod{p}$. To see this, note that the Frobenius automorphism which generates $\mathrm{Gal}(\overline{\mathbb{F}_{q_0^v}}/\mathbb{F}_{q_0^v})$ is $\mathrm{Frob}_{\mathfrak{Q}}^v$. One then checks that

$$\begin{aligned}\mathrm{Tr}(\rho_{\tilde{E}_{/\mathbb{F}_{q_0^v}},p}(\mathrm{Frob}_{\mathfrak{Q}}^v)) &\equiv b_{\mathfrak{Q}}(\mathrm{Frob}_{\mathfrak{Q}}^v)\tilde{\chi}_p(\mathrm{Frob}_{\mathfrak{Q}}^v)^k + b_{\mathfrak{Q}}(\mathrm{Frob}_{\mathfrak{Q}}^v)^{-1}\tilde{\chi}_p(\mathrm{Frob}_{\mathfrak{Q}}^v)^{1-k} \\ &\equiv q_0^{vk} + q_0^{v(1-k)} \pmod{p}.\end{aligned}$$

These conclusions are summarized as such (see Prop. 6.3, Cor. 6.1 [Maz78]).

Proposition 7. *With notation as in this section, one has that*

a. $b_{\mathfrak{Q}}(\mathrm{Frob}_{\mathfrak{Q}})q_0^k + b_{\mathfrak{Q}}(\mathrm{Frob}_{\mathfrak{Q}})^{-1}q_0^{1-k}$ *is congruent mod* p *to the trace of Frobenius of some elliptic curve* $E_{/\mathbb{F}_{q_0}}$*;*

[8] Here, $\mathrm{Frob}_q : k_{\mathfrak{Q}} \to k_{\mathfrak{Q}}$ is the usual Frobenius automorphism $\alpha \mapsto \alpha^q$; we emphasize that q is prime and different from p.

b. $q_0^{vk} + q_0^{v-vk}$ *is congruent mod* p *to the trace of Frobenius of some elliptic curve* $E_{/\mathbb{F}_{q_0}}$ *computed over* $\mathbb{F}_{q_0^v}$.

Next, we state the result for the case $K = \mathbb{Q}$. We note that the order of α divides 12 as per the tables, and that $q_0 = q$ as we are taking $q_0 := \#|k_{\mathfrak{Q}}|$. To emphasize, q is a prime different from p.

Corollary 8. *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* $\mathbb{F}_{q^{12}}$.

The utility of this corollary is as follows. If we are given an elliptic curve $E_{/\mathbb{Q}}$ with a rational p-isogeny where $p \geq 5$, then E has good reduction at all odd primes q. For each such $q \neq p > 2$, the reduction $\tilde{E}_{/\mathbb{F}_q}$ is such that the trace of Frobenius w.r.t. the p-torsion is

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

Noting that the order of b_q divides 12, we pass to $\mathbb{F}_{q^{12}}$ and see that

$$\mathrm{Tr}(\rho_{\tilde{E}_{/\mathbb{F}_{q^{12}}},p}(\mathrm{Frob}_{q^{12}})) \equiv q^{12k} + q^{12(1-k)} \pmod{p}.$$

The trace of Frobenius $\mathrm{Tr}(\rho_{\tilde{E},p})$ for each case $\tilde{E}_{/\mathbb{F}_{q^n}}$ $n \geq 1$ is an integer in $\mathbb{Z}$, and is independent of p; we recall (e.g. Rmk. 2.6 [Sil09]) that the trace of Frobenius over $\mathbb{F}_{q^n}$ is

$$\mathrm{Tr}(\rho_{\tilde{E}_{/\mathbb{F}_{q^n}},p}(\mathrm{Frob}_{q^n})) = 1 + q^n - \#\tilde{E}(\mathbb{F}_{q^n}).$$

In particular, having a rational p-isogeny $(E_{/\mathbb{Q}}, C_p)$ means that for all odd $q \neq p$ we have an integer $a(\mathbb{F}_{q^{12}}/\mathbb{F}_q) := 1 + q^{12} - \#\tilde{E}(\mathbb{F}_{q^{12}})$ such that

$$a(\mathbb{F}_{q^{12}}/\mathbb{F}_q) \equiv q^{12k} + q^{12(1-k)} \pmod{p} \tag{3}$$

with restrictions on k as in Proposition 6. Therefore, we may determine all elliptic curves over $\mathbb{F}_q$ – of which there are finitely many – and then their traces of Frobenius over $\mathbb{F}_{q^{12}}$; then, in each case of k we compute $q^{12k} + q^{12(1-k)}$, and check for which p the congruence in (3) is satisfied. In particular, only finitely many p may satisfy (3) for any one q. After building a small set of p from checking (3) for a few q, we will investigate each unexpected p a bit closer. This will be done in the proof of the main theorem on rational prime isogenies.

Here is some pseudocode for a function that will compute the possible traces of Frobenius over $\mathbb{F}_{q^{12}}$ for any elliptic curve defined over $\mathbb{F}_q$.

```
//The following function computes all possible traces of Frobenius over
F_{q_0^v} for an elliptic curve defined over F_{q_0}.

a:=function(q0,v)
        EC:=[];
        for a1,a2,a3,a4,a6 in [0..q0-1] do
                b2 := a1 ^ 2 + 4 * a2;
                b4 := 2 * a4 + a1 * a3;
                b6 := a3 ^ 2 + 4 * a6;
                b8 := a1 ^ 2 * a6 + 4 * a2 * a6 - a1 * a3 * a4
                + a2 * a3 ^ 2 - a4 ^ 2;
                Disc := -b2^2 * b8 - 8 * b4^3 - 27 * b6^2
                + 9 * b2 * b4 *b6;
                if Disc mod q0 ne 0 then
                        Append(~EC, [a1,a2,a3,a4,a6]);
                end if;
        end for;
        trace:=[];
        for curve in EC do
                E:=EllipticCurve([GF(q0^v)!curve[1],curve[2],curve[3],
                curve[4],curve[5]]);
                aE:=q0^v+1-#E;
                if (aE in trace) eq false then
                        Append(~trace,aE);
                end if;
        end for;
return trace;
end function;
```

For example, with this code we compute $a(\mathbb{F}_{2^{12}}/\mathbb{F}_2) = \pm 128, -47$, $a(\mathbb{F}_{3^{12}}/\mathbb{F}_3) = 1458, 658, -1358$, and $a(\mathbb{F}_{5^{12}}/\mathbb{F}_5) = 31250, 23506, -25774, -28334$. To drive home the utility of Corollary 8, let us do one example: suppose we have a $\mathbb{Q}$-rational p-isogeny $(E_{/\mathbb{Q}}, C_p)$ with $p \geq 5$. Then by Proposition 5, E will have potentially good reduction at $q = 3$, and by the remark at the beginning of this section E will in fact have good reduction at $q = 3$. The trace of Frobenius for $\tilde{E}_{/\mathbb{F}_3}$ computed over $\mathbb{F}_{3^{12}}$ must lie in $\{1458, 658, -1358\}$, and by Corollary 8 one must then have

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

Going through each of the cases for k, we can check which p will satisfy this congruence – we will do this in the proof of the main theorem. As we will see, this set of p isn't always reasonable!

8. Prime isogenies III: the proof

We will now prove the main theorem of the paper, restated here.

Theorem (On rational isogenies of prime degree)**.** *Let prime $p \in \mathbb{Z}$ be such that the genus of $X_0(p)$ is positive (i.e., $p = 11$ or $p \geq 17$). Then $Y_0(p)(\mathbb{Q}) = \emptyset$ except when $p = 11, 17, 19, 37, 43, 67, 163$; equivalently, for prime $p \geq 23$ there are no elliptic curves over $\mathbb{Q}$ which possess $\mathbb{Q}$-rational p-isogenies unless $p = 37, 43, 67, 163$.*

Proof. Suppose that $Y_0(p)(\mathbb{Q}) \neq \emptyset$ with $p = 11$ or $p \geq 17$; let $E_{/\mathbb{Q}}$ be an elliptic curve with a $\mathbb{Q}$-rational p-isogeny C_p. by Proposition 5 and the remark at the start of Section 7, E has good reduction at all primes $q \geq 3$. In particular, E has good reduction at $q := p$, and thus the isogeny character of C_p has the form $r = \alpha \cdot \chi_p^k$, where α has order dividing 12 and k may only be $0, 1, \frac{1}{2}, \frac{1}{3}$, or $\frac{2}{3}$ mod $\frac{p-1}{2}$; see Proposition 6.

The canonical involution $\omega := \omega_p : X_0(p) \to X_0(p)$ is $\mathbb{Q}$-rational[9], and since it interchanges k and $1-k$ we need only to consider the cases $k \equiv 0, \frac{1}{2}, \frac{1}{3} \bmod \frac{p-1}{2}$. By twisting with quadratic characters, we may assume $k \equiv 0, 3k \equiv 1$, and $2k \equiv 1 + \frac{p-1}{2}$ mod $p-1$ in the respective cases above.

(1) $k \equiv 0 \pmod{p-1}$: by Corollary 8.b. with $q = 3$, we then must have

$$1 + 3^{12} \equiv a(\mathbb{F}_{3^{12}}/\mathbb{F}_3) \pmod{p}$$

with $a(\mathbb{F}_{3^{12}}/\mathbb{F}_3) \in \{1458, 658, -1358\}$. It is now a simple computation to check which p satisfy such a congruence relation. For example, we may use the following pseudocode to find such p.

```
case1:=1+3^(12);
admissablePrimes:=[];
traceList:=[658,-1358,1458];
UpperBd:=Max([case1,658,-1358,1458]);
for prime p in [2..UpperBd] do
        found:=false;
        for trace in traceList do
                if (case1 mod p) eq (trace mod p) then
                        found:=true;
                end if;
                if found eq true then
                        if (p in admissablePrimes) eq false then
                                Append(~admissablePrimes, p);
                        end if;
                end if;
        end for;
end for;
admissablePrimes;
```

We find that the only such primes are $p = 2, 3, 5, 7, 13, 19, 37, 97$. The only prime we do not have an example of a rational point on $Y_0(p)$ for is $p = 97$. To rule this number out, we take $q = 5$ and mimic the previous computations, using $a(\mathbb{F}_{5^{12}}/\mathbb{F}_5) = 31250, 23506, -25774, -28334$ and check which p satisfy $1 + 5^{12} \equiv a(\mathbb{F}_{5^{12}}/\mathbb{F}_5) \pmod{p}$. Doing this shows us that precisely the primes

$$p = 2, 3, 5, 7, 13, 17, 31, 37, 61, 157, 229$$

satisfy such a congruence relation. The absence of $p = 97$ in this second list implies that $Y_0(97)(\mathbb{Q})$ is empty, as per Proposition 5.

(2) $3k \equiv 1 \pmod{p-1}$: Corollary 8.b. with $q = 3$ shows us that

$$3^4 + 3^8 \equiv a(\mathbb{F}_{3^{12}}/\mathbb{F}_3) \pmod{p}$$

with $a(\mathbb{F}_{3^{12}}/\mathbb{F}_3) \in \{1458, 658, -1358\}$. Modifying our previous code, computations tell us that $p = 2, 3, 5, 11, 17$. We already know of $\mathbb{Q}$-rational p-isogenies for each of these values.

(3) $2k \equiv 1 + \frac{p-1}{2} \pmod{p-1}$: in this case, our initial congruence relation becomes

$$2 \cdot 3^6 \equiv a(\mathbb{F}_{3^{12}}/\mathbb{F}_3) \pmod{p},$$

[9] See *Atkin-Lehner involution.* In particular, ω is defined on $X_0(p)$ by $(E, C_p) \mapsto (E/C_p, E[p]/C_p)$.

which unfortunately works for 231 distinct primes. On the other hand, taking $q = 5$ gives us 3368 distinct p. We must use a different method to tackle this problem.

Following Mazur, we will break this case up into arguments involving elementary algebraic number theory. First, one can show that for any prime $2 < r < \frac{p}{4}$ one must have $\left(\frac{r}{p}\right) = -1$, e.g. r is not a square mod p. Using this, we will show that $\mathbb{Q}(\sqrt{-p})$ must have class number one, and thus $p \in \{11, 19, 43, 67, 163\}$ – which we have examples for, as per the CM points we described in Section 3.

To argue that $K := \mathbb{Q}(\sqrt{-p})$ has class number one, we first note that $p \equiv 3 \pmod 4$ and thus $\Delta_{K/\mathbb{Q}} = -p$. As we have noted, for odd $r < \frac{p}{4}$ we have $\left(\frac{r}{p}\right) = -1$; thus, such r must stay inert in K. We conclude that any prime ideal of odd norm $< \frac{p}{4}$ is principal, as the prime they lie above must stay inert in $\mathcal{O}_K$. For example, if $\mathfrak{R} \subseteq \mathcal{O}_K$ is such a prime, say $(r) = \mathfrak{R} \cap \mathbb{Z}$; then $r \mid N\mathfrak{R} < \frac{p}{4}$ implies r is inert in $\mathcal{O}_K$, and thus $r\mathcal{O}_K = \mathfrak{R}$. From this, we may conclude that all ideals of odd norm $< \frac{p}{4}$ are principal.

Next, we note that Minkowski's bound here is

$$M_K = \frac{2\sqrt{p}}{\pi},$$

hence every ideal class $A \in \mathrm{Cl}(\mathcal{O}_K)$ contains an ideal I of norm $N(I) < \frac{2\sqrt{p}}{\pi}$. Since $M_K < \frac{p}{4}$ for $p \geq 11$, we conclude that all ideal classes contain an ideal of norm $< \frac{p}{4}$. This does not imply that such an ideal is principal, as the ideal may have even norm. Thus, we are left to show that any prime ideal of norm 2 is principal, which is a simple case check for p mod 16. □

9. What's next: K-rational isogenies of prime degree

In the final section of his paper, Mazur [Maz78] proves a result for isogenies defined over imaginary quadratic fields, analogous to his main theorem.

Theorem 9. *Let K be an imaginary quadratic field. Then for all but finitely many primes $p \in \mathbb{Z}$ which remain inert in K, there are no elliptic curves defined over K with a K-rational p-isogeny, i.e., $Y_0(p)(K) = \emptyset$.*

Here is a sketch of the proof. First, Mazur shows in a previous paper [Maz76] that for an imaginary quadratic field K, for all but finitely many primes $p \in \mathbb{Z}$ if p stays inert in K then $J_0(p)$ has a nontrivial optimal quotient A with finite Mordell-Weil group $A(K)$. In particular, consider an elliptic curve $E_{/K}$ with a K-rational p-isogeny C_p, for such an inert prime p. For any prime $\mathfrak{q} \subseteq \mathcal{O}_K$ with ramification index $e_{\mathfrak{q}}(K/\mathbb{Q}) < q - 1$ (where q is the prime below $\mathfrak{q}$) one has by Proposition 4 that E has potentially good reduction at $\mathfrak{q}$; thus, E will have potentially good reduction at all primes above an odd prime if 3 does not ramify in K, else above all primes of characteristic ≥ 5.

Mazur then proceeds to argue what the Frobenius automorphism under the isogeny character for a K-rational p-isogeny may look like, using Propositions 6 and 7.b. This involves a lot of algebraic number theory calculations for the different cases of exponent k.

References

[BK75] B. J. Birch and W. Kuyk, *Modular functions of one variable*, IV, Lecture notes in Math., Vol. 476, Springer-Verlag, Berlin and New York (1975), 78–80.

[Con] K. Conrad, *The Conductor Ideal.* `https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf`.

[DR73] P. Deligne and M. Rapoport, *Les schmas de modules de courbes elliptiques.* Modular functions of one variable, II, Lecture notes in Math., vol. 349, Springer, Berlin and New York (1973), 143–316.

[Ken81] M. A. Kenku,*On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*. J. London Math. Soc. (2) 23 (1981), 415–427.

[Kub76] D. Kubert, *Universal bounds on the torsion of elliptic curves.* Proc. London Math Soc. (3) **33** (1976), 193–237.

[Maz76] B. Mazur, *Rational points on modular curves*, *Modular functions of one variable*, V, Lecture notes in Math., Vol. 601 (1977), 107–148.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal.* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977).

[Maz78] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. Vol. 44 (1978), 129–162.

[Me96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. 124 (1996), 437–449.

[Ogg74] A. Ogg, *Hyperelliptic modular curves.* Bull. Soc. Math. France 102 (1975), 449-462.

[Ogg75] A. Ogg, *Diophantine equations and modular forms.* Bull. Amer. math. soc. 81 (1975), 14–27.

[Sil94] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151, Springer, 1994.

[Sil09] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer, 2009.