Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Master in Advanced Mathematics and Mathematical Engineering

Master's thesis

Elliptic Curves and Mazur's Theorem

Marta Herrerias Medina

Supervised by Joan Carles Lario

June, 2020

Thanks to my supervisor, Joan-Carles Lario, for providing guidance and feedback throughout this project. I also want to thank my friends and family for their constant support.

Abstract

This paper gives a sketch of proof of Mazur's Theorem classifying the possible rational torsion subgroups of elliptic curves defined over $\mathbb{Q}$. We will prove Mazur's theorem by using two main lemmas. The sketch of proof of these two lemmas will be the goal of all the work. We will provide the tools needed to understand the proofs, trying to make the work as self-contained as possible although we must avoid some technical parts. We will present the basic notions of the theory of elliptic curves, discuss about Weierstrass equations, the Mordell-Weil group, isogenies, endomorphisms, the basics of the theory of group schemes, Néron models for elliptic curves, and modular curves.

Keywords

Elliptic Curves, Isogenies, Ramified and Unramified Extensions, Galois Modules, Néron Models, Group Schemes, Modular Curves

Contents

1. Introduction

The study of elliptic curves has been an area of great interest to mathematicians since long ago. From the arithmetic point of view, one of the most important theorems in that area is the theorem of Mazur that describes the possible subgroups of rational torsion points in the Mordell-Weil group of the elliptic curves defined over $\mathbb{Q}$.

Let E be an elliptic curve over $\mathbb{Q}$. The Mordell-Weil group $E(\mathbb{Q})$ is a finitely generated (abelian) group. Hence we can write

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}\,.$$

The positive integer r is called the rank of $E(\mathbb{Q})$. A formula for this rank is given by the conjecture of Birch and Swinnerton-Dyer, whose solution rewards the Clay Institute of Mathematics with a million dollars. As for the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$, Barry Mazur proved the following elegant theorem (twice, in 1977 and 1978, referenced in [16] and [18], respectively).

Theorem 1.1. (Mazur). *Let E be an elliptic curve over $\mathbb{Q}$. The possible torsion subgroups of $E(\mathbb{Q})$ are:*

(1) $\mathbb{Z}/N\mathbb{Z}$, *where* $1 \leq N \leq 10$ *or* $N = 12$;

(2) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}$, *where* $N = 1, 2, 3, 4$.

It is known that all the above 15 groups do arise for infinitely many elliptic curves over $\mathbb{Q}$. The reason for that is that the corresponding modular curves have genus zero. Modular curves are algebraic curves whose points classify elliptic curves with torsion level structures. They are an essential tool in the more delicate and key point of Mazur's proof.

Our goal in this memory is to discuss Mazur's proof that elliptic curves over $\mathbb{Q}$ cannot have torsion points of prime order larger than 13. The complete details of the proof are far beyond our scope but we will try to make an sketch of the proof as self-contained as possible. However, there are aspects that we can just mention, because of the difficulty involved in proving some concepts and others, simply, because it is assumed that the reader is aware of these results. In terms of prerequisites, we assume that the reader has a graduate level understanding of most mathematical fields. In particular, we freely use without mention fundamental results from algebraic geometry, algebraic number theory, and Galois theory.

The plan is as follows. In Section 2, we begin directly with the proof of Mazur's theorem based on two lemmas. The remainder of the memory is devoted to understand and sketch a proof of these two lemmas. In Section 3, we present the basic notions of the theory of elliptic curves, where we focus on those results which will be needed in the proof of Mazur's Theorem. For example, we discuss about Weierstrass equations, the Mordell-Weil group, isogenies and endomorphisms. In Sections 4 and 5 we will give the necessary requirements for the proofs of the lemmas 2.2 and 2.3, respectively. We develop the basics of the theory of group schemes, Néron models for elliptic curves and modular curves.

Finally, we include an appendix that contains some final remarks: the case $N = 11$, the Lutz-Nagell theorem, examples of elliptic curves with different torsion subgroups over $\mathbb{Q}$ and generalizations of Mazur's theorem.

2. Mazur's theorem

Our goal in this section is to give a sketch of the proof of the following result:

Theorem 2.1. (Mazur). *Let $E/\mathbb{Q}$ be an elliptic curve, and suppose that $P \in E(\mathbb{Q})_{\text{tors}}$ is a point of prime order p. Then $p \leq 13$.*

In a manner similar to Alfred Hitchcock's movie *Dial M for Murder*, we shall present the proof first, and then we will describe the main characters involved in the proof. To this end, one reduces the Theorem to the following two lemmas.

Lemma 2.2. *Let $E/\mathbb{Q}$ be an elliptic curve with a point $P \in E(\mathbb{Q})_{\text{tors}}$ of odd prime order p. Then E is isogenous over $\mathbb{Q}$ to an elliptic curve $E'/\mathbb{Q}$ such that: (i) E' has also a point of order p in $E'(\mathbb{Q})_{\text{tors}}$, and (ii) the extension $\mathbb{Q}(E'[p])/\mathbb{Q}(\mu_p)$ is ramified.*

Lemma 2.3. *Let $E/\mathbb{Q}$ be an elliptic curve with a point $P \in E(\mathbb{Q})_{\text{tors}}$ of prime order $p > 13$. Then the extension $\mathbb{Q}(E[p])/\mathbb{Q}(\mu_p)$ is unramified.*

Here, $\mathbb{Q}(\mu_p)$ denotes the p-th cyclotomic field. Before we start with the proof of the above lemmas, it is worth to consider the following example that illustrates them. It concerns with the rational isogeny class of the *first* elliptic curve of conductor 11. This class contains three elliptic curves:

E	Weierstrass equation	j_E
$11A$	$y^2 + y = x^3 - x^2 - 10x - 20$	$-2^{12}31^3/11^5$
$11B$	$y^2 + y = x^3 - x^2$	$-2^{12}/11$
$11C$	$y^2 + y = x^3 - x^2 - 7820x - 263580$	$-2^{12}29^3809^3/11$

We take the prime $p = 5$ and want to check that Lemma 2.2 holds, but Lemma 2.3 does not apply since $p < 13$. The rational torsion 5-points of these curves are as follows:

E	$E(\mathbb{Q})[5]$
$11A$	$(0:1:0), (5:-6:1), (5:5:1), (16:-61:1), (16:60:1)$
$11B$	$(0:1:0), (0:-1:1), (0:0:1), (1:-1:1), (1:0:1)$
$11C$	$(0:1:0)$

Both lemmas focus in the relative extension $\mathbb{Q}(E[p])/\mathbb{Q}(\mu_p)$. With the help of Sage one finds:

E	$\text{disc}(\mathbb{Q}(E[p])/\mathbb{Q}(\mu_p))$	$\mathbb{Q}(E[p])/\mathbb{Q}(\mu_p)$
$11A$	(1)	unramified
$11B$	$\mathfrak{P}_{11}'^4\mathfrak{P}_{11}''^4\mathfrak{P}_{11}'''^4\mathfrak{P}_{11}''''^4$	ramified
$11C$	$\mathfrak{P}_5^8\mathfrak{P}_{11}'^4\mathfrak{P}_{11}''^4\mathfrak{P}_{11}'''^4\mathfrak{P}_{11}''''^4$	ramified

We can apply Lemma 2.2 to E=11A or E=11B since they have a rational 5th torsion point. The corresponding E' is 11B in both cases. The conclusion of Lemma 2.3 is true for E =11A but

it is false for E=11B (recall we have $p = 5 < 13$). We cannot apply neither Lemma 2.2 or Lemma 2.3 to E =11C since it does not have a rational 5-torsion point.

Our next task is to give the proof of Lemma 2.2. To this end, we shall need to make use of the following tools: the Weil paring, the finiteness of the elliptic curves in a rational isogeny class and the Hilbert class field of cyclotomic extensions (see Section 4).

Proof. (of Lemma 2.2) Suppose, for contradiction, that all the elliptic curves in the rational isogeny class of E having a rational p-torsion point contain a Galois submodule isomorphic to μ_p; that is, the attached exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E'[p] \longrightarrow \mu_p \longrightarrow 0$$

splits (see Section 4.2) for all the elliptic curves E' rationally isogenous to E with a rational p-torsion point.

Let $E_1 = E$. To the attached Galois submodule of $E_1[p]$ isomporphic to μ_p, it corresponds a rational isogeny

$$E_1 \longrightarrow E_2$$

with kernel μ_p (see Section 3.4). The image of the Galois submodule isomorphic to $\mathbb{Z}/p\mathbb{Z}$ gives rise to a point of order p in $E_2(\mathbb{Q})$. By assumption, E_2 also has a Galois submodule isomorphic to μ_p. Then we can repeat the process, and we obtain a sequence of rational isogenies

$$E_1 \longrightarrow E_2 \longrightarrow E_3 \longrightarrow \ldots$$

where every elliptic curve has a rational p-torsion point and a Galois submodule isomorphic to μ_p. Since the rational isogeny graph is finite (see Section 3.4), one must have some E_j isomorphic to E_i for some $j > i$. Composing the corresponding isogenies and this isomorphism, we get an endomorphism

$$f : E_i \longrightarrow E_i \, .$$

Observe that $E_i(\mathbb{Q})$ has point of order p and this point does not belong to $\mathrm{Ker}(f)$ by construction. Since f is defined over $\mathbb{Q}$, it should be an scalar (see Proposition 3.12) and this gives a contradiction since $\deg f$ is a power of p.

By the previous paragraph, there exists an elliptic curve $E'/\mathbb{Q}$ in the rational isogeny class of E such that it contains a rational p-torsion point and the corresponding exact sequence does not split. In other words, the Galois representation attached to $E'[p]$ looks like

$$\varrho_{E',p} \simeq \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$$

with $* \neq 0$. Let $K = \mathbb{Q}(E'[p])$. We claim that the extension $K/\mathbb{Q}(\mu_p)$ is ramified.

Indeed, the representation $\varrho_{E',p}$ factors through $\mathrm{Gal}(K/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$, and the image of the subgroup $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$ is the group consisting of the matrices

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

for k in $\mathbb{F}_p$. Since

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & k' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+k' \\ 0 & 1 \end{pmatrix} ,$$

the extension $K/\mathbb{Q}(\mu_p)$ is abelian. Suppose, for contradiction, that $K/\mathbb{Q}(\mu_p)$ is unramified. Then, K must be contained in the Hilbert class field (see Section 4.3) of $\mathbb{Q}(\mu_p)$. In fact, since $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$ has order p and the conjugation of $(\mathbb{Z}/p\mathbb{Z})^* \simeq \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ on $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$ is given by

$$\begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} 1 & k/a \\ 0 & 1 \end{pmatrix}$$

one realizes that K corresponds to the Herbrand subgroup $Y^{-1} = Y^{p-2}$ (see Section 4.3). But if this subgroup is non-trivial, then by the Herbrand theorem (theorem 4.3) we have that the Bernoulli number $B_2 = 1/6$ has numerator divisible by p which is impossible. Thus, necessarily $K/\mathbb{Q}(\mu_p)$ is a ramified extension. □

The next step is to prove Lemma 2.3. For this proof we will use the theory of the Néron models and deep properties of the Jacobian of the modular curve $X_0(N)$, for N prime, as well as some other concepts that you can find in Section 5.

Proof. (of Lemma 2.3). Suppose that $E/\mathbb{Q}$ is an elliptic curve with a point $P \in E(\mathbb{Q})_{\mathrm{tors}}$ of prime order $p > 13$. Denote $K = \mathbb{Q}(E[p])$. We want to show that $K/\mathbb{Q}(\mu_p)$ is unramified. By the Néron-Ogg-Safarevich criterion (see proposition 5.6), we know that $K/\mathbb{Q}(\mu_p)$ is unramified at all primes of $\mathbb{Q}(\mu_p)$ lying over rational primes of good reduction for E, except possibly those primes lying over p. Thus, we need to analyze the (eventual) ramification at primes lying over q at which E has bad reduction and the primes lying over p (whether E has bad or good reduction at p). The strategy is to construct a split exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0$$

of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p))$-modules. The point P provides the kernel submodule $\mathbb{Z}/p\mathbb{Z}$ with trivial action. To obtain the complementary submodule μ_p we shall make use of the Néron model of E.

First, we fix a prime q of bad reduction, and let $\mathcal{E}$ be the Néron model for E over $\mathbb{Z}_q$ (see section 5.2). Let $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{E}$ be the constant finite flat subgroup scheme generated by P. Consider the special fiber $\mathcal{E}/\mathbb{F}_q$ of the Néron model and the short exact sequence

$$0 \longrightarrow \mathcal{E}^0_{/\mathbb{F}_q} \longrightarrow \mathcal{E}_{/\mathbb{F}_q} \longrightarrow \Phi_p \longrightarrow 0$$

where $\mathcal{E}^0$ is the *identity component* and Φ_q is the group of components.

We claim that $\mathcal{E}^0_{/\mathbb{F}_q}[p]$ is nontrivial. Indeed, by lemma 5.9 we know that E has multiplicative reduction at q, and therefore $\mathcal{E}^0$ is isomorphic to $\mathbb{G}_m$ over $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$. The multiplicative group $\mathbb{G}_m(\overline{\mathbb{F}}_q) = \overline{\mathbb{F}}_q^*$ has points of all orders relatively prime to q (a different argument using the Tate curve is needed in the case $q = p$). On the other hand, since $p > 13$, we have $\mathbb{Z}/p\mathbb{Z} \not\subset \mathcal{E}(\mathbb{F}_q)^0$ by the crucial lemma 5.14 (it is precisely here where the modular curves play a role!) From the exact sequence

$$0 \longrightarrow \mathcal{E}^0(\overline{\mathbb{Q}}_q) \longrightarrow \mathcal{E}(\overline{\mathbb{Q}}_q) \longrightarrow \mathcal{E}(\overline{\mathbb{Q}}_q)/\mathcal{E}^0(\overline{\mathbb{Q}}_q) \longrightarrow 0$$

we obtain the desired (nontrivial) complementary submodule. Note that

$$\mathcal{E}^0_{/\mathbb{F}_q}[p] = \mathcal{E}^0(\overline{\mathbb{Q}}_q)[p]^{I_q} \subseteq \mathcal{E}(\overline{\mathbb{Q}}_q)[p] = E(\overline{\mathbb{Q}}_q)[p]$$

where $I_q = \mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q^{\mathrm{nr}})$ is the inertia group at q.

Finally, we need to show that the extension $K/\mathbb{Q}(\mu_p)$ is unramified over the primes lying over p whenever E has good reduction at p. To do this, we consider again the short exact sequence of $\mathbb{Z}_p$-group schemes

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E[p] \longrightarrow \mu_p \longrightarrow 0.$$

Over $\overline{\mathbb{F}}_p$ the group $\mathbb{Z}/p\mathbb{Z}$ is completely disconnected, while μ_p collapses to a point. Applying the connected component of the identity functor shows that $E[p]^0 = \mu_p$, and this exact sequence must also split. We conclude that $\mathbb{Q}(E[p])$ is unramified over $\mathbb{Q}(\mu_p)$ also at all primes lying over p, and this completes the proof. □

2.1 Proof of Mazur's Theorem

The proof of Mazur's Theorem follows immediately from lemma 2.2 and lemma 2.3.

Proof. Suppose that $E(\mathbb{Q})$ has a torsion point P of prime order p. By lemma 2.2, E is isogenous over $\mathbb{Q}$ to an elliptic curve $E'/\mathbb{Q}$ such that E' has also a point of order p in $E'(\mathbb{Q})_{\text{tors}}$ and $\mathbb{Q}(E'[p])/\mathbb{Q}(\mu_p)$ is ramified. Now, by lemma 2.3, the relative extension $\mathbb{Q}(E'[p])/\mathbb{Q}(\mu_p)$ is unramified since $p > 13$. Therefore, we get a contradiction and p must be less or equal than 13. □

3. Elliptic curves: basic facts

In this section we give a brief introduction to the theory of elliptic curves: Weierstrass equations, Mordell-Weil group, isogenies, and endomorphisms. Throughout, our primary references are the two books by Silverman [4] and [5].

Definition 3.1. An elliptic curve (E, O_E) over a field K is a smooth, projective curve E of genus 1 along with a specified point O_E, all defined over K.

In practise we will simply talk about the elliptic curve E/K, and O_E will be understood to be the base point. Further, as is standard practise we use the notation $E(K')$ to denote the set of points of E defined over K' for any field extension K' of K.

3.1 Weierstrass equations

Let K be an arbitrary field. A Weierstrass equation for an elliptic curve E/K is an equation of the form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where a_1, a_2, a_3, a_4, a_6 are constants in K. As consequence of the Riemann-Roch theorem, all elliptic curves admit Weierstrass models in the projective plane $\mathbb{P}^2(K)$.

If $\text{char}(K) \neq 2$, then we can simplify the equation by completing the square. The substitution

$$y \mapsto \frac{1}{2}(y - a_1x - a_3)$$

gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where

$$b_2 = a_1^2 + 4a_4$$
$$b_4 = 2a_4 + a_1a_3$$
$$b_6 = a_2^2 + 4a_6\,.$$

We also define quantities

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta, \\ \omega &= \frac{dx}{2y + a_1x + a_3} \cdot \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}. \end{aligned}$$

Definition 3.2. The quantity Δ is the discriminant of the Weierstrass equation, the quantity j is the j-invariant of the elliptic curve, and ω is the invariant differential associated to the Weierstrass equation.

Assuming now that the characteristic of K is not 2 or 3, our elliptic curves have Weierstrass equations of the form $E : y^2 = x^3 + Ax + B$. In that case, we have

$$\Delta = -16(4A^3 + 27B^2) \quad \text{and} \quad j = -1728\frac{(4A^3)}{\Delta}.$$

Since elliptic curve are non-singular curves, their Weierstrass equations satisfy $\Delta \neq 0$. However, we shall need to consider their reductions at certain places and then we obtain Weierstrass equations corresponding to cubic curve that can have singularities. Now, we shall analyze the possible singularities of a cubic curve: nodes and cusps. To this end, we consider a general situation. Let $P = (x_0, y_0)$ be a point satisfying a Weierstrass equation

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0,$$

and assume that P is a singular point on the curve $f(x, y) = 0$. Then we have

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

It follows that there are α, β in a separable algebraic closure $\overline{K}$ of K such that the Taylor series expansion of $f(x, y)$ at P has the form

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3.$$

Definition 3.3. The singular point P is a node if $\alpha \neq \beta$. In this case, the lines

$$y - y_0 = \alpha(x - x_0) \quad \text{and} \quad y - y_0 = \beta(x - x_0)$$

are the tangent lines at P. On the other hand, if $\alpha = \beta$, then we say that P is a cusp, in which case the tangent line at P is given by $y - y_0 = \alpha(x - x_0)$.

Proposition 3.4. *The following statements hold:*

(a) A cubic curve given by a Weierstrass equation satisfies:

(i) It is nonsingular if and only if $\Delta = 0$.

(ii) It has a node if and only if $\Delta = 0$ *and* $c_4 \neq 0$.

(iii) It has a cusp if and only if $\Delta = c_4 = 0$.

In cases (ii) and (iii), there is only the one singular point.

(b) Two elliptic curves are isomorphic over $\overline{K}$ *if and only if they both have the same j-invariant.*

(c) Let $j_0 \in \overline{K}$. *There exists an elliptic curve defined over* $K(j_0)$ *whose j-invariant is equal to* j_0.

Proof. See [4] (page 45). □

Let E be an elliptic curve defined over a number field K and let $\mathfrak{P}$ be a prime of the ring of integers of K. From the previous discussion, the reduced curve $\tilde{E}$ mod $\mathfrak{P}$ is of one of three types:

Definition 3.5. (a) E has good (or stable) reduction if $\tilde{E}$ is nonsingular.

(b) E has multiplicative (or semistable) reduction if $\tilde{E}$ has a node.

(c) E has additive (or unstable) reduction if $\tilde{E}$ has a cusp.

In cases (b) and (c) we say that E has bad reduction. If E has multiplicative reduction, then the reduction is said to be split if the slopes of the tangent lines at the node are in the residue field of $\mathfrak{P}$, and otherwise it is said to be nonsplit.

The following two results play an important role in the proof of Mazur's theorem.

Proposition 3.6. *Let* $E/\mathbb{F}_q$ *be an elliptic curve. Then there exists* $\alpha \in \mathbb{C}$ *with* $|\alpha| = \sqrt{q}$ *so that for all positive integers n the curve* $E(\mathbb{F}_{q^n})$ *contains exactly* $q^n - \alpha^n - \overline{\alpha}^n + 1$ *points.*

Proof. See [1], page 11. □

Proposition 3.7. *Let* $E/\mathbb{Q}_p$ *be an elliptic curve for some prime p, and suppose that E has additive reduction at the maximal ideal of* $\mathbb{Z}_p$. *Then there exists an extension field* $K/\mathbb{Q}_p$ *with ring of integers* $\mathcal{O}$ *so that* E/K *has either good or multiplicative reduction at the maximal ideal of* $\mathcal{O}$. *Furthermore, one can choose K to have absolute ramification index at most six over* $\mathbb{Q}_p$.

Proof. See [10], chapter 2. □

3.2 Mordell-Weil theorem

Let A be an abelian variety defined over a field K. Then, the set of K-rational points $A(K)$ has structure of an abelian group. In the case of abelian varieties of dimension one (that is, elliptic curves) it is a classical fact that one can make completely explicit the addition law on points through algebraic expressions from the Weierstrass equations (see section 3.3).

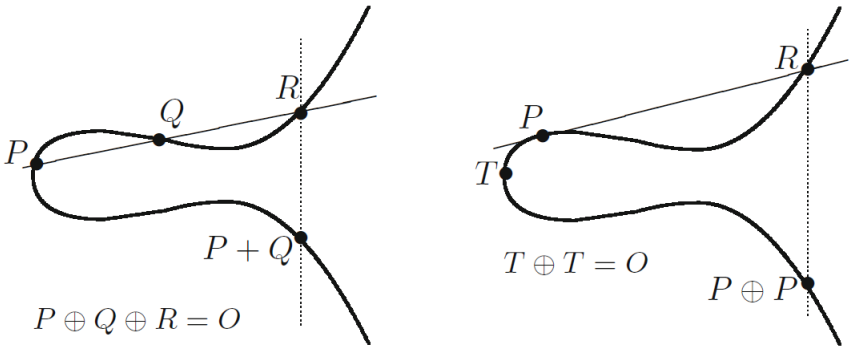

Figure 1: The composition law.

In general, an important theorem due to Weil ensures that the abelian group $A(K)$ is finitely generated and it can therefore be written as

$$A(K) = \mathbb{Z}P_1 \oplus ... \oplus \mathbb{Z}P_r \oplus A(K)_{\text{tors}}$$

where the torsion group $A(K)_{\text{tors}}$ is finite and r is called the rank of A over K.

It is very difficult to control the rank and the torsion subgroup of abelian varieties. Even for the case elliptic curves, we are far from having a complete understanding of the torsion subgroup, the Theorem of Mazur for elliptic curves over $\mathbb{Q}$ being one of the exceptions. See the Appendix [6] for more information on this.

3.3 Group law

Let E be an elliptic curve defined over a field K given by a Weierstrass equation. If P and Q are two points in $E(K)$, then we can uniquely describe a third point, $P+Q$, in the following way: draw the line that intersects P and Q. This will generally intersect the cubic at a third point, R. We then take $P+Q$ to be $-R$, the point opposite R (symmetric with respect to the x-axis).

This definition for addition works except in a few special cases related to the point at infinity and intersection multiplicity:

- When one of the points is O_E. Here, we define $P + O_E = P = O_E + P$, making O_E the identity of the group.

- If P and Q are opposites of each other, we define $P + Q = O_E$.

- If $P = Q$ we only have one point, thus we can't define the line between them. In this case, we use the tangent line to the curve at this point as our line. In most cases, the tangent will intersect a second point R and we can take its opposite. However, if P happens to be an inflection point (see point T on Figure 1) , we take R to be P itself and $P+P$ is simply the point opposite itself.

In algebraic terms, given the elliptic curve $E\colon y^2 = x^3 + ax + b$ over the field K (whose characteristic we assume to be neither 2 nor 3), and points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ on the curve. There are two cases:

1. Assume that $x_P \neq x_Q$. Let $y = sx + d$ be the line that intersects P and Q, which has the following slope:
$$s = \frac{y_P - y_Q}{x_P - x_Q}.$$
Now, we define $R = (x_R, y_R) = -(P + Q)$ as
$$x_R = s^2 - x_P - x_Q, \quad y_R = y_P + s(x_R - x_P).$$

2. If $x_P = x_Q$, then there are two options: if $y_P = -y_Q$, including the case where $y_P = y_Q = 0$, then the sum is defined as O_E; thus, the inverse of each point on the curve is found by reflecting it across the x-axis. If $y_P = y_Q \neq 0$, then $Q = P$ and $R = (x_R, y_R) = -(P + P) = -2P = -2Q$ is given by
$$s = \frac{3x_P^2 + a}{2y_P}, \quad x_R = s^2 - 2x_P, \quad y_R = y_P + s(x_R - x_P).$$

3.4 Isogenies

A rational map between smooth curves is always a morphism (regular everywhere). Since elliptic curves have a distinguish point (the origin), it is natural study morphisms between elliptic curves that send the origin to the origin. For the following definition, we do not assume that K is algebraically closed.

Definition 3.8. (Isogeny) Let (E_1, O_1) and (E_2, O_2) be elliptic curves defined over a field K. Then an isogeny is a morphism of curves $f : E_1 \longrightarrow E_2$ such that $f(O_1) = O_2$. If there exists a nonzero such map, then E_1 and E_2 are said to be isogenous. The degree of the isogeny is by definition the degree of the morphism f. It can be proven that to be isogenous is an equivalence relation among elliptic curves over K.

An isogeny f satisfies that either $f(E_1) = \{O_2\}$ or $f(E_1) = E_2$. Thus except for the zero isogeny defined by $[0](P) = O_2$ for all $P \in E_1$, every other isogeny is a finite map of curves. Hence we obtain the usual injection of function fields
$$f^* : \overline{K}(E_2) \longrightarrow \overline{K}(E_1).$$
The degree of f, which is denoted by $\deg(f)$, is the degree of the finite extension $\overline{K}(E_1)/f^*\overline{K}(E_2)$.

Elliptic curves are abelian groups, so the maps between them form groups. We denote the set of isogenies from E_1 to E_2 by
$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \longrightarrow E_2\}.$$
The sum of two isogenies is defined by
$$(f + g)(P) = f(P) + g(P)$$

and $f+g$ is a morphism, so it is an isogeny.

If $E_1 = E_2$, then we can also compose isogenies. Thus if E is an elliptic curve, we let

$$\mathrm{End}(E) = \mathrm{Hom}(E, E)$$

be the ring whose addition law is as given above and whose multiplication is composition,

$$(fg)(P) = f(g(P)).$$

Definition 3.9. Let E be an elliptic curve over K and let $m \in \mathbb{Z}$ with $m \geq 1$. The multiplication map $[m]\colon E \to E$ is an isogeny of degree n^2. The m-torsion subgroup of E, denoted by $E[m]$, is the kernel of this isogeny,

$$E[m] = \{P \in E(\overline{K}) : [m]P = 0\}.$$

For $\mathrm{char}(K) = 0$, the map $[\ ] : \mathbb{Z} \longrightarrow \mathrm{End}(E)$ is usually the whole story, i.e., $\mathrm{End}(E) \cong \mathbb{Z}$; otherwise, we say that E has complex multiplication. When necessary, we can specify $\mathrm{End}_K(E)$ to restrict to the subring of endomorphisms defined over the field K.

Example 1. Assume that $\mathrm{char}(K) \neq 2$ and let $i \in \overline{K}$ be a primitive fourth root of unity, i.e., $i^2 = -1$. Then, the elliptic curve E/K given by the equation

$$E : y^2 = x^3 - x$$

has endomorphism ring $\mathrm{End}(E)$ strictly larger than $\mathbb{Z}$, since it contains a map, which we denote by $[i]$, given by

$$[i] : (x, y) \mapsto (-x, iy).$$

Thus E has complex multiplication. Clearly $[i]$ is defined over K if and only if $i \in K$. Hence even if E is defined over K, it may happen that $\mathrm{End}_K(E)$ is strictly smaller than $\mathrm{End}(E)$.

Continuing with this example, we observe that

$$[i] \circ [i](x, y) = [i](-x, iy) = (x, -y) = -(x, y),$$

so, $[i] \circ [i] = [-1]$. There is thus a ring homomorphism

$$\begin{aligned} \mathbb{Z}[i] &\longrightarrow \mathrm{End}(E) \\ m + ni &\mapsto [m] + [n] \circ [i]. \end{aligned}$$

If $\mathrm{char}(K) = 0$, this map is an isomorphism, $\mathbb{Z}[i] \cong \mathrm{End}(E)$, in which case $\mathrm{Aut}(E) \cong \mathbb{Z}[i]^* = \{\pm 1, \pm i\}$ is a cyclic group of order 4.

Example 2. This second example deals with elliptic curves over $\mathbb{Q}$. In [18], Mazur shows that the modular curve $X_0(43)$ has a unique rational point corresponding to the elliptic curve

$$E\colon y^2 + y = x^3 - 1590140x - 771794326$$

with Cremona's label 1849a2. This elliptic curve is $\mathbb{Q}$-isogenous to 1949a1. Composing with $\overline{\mathbb{Q}}$-isomorphisms (twists), the elliptic curve E is also $\overline{\mathbb{Q}}$-isogenous to the elliptic curves 16641e2, 16641e1, 29584h2, 29584h1, 46225a2, 46225a1, ... all defined over $\mathbb{Q}$. Obviously, the defining equations of these isogenies are too monstrous to be written here.

Proposition 3.10. *The following properties hold:*

(i) Isogenies preserve the group addition law.

(ii) Let $f : E \to E'$ be an isogeny. Then, $\mathrm{Ker}(f)$ is a finite subgroup of E and $E' \simeq E/\ker f$.

(ii) If $G \subseteq E$ is a finite subgroup, then there is an isogeny $f : E \to E'$ with $\mathrm{Ker}(f) = G$.

Proof. See [4], pages 71-74. □

Definition 3.11. (Dual Isogeny) Given a degree n isogeny $f : E \to E'$ of elliptic curves over a field K, there is another isogeny defined over K (called the dual isogeny) $\hat{f} : E' \to E$ of the same degree such that $f \circ \hat{f} = [n]$.

3.5 Endomorphisms

Let E be an elliptic curve defined over a field K. An important tool in the study of the endomorphism ring $\mathrm{End}(E)$ is the map

$$\deg : \mathrm{End}(E) \longrightarrow \mathbb{Z}.$$

We denote by $\mathrm{Hom}_K(E_1, E_2)$ the collection of homomorphisms from E_1 to E_2 defined over K, and let $\mathrm{End}_K(E) = \mathrm{Hom}_K(E, E)$. The group structure on E_2 determines a group structure on $\mathrm{Hom}(E_1, E_2)$ such that as a $\mathbb{Z}$-module, $\mathrm{Hom}(E_1, E_2)$ is free of rank at most four. Composition of endomorphisms gives a ring structure on $O = \mathrm{End}(E)$, and we refer to O as the ring of endomorphisms of E. For an elliptic curve E, the abelian group law $E \times E \longleftarrow E$ is a morphism of varieties. Thus the map

$$\begin{aligned}[m] : & E \to E \\ & P \mapsto P + \cdots + P\end{aligned}$$

sending a point to the sum of P with itself m times is a morphism of E to itself sending O to O. This allows us to define an injective ring homomorphism

$$\mathbb{Z} \longrightarrow \mathrm{End}(E).$$

Since any isogeny $f : E_1 \longrightarrow E_2$ is a group homomorphism, for all integers m we have

$$[m]_{E_2} \circ f = f \circ [m]_{E_1}.$$

The following proposition gives an important result about this map that is used in the proof of Mazur's theorem. To prove it would require developing the theory of dual isogenies.

Proposition 3.12. *Let $E/\mathbb{Q}$ be an elliptic curve, and let $f \in \mathrm{End}_{\mathbb{Q}}(E)$ be an endomorphism defined over $\mathbb{Q}$. Then f is a scalar; that is, $f = [m]$ for some $m \in \mathbb{Z}$.*

Proof. See [1], page 13. □

4. Requisites for the proof of Lemma 2.2

4.1 Weil pairing

The Weil pairing was introduced by André Weil in 1940 and it plays an important role in the study of the arithmetic properties of elliptic curves.

In this section we let E/K be an elliptic curve and we fix an integer $m \geq 2$ which we assume to be prime to $p = \mathrm{char}(K)$ if $p > 0$. As an abstract group, the group of m-torsion points satisfies

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

Let $T \in E[m]$. Then there is a function $f \in \overline{K}(E)$ satisfying $\mathrm{div}(f) = m(T) - m(O)$. Next take a point $T' \in E(\overline{K})$ with $[m]T' = T$. Then there is similarly a function $g \in \overline{K}(E)$ satisfying

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} (T' + R) - (R).$$

Since $f \circ [m]$ and g^m have the same divisor, we can (and do) assume that $f \circ [m] = g^m$ after multiplying f by a convenient scalar in $\overline{K}^*$. Now let $S \in E[m]$ be another m-torsion point, where we allow $S = T$. Then for any point $X \in E(\overline{K})$, we have

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m.$$

The Weil pairing is the bilinear form

$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$

on the torsion points of order m of an elliptic curve E defined over a field K taking values on the n^{th} roots of unity, defined as follows. Given S and T points in $E[m]$, we declare:

$$e_m(S, T) = \frac{g(X + S)}{g(X)},$$

where $X \in E$ is any point such that $g(X + S)$ and $g(X)$ are both defined and nonzero. The Weil pairing has the following properties:

Proposition 4.1. (Weil pairing).

(i) Linearity: If $P, Q, R \in E[n]$ then

$$e_n(P + Q, R) = e_n(P, R)e_n(Q, R),$$
$$e_n(P, Q + R) = e_n(P, Q)e_n(P, R).$$

(ii) Alternating: If $P \in E[n]$, then $e_n(P, P) = 1$. This, along with linearity, implies that if $P, Q \in E[n]$, then $e_n(Q, P) = e_n(P, Q])^{-1}$, which is usually called anti-symmetry.

(iii) Non-degeneracy: If $O \neq P \in E[n]$, there exists $Q \in E[n]$ such that $e_n(P, Q) \neq 1$.

(iv) Compatibility: If $P \in E[mn]$ and $Q \in E[n]$, then $e_{mn}(P, Q) = e_n(mP, Q)$.

(v) Galois action: Let $P, Q \in E[n]$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, then

$$e_n(P, Q)^\sigma = e_n(P^\sigma, Q^\sigma).$$

Proof. See [4] (page 94). □

For any elliptic curve E/K and each prime p different from $\mathrm{char}(K)$, we obtain a Galois representation

$$\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Thanks to the Weil pairing, the determinant $\mathrm{Gal}(\overline{K}/K) \longrightarrow \mathbb{F}_p^*$ of this representation is the cyclotomic character giving the Galois action of the p-th roots of unity.

Corollary 4.2. *There exist points $S, T \in E[m]$ such that $e_m(S,T)$ is a primitive m-th root of unity. In particular, if $E[m] \subset E(K)$, then $\mu_m \subset K^*$.*

Proof. The image of e_m is a subgroup of μ_m, hence we may suppose that $\mathrm{Im}(e_m) = \mu_d$. It follows that

$$1 = e_m(S,T)^d = e_m([d]S, T) \quad \text{for all} \quad S, T \in E[m].$$

The nondegeneracy of the e_m-pairing implies that $[d]S = O$, and since S is arbitrary, $d = m$. So, $e_m(S,T)$ is a primitive mth root of unity. Finally, if $E[m] \subset E(K)$, then the Galois invariance of the e_m-pairing implies that $e_m(S,T) \in K^*$ for all $S, T \in E[m]$. Hence $\mu_m \subset K^*$. □

In particular, one has the inclusions of field extensions $K \subseteq K(\mu_p) \subseteq K(E[p])$ that has been used in lemma 2.3. The Weil pairing admits a generalization to abelian varieties and it has also applications to elliptic curve cryptography and identity based encryption.

4.2 Galois representation attached to torsion points

To begin, recall that given an elliptic curve E defined over $\mathbb{Q}$, then the set of p-torsion points

$$E[p] := E(\overline{\mathbb{Q}})[p] = \{P = (x,y) \in E(\overline{\mathbb{Q}}) \colon p \cdot P = \mathrm{O}_E\} \cup \{\mathrm{O}_E\}$$

is a 2-dimensional $\mathbb{F}_p$-vector space where the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts in a natural way:

$$P^\sigma = (x,y)^\sigma = (x^\sigma, y^\sigma)\,.$$

Since the action is linear $(P+Q)^\sigma = P^\sigma + Q^\sigma$, we get an homomorphism

$$\varrho_{E,p} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)\,.$$

It is clear that $\varrho = \varrho_{E,p}$ factors through $\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q})$, given an embedding

$$\mathrm{Gal}(\mathbb{Q}(E[p])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)\,.$$

Due to the Weil pairing, the determinant $\det \varrho$ is the cyclotomic character

$$\chi \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \simeq \mathbb{F}_p^*\,.$$

which gives the Galois action on the p-th roots of unity: $\zeta^\sigma = \zeta^{\chi(\sigma)}$ for $\zeta \in \mu_p$. In particular, this amounts to the inclusions

$$\mathbb{Q} \subseteq \mathbb{Q}(\mu_p) \subseteq \mathbb{Q}(E[p])\,.$$

Assume that $E(\mathbb{Q})_{\mathrm{tors}}$ contains a point P of primer order p. Then, the 2-dimensional vector space $E[p]$ has a 1-dimensional vector subspace $\langle P \rangle$ with trivial action. Hence, we get a short exact sequence

$$0 \longrightarrow \langle P \rangle \longrightarrow E[p] \longrightarrow E[p]/\langle P \rangle \longrightarrow 0$$

where the action on the quotient is given by the cyclotomic character, since $\det \varrho = \chi$. Alternatively, we can use the Weil pairing e_p to define a map $E[p] \to \mu_p$ by $Q \mapsto e_p(P, Q)$. Since $P \in E(\mathbb{Q})$, this gives the short exact sequence of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E[p] \longrightarrow \mu_p \longrightarrow 0\,.$$

As a consequence, the image of the Galois representation should be of either form:

$$\mathrm{Im}\,\varrho = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & \chi \end{pmatrix} \\ \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix} \end{cases}$$

The above exact sequence *splits* in the first case, and it is *non-split* in the case $* \neq 0$.

4.3 Hilbert class field of cyclotomic extensions

Given a number field extension $N/\mathbb{Q}$, the Hilbert class field of N is defined as the maximal abelian extension of L/N. It turns out to be a finite extension (so L is a number field). In fact, the abelian Galois group $\mathrm{Gal}(L/N)$ is isomorphic to the ideal class group of N.

In view of Mazur's theorem, we restrict ourselves here to the cyclotomic case $N = \mathbb{Q}(\mu_p)$ for an odd prime p. We will announce Herbrand theorem without proof. We refer the reader to [16] and [17] for more details.

Let $\mathbb{Q}(\mu_p)$ be the p-th cyclotomic field and let K be its Hilbert class field. Let Y' be the maximal quotient of $\mathrm{Gal}(L/\mathbb{Q}(\mu_p))$ where every element has order a power of p, and let Y be the subgroup of Y' generated by elements of order p. In particular, we see that Y is the trivial group whenever $p-$ is a regular prime. An odd prime number p is defined to be regular if it does not divide the class number of the p-th cyclotomic field $\mathbb{Q}(\mu_p)$.

The group $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on $\mathrm{Gal}(K/\mathbb{Q}(\mu_p))$ by conjugation in $\mathrm{Gal}(K/\mathbb{Q})$, and $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts on Y. We consider ζ any primitive p-th root of unity and an arbitrary element σ on $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$. We have $\sigma(\zeta) = \zeta^d$ for some $d \in (\mathbb{Z}/p\mathbb{Z})^*$ and d does not depend on the choice of ζ. Thus, there exists

$$\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^*$$

a canonical isomorphism, and we obtain an action of $(\mathbb{Z}/p\mathbb{Z})^*$ on Y. Now, for any integer j, we define $Y^{(j)}$ to be the subgroup of Y on which $a \in (\mathbb{Z}/p\mathbb{Z})^*$ acts as multiplication by a^j.

We can now state Herbrand's Theorem.

Theorem 4.3. (Herbrand). *Using the above notations, let $1 < j < p-1$ be an odd integer. If $Y^{(j)}$ is non-trivial, then the Bernoulli number B_{p-j} has numerator divisible by p.*

For example, consider the smallest irregular prime $p = 37$. We need j such that $1 < j < 36$ and j odd. Choosing $j = 5$, one has:

$$B_{p-j} = B_{32} = \frac{-7709321041217}{510}$$

and we can see that $\frac{7709321041217}{37} = 208360028141$ and, therefore $Y^{(j)} = Y^{(5)} \neq 0$.

Ribet's theorem provides the reciprocal of Herbrand's theorem (see [17]):

Theorem 4.4. (Ribet). *Let $1 < j < p-1$ be an odd integer. If the Bernoulli number B_{p-j} has numerator divisible by p then $Y^{(j)}$ is non-trivial.*

5. Requisites for the proof of Lemma 2.3

5.1 Group schemes

Definition 5.1. (i) Let S be a scheme. A group scheme over S, or an S-group scheme, is an S-scheme $\pi : G \longrightarrow S$ together with S-morphisms $m : G \times_S G \longrightarrow G$ (group law, or multiplication), $i : G \longrightarrow G$ (inverse), and $e : S \longrightarrow G$ (identity section), such that the following identities of morphisms hold:

$$\begin{aligned} m \circ (m \times id_G) &= m \circ (id_G \times m) : G \times_S G \longrightarrow G, \\ m \circ (e \times id_G) &= j_1 : S \times_S G \longrightarrow G, \\ m \circ (id_G \times e) &= j_2 : G \times_S S \longrightarrow G, \end{aligned}$$

and

$$e \circ \pi = m \circ (id_G \times i) \circ \Delta_{G/S} = m \circ (i \times id_G) \circ \Delta_{G/S} : G \longrightarrow G,$$

where $j_1 : S \times_S G \longrightarrow G$ and $j_2 : G \times_S S \longrightarrow G$ are the canonical isomorphisms.

(ii) A group scheme G over S is said to be commutative if, writing $s : G \times_S G \longrightarrow G \times_S G$ for the isomorphism switching the two factors, we have the identity $m = m \circ s : G \times_S G \longrightarrow G$.

(iii) Let

$$\pi_1 : G_1 \longrightarrow S,\ m_1,\ i_1,\ e_1$$

and

$$\pi_2 : G_2 \longrightarrow S,\ m_2,\ i_2,\ e_2$$

be two group schemes over S. A homomorphism of S-group schemes from G_1 to G_2 is a morphism of schemes $f : G_1 \longrightarrow G_2$ over S such that

$$f \circ m_1 = m_2 \circ (f \times f) : G_1 \times_S G_1 \longrightarrow G_2.$$

This condition implies that $f \circ e_1 = e_2$ and $f \circ i_1 = i_2 \circ f$.

In practice it will usually either be understood what m, i and e are, or it will be unnecessary to make them explicit; in such case we will simply speak about "a group scheme G over S" without further specification.

We present two examples, the additive group and the multiplicative group.

1. *Additive Group*: Consider Spec $\mathbb{Z}[x]$, and we need to define the multiplication

$$\text{Spec } \mathbb{Z}[x] \times_{\mathbb{Z}} \text{Spec } \mathbb{Z}[x] \longrightarrow \text{Spec } \mathbb{Z}[x].$$

The structure of a group scheme is given, on rings, by the following homomorphisms:

$m : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Z}[x] \cong \mathbb{Z}[x_1, x_2]$ given by $x \mapsto x \otimes 1 + 1 \otimes x$, defining the group law;
$i : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$ given by $x \mapsto -x$ defining the inverse;
$e : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ given by $x \mapsto 0$ defining the identity.

The group scheme Spec $\mathbb{Z}[x]$ is denoted $\mathbb{G}_a$, and it is so called because for any ring R we have $\mathbb{G}_a(R) = \mathbb{G}_a(\text{Spec } R) \cong R^+$, the abelian group underlying R.

2. *Multiplicative Group*: One can similarly define a $\mathbb{Z}$-group scheme $\mathbb{G}_m$ so that $\mathbb{G}_m(R) \cong R^\times$ for any ring R. In this case $\mathbb{G}_m$ is dual to the ring $\mathbb{Z}[x, x^{-1}]$. The structure of a group scheme is defined by the homomorphisms given by

$$x \mapsto x \otimes x, \text{ defining the multiplication;}$$
$$x \mapsto x^{-1}, \text{ defining the inverse;}$$
$$x \mapsto 1, \text{ defining the identity element.}$$

We obtain R-group scheme analogs of the additive and multiplicative groups schemes, which we denote $(\mathbb{G}_a)_R$ and $(\mathbb{G}_m)_R$. However, for any R-algebra A, one easily checks that $(\mathbb{G}_a)_R(A) \cong \mathbb{G}_a(A)$ and $(\mathbb{G}_m)_R(A) \cong \mathbb{G}_m(A)$ as groups. Hence $(\mathbb{G}_a)_R$ and $(\mathbb{G}_m)_R$ are in some sense the same as $\mathbb{G}_a$ and $\mathbb{G}_m$.

Definition 5.2. A finite flat group scheme of order n is a Spec R-group scheme Spec A where A is a locally free R-algebra of rank n.

Now, we collect a couple of results on group schemes which will be needed in the proof of Mazur's Theorem. In both cases the proofs are complicated to be included here, so we will give references for the proofs.

Proposition 5.3. (Raynaud). *Let p be an odd prime, and let O be the ring of integers of a field $K/\mathbb{Q}_p$ of absolute ramification index less than $p - 1$. Let G be a commutative, finite flat O-group scheme of order a power of p. Then G is uniquely determined up to isomorphism by the isomorphism type of its generic fiber.*

Proof. See [19], p. 152. □

Proposition 5.4. *Let T be an open subscheme of* Spec $\mathbb{Z}$ *over which* 2 *is invertible, let A be an abelian T-group scheme, and let p be any prime giving a closed point of T. Then the specialization map $A(T)_{\text{tors}} \longrightarrow A(\mathbb{F}_p)$ is injective.*

Proof. See [24]. □

5.2 Néron model

The purpose of this section is to explain the definition and basic properties of the Néron model $\mathcal{E}$ of an elliptic curve E over a global or local field K.

The motivation is due to the fact that the reduction mod q of an elliptic curve E defined over $\mathbb{Q}$ is not a problematic issue as long as we stay at primes q where the elliptic curve has good reduction (which are all the primes except finitely many). But when trying to reduce at primes of bad reduction we do not get anymore an elliptic curve in positive characteristic. Indeed, the reduction is a curve with (a unique) singularity and one should be careful with the reduction map.

André Néron proposed in the 1960s the minimal regular models for curves (arbitrary genus) as well as for abelian varieties (arbitrary dimension) as a good solution to deal with the special fibers at primes of bad reduction. In the case of elliptic curves (genus one and one dimensional varieties at the same time), the computation of these minimal regular models can be done explicitly with Tate's algorithm.

An excellent expository about Néron models is offered by Silverman in Chapter IV of [5]. Here, we limit ourselves to recall its definition and main features, emphasizing the properties needed with regard to the proof of Mazur's theorem.

Let R be a Dedekind domain with field of fractions K, and let C/K be a curve. A regular model for C is a proper flat scheme $\mathcal{C}$ over R which is regular and whose generic fiber is C. A regular model $\mathcal{C}$ is minimal if for any other regular model $\mathcal{C}'$, there exists a map of schemes $\mathcal{C}' \longrightarrow \mathcal{C}$ extending the identity on the generic fiber. The main theorem is that minimal regular models exist and are canonically unique. One can find a regular model for C by starting with any model and repeatedly blowing-up and normalizing. From there, one can find a minimal regular model by blowing-down certain divisors in the special fiber.

Let E/K be an elliptic curve and let $\mathcal{C}/R$ be its minimal regular model. The Néron model of E is then the smooth locus in $\mathcal{C}$. This can be taken as a definition.

What are the advantages to consider the Néron model of E? Assume that R is a Henselian DVR (discrete valuation ring), let K its fraction field as above, and k be its residue field. Let $\mathcal{W}$ be the minimal Weierstrass model of the elliptic curve E/K. Since $\mathcal{W}$ is proper over R, we have $\mathcal{W}(R) = \mathcal{W}(K) = E(K)$. However, $\mathcal{W}$ is typically singular. Its smooth locus $\mathcal{W}_{\mathsf{sm}}$ is a group scheme over R. Typically, it is not proper, and not all K-points of E extend to $\mathcal{W}_{\mathsf{sm}}$. Those that do are the subgroup $E_0(K)$, which has finite index in $E(K)$.

The Néron model is an extension $\mathcal{E}$ of E over R which combines the desirable properties of $\mathcal{W}$ and $\mathcal{W}_{\mathsf{sm}}$: it is a smooth group scheme and all K-points extend to R-points. The identity component of $\mathcal{E}$ is usually denoted by $\mathcal{E}^0$ and it is $\mathcal{W}_{\mathsf{sm}}$, while the component group of $\mathcal{E}/k$ (at least for k algebraically closed) is $E(K)/E_0(K)$. So all points of $E(K)$ extend to $\mathcal{E}(R)$, and $E_0(K)$ is the subgroup of points which extend to $\mathcal{E}^0$.

Theorem 5.5. (Kodaira-Néron) *Let R be a Dedekind domain with field of fractions K, let $\mathcal{E}$ be a Néron model over R for an elliptic curve E/K, and let $q \subset R$ be any nonzero prime ideal with residue field k_q. Let $\mathcal{E}(k_q)$ denote the special fiber of $\mathcal{E}$ at q.*

1. *If E has stable reduction at q, then $\mathcal{E}(k_q) = \mathcal{E}(k_q)^0$ is an elliptic curve.*
2. *If E has semi-stable reduction at q, then there exists an extension k of k_q of degree at most two so that $\mathcal{E}(k)^0 \cong k^*$ and $\mathcal{E}(k)/\mathcal{E}(k)^0 \cong \mathbb{Z}/n\mathbb{Z}$ for some positive integer n.*

3. *If E has unstable reduction at q, then $\mathcal{E}(k_q)^0 \cong k_q^+$, and $\mathcal{E}(k_q)/\mathcal{E}(k_q)^0$ is a finite group of order at most four.*

Proof. See [5], p. 361-379. □

Examples of Néron models. We are going to illustrate the Néron models of the elliptic curves 11A, 11B considered in the introduction. Since the conductor of these elliptic curves is 11, the only prime of bad reduction is $q = 11$.

E	Weierstrass equation	j_E	$E(\mathbb{Q})$
$11A$	$y^2 + y = x^3 - x^2 - 10x - 20$	$-2^{12}31^3/11^5$	$\langle [5:5:1] \rangle$
$11B$	$y^2 + y = x^3 - x^2$	$-2^{12}/11$	$\langle [0:-1:1] \rangle$

E	$E(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_{11})$	singular point
$11A$	collapse	$(5, 5)$
$11B$	injective	$(8, 5)$

The process to build the minimal regular model of an elliptic curve is rather intricate. A detailed description and examples are given by Silverman in [5]. At each step, one should make a translation to bring a non-regular point at the origin, and then do the blowing up with three local charts. Then inspect how they glue each other and check if there are still non-regular points to initialize the process again. The software package MAGMA has the functionality to compute regular models of curves of arbitrary genus (Steve Donnelly was the author of that part of the code).

• Case 11B: $y^2 + y = x^3 - x^2$. Since $v_{11}(j) = -1$, the Kodaira symbol is I_1 and that means that the special fiber of the Néron model has only one component. We run the following script in MAGMA (web page: `http://magma.maths.usyd.edu.au/calc/`):

```
****************************************
P<x,y,z>:=ProjectiveSpace(Rationals(),2);
C:=Curve(P,y^2*z+y*z^2-x^3+x^2*z);

M:=RegularModel(C, 11);

IntersectionMatrix(M);

ComponentGroup(M);

Q:=PointsCubicModel(C,10^4)[i];

PointOnRegularModel(M,Q);
****************************************
```

This script returns the patch index like $< n, i >$ where n counts the blowups and i counts the patches of each blowup. Also, returns patch equations, point coordinates, the component

indices and component equations for each point Q:= $PointsCubicModel(C, 10^4)[i]$, for i from 1 to 5 (because we have five torsion points).

The intersection matrix of its components is trivial, because it has only one component. The component is given by the equations

$$\begin{cases} x^3 + 10x^2 + 10y^2 + 10y, \\ z. \end{cases}$$

except for point $(0 : 1 : 0)$, the point to infinity, which has the equation given by:

$$\begin{cases} x^3 + 10x^2y + 10y^2 + 10y, \\ z. \end{cases}$$

Now, we want to see where the torsion points are:

Torsion Points	Coordinate points	Point reduction	Component indices
$(0 : 0 : 1)$	$[0, 0, 11]$	$[0, 0, 0]$	[1]
$(0 : 1 : 0)$	$[0, 0, 11]$	$[0, 0, 0]$	[1]
$(0 : -1 : 1)$	$[0, -1, 11]$	$[0, 10, 0]$	[1]
$(1 : -1 : 1)$	$[1, -1, 11]$	$[1, 10, 0]$	[1]
$(1 : 0 : 1)$	$[1, 0, 11]$	$[1, 0, 0]$	[1]

Notice that all the torsion points fall on the same component.

• Case 11A: $y^2 + y = x^3 - x^2 - 10x - 20$. Since $v_{11}(j) = -5$, the Kodaira symbol is I_5 and that means that the special fiber of the Néron model has five components. We run the following script in MAGMA:

```
****************************************
P<x,y,z>:=ProjectiveSpace(Rationals(),2);

C:=Curve(P,y^2*z+y*z^2-x^3+x^2*z+10*x*z^2+20*z^3);

M:=RegularModel(C, 11);

IntersectionMatrix(M);

Q:=PointsCubicModel(C,10^4)[i];

PointOnRegularModel(M,Q);
****************************************
```

The intersection matrix of its components is:

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

where the position a_{ij} denotes the intersection number between the components i and j. We can represent the special fiber of the Néron model with Figure 2.

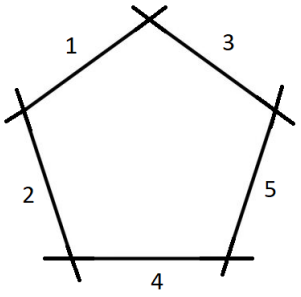

Figure 2: Distribution of components

The five 11A torsion points are located in the special fiber of the Néron model.

Torsion Points	Coordinate points	Point reduction	Component indices
$(0:1:0)$	$[0,0,11]$	$[0,0,0]$	[1]
$(5:-6:1)$	$[0,-1,11]$	$[0,10,0]$	[2]
$(5:5:1)$	$[0,0,11]$	$[0,0,0]$	[3]
$(16:60:1)$	$[11,0,0]$	$[0,0,0]$	[4]
$(16:-61:1)$	$[11,-1,0]$	$[0,10,0]$	[5]

In this case, each torsion point belongs to a different component of the special fiber:

Torsion Points	Component equation
$(0:1:0)$	$x_2^3 + 10x_2^2y_2 + x_2y_2^2 + 2y_2^3 + 10y_2^2 + 10y_2, z_2$
$(5:-6:1)$	$x_2 + 9y_2 + 9, z_2$
$(5:5:1)$	$x_2 + 2y_2, z_2$
$(16:60:1)$	$x_2, y_2 + z_2$
$(16:-61:1)$	$x_2, y_2 + 1$

Observe the different behaviour in the previous two examples. In the first, all the five torsion points fell in the same component (the unique component, the identity component), while in the

second example each one of the five torsion points fall in a different component. This observation is the key to the strategy in the proof of Mazur's theorem, since we will come to contradiction for $p > 13$. More precisely, if $E(\mathbb{Q})$ has rational cyclic subgroup of order $p > 13$, then Mazur shows that, one the hand, all the p-torsion points should fall in the identity component of the special fiber if the Néron model of E (as for the case 11B) and, on the other hand, he shows that all of them should fall in the different components of the special fiber (as for 11A, where $p = 5$). This yields a contradiction with the existence of a p-torsion point with $p > 13$.

5.3 Néron-Ogg-Shafarevich

We state without proof the ramification criterion of Néron-Ogg-Shafarevic, which is used in the proof of lemma 2.3. We refer to [3] for a proof.

Proposition 5.6. (Néron-Ogg-Shafarevich). *Let E be an ellipitc curve defined over a number field K. Let m be a positive integer, and let $\mathfrak{P}$ be a finite place of K with $\mathfrak{P} \nmid m$. If E has good reduction at $\mathfrak{P}$, then $K(E[m])/K$ is unramified at $\mathfrak{P}$. Also, if $K(E[m])/K$ is unramified at $\mathfrak{P}$ for infinitely many m, then E has good reduction at $\mathfrak{P}$.*

Corollary 5.7. *Let E_1 and E_2 be elliptic curves defined over a number field K. Suppose that there is an isogeny $f : E_1 \to E_2$ defined over K. Then E_1 has good reduction at any given prime of K if and only if E_2 does.*

Proof. Suppose that there is an isogeny $f : E_1 \to E_2$ defined over K. Let $\mathfrak{P}$ be any prime of K. Let $m > 1$ be any integer relatively prime to *deg* f and $m \nmid \mathfrak{P}$. Now, we restrict f to $E_1[m]$ and we obtain that $f|_{E_1[m]}$ is injective. And we can see that $\overline{f} : E_1[m] \longrightarrow E_2[m]$ is bijective. Because f is defined over K we see that this is an isomorphism of $\mathrm{Gal}(\overline{K}/K)-$modules, and consequently $K(E_1[m])$ is unramified over $\mathfrak{P}$ if and only if $K(E_2[m])$ is.
This equivalence holds for infinitely many integers m. Now we can apply the Néron-Ogg-Shafarevich (see proposition 5.6), and we see that E_1 has a good reduction at K if and only if E_2 does. □

We complete this section with a result of Shafarevich. For more information we refer to [4] p. 264.

Proposition 5.8. (Shafarevich). *Let K be a number field, and let S be a finite set of places of K including all the infinite places. Then, up to isomorphism over K, there are only finitely many elliptic curves defined over K with good reduction at all primes not in S.*

5.4 Multiplicative lemmas

In this section we prove two lemmas on the possible reduction of an hypothetical elliptic curve over $\mathbb{Q}$ with a rational point $P \in E(\mathbb{Q})_{tors}$ of order $p > 13$.

Lemma 5.9. *Let $E/\mathbb{Q}$ be an elliptic curve with a point $P \in E(\mathbb{Q})_{\mathrm{tors}}$ of prime order $p > 13$. Then E has either good or multiplicative reduction at all primes q.*

Proof. Let $\mathcal{E}$ be the Néron model for E over $\mathbb{Z}$, and let $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{E}$ be the constant finite flat subgroup scheme generated by P. Suppose that E has a additive reduction at a prime q. We know

that $\mathcal{E}(\mathbb{F}_q)^0$ has index at most four in $\mathcal{E}(\mathbb{F}_q)$ by theorem 5.5. This implies

$$\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \subseteq \mathcal{E}(\mathbb{F}_q)^0.$$

By theorem 5.5, we also know that

$$\mathcal{E}(\mathbb{F}_q)^0 \cong \mathbb{F}_q^+.$$

Therefore, we have

$$\mathbb{Z}/p \subseteq \mathbb{F}_q^+,$$

which is a contradiction when $q \neq p$. It remains to to study the case $q = p$.

By proposition 3.7, we know that there exists a field extension $K/\mathbb{Q}_p$ of absolute ramification index at most 6 so that E/K has either good or multiplicative reduction at the maximal ideal of $\mathcal{O}$, the ring of integers of K. If $e = [K : \mathbb{Q}_p]$ is the absolute ramification index, we may choose K so that $e \leq 6$.

We consider $\mathcal{E}'$ the Néron Model for E over $\mathcal{O}$ and $\mathcal{E} \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(\mathcal{O})$ the base change of $\mathcal{E}$ from $\mathbb{Z}_p$ to $\mathcal{O}$. By NMP there exists a morphism

$$f : \mathcal{E} \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(\mathcal{O}) \longrightarrow \mathcal{E}'$$

which is an isomorphism on the generic fibers.

Now, we can conclude that f must be trivial on the special fibers because there are no nontrivial maps from an additive group to a multiplicative group or to elliptic curves over given field.

Let $G \subset \mathcal{E}'$ be the closed subgroup scheme generated by $\mathbb{Z}/p\mathbb{Z}(K) \subseteq \mathcal{E}'$. We have a natural morphism

$$(\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}} \longrightarrow G_{\mathcal{O}}$$

which is an isomorphism on generic fibers, and not an isomorphism on the special fibers, by the above discussion. Since $e \leq 6 < p-1$, we can apply proposition 5.3 to the finite flat group scheme G of order p and we get a contradiction.

Therefore, the elliptic curve E has either good or multiplicative reduction at all primes q. □

Lemma 5.10. *Let $E/\mathbb{Q}$ be an elliptic curve with a point $P \in E(\mathbb{Q})_{\mathrm{tors}}$ of prime order $p > 13$. Then E has bad reduction at 2 and 3.*

Proof. If E has good reduction at some prime q, then by proposition 3.6, the reduction $\mathcal{E}(\mathbb{F}_q)$ has at most $q+2\sqrt{q}+1$ points. On the other hand, the reduction is injective as well, and consequently $p \leq q + 2\sqrt{q} + 1$. This is a contradiction for $q < 7$.

By lemma 5.9 we see that E must have a multiplicative reduction at $2, 3$ and 5. But, by Tate's theory, $\mathcal{E}(\mathbb{F}_{q^2}) \cong \mathbb{F}_{q^2}^*$ a cyclic group of order $q^2 - 1$. We cannot have $\mathbb{Z}/p\mathbb{Z} \subseteq \mathbb{F}_{q^2}^*$ for $q = 2, 3$, by virtue of our hypotheses on p. □

5.5 Modular curves and the key theorem

We will discuss here only those modular curves used in the proof of Mazur's Theorem, and even in this specific case we shall omit proofs.

Let $\mathbb{H}$ denote the upper-half plane, that is $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. For any $\tau \in \mathbb{H}$ we obtain a lattice $\Lambda \in \mathbb{C}$ generated by 1 and τ. This lattice corresponds to a complex elliptic curve. We define

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - cb = 1 \right\}$$

We will also use the notation $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

Proposition 5.11. *The map $j : \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathbb{C}$ is bijective.*

Proof. See [1], page 13. □

The Riemann surface $X(1) = \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$ is the simplest example of a modular curve.

The modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half-plane $\mathbb{H}$ by fractional linear transformations. The definition of a general modular curve involves a choice of a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$. A classical example is that of, for a fix any positive integer N, we consider the congruence subgroups

$$\begin{aligned}
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \mod N \right\} \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0\,, a \equiv 1\,, d \equiv 1 \mod N \right\} \\
\Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 a \equiv 1\,, d \equiv 1\,, b \equiv 0 \mod N \right\}
\end{aligned}$$

giving rise to the modular curves $X_0(N)$, $X_1(N)$, and $X(N)$, respectively.

In fact, the above curves $\mathbb{H}/\Gamma_0(N)$, $\mathbb{H}/\Gamma_1(N)$, $\mathbb{H}/\Gamma(N)$ need a compactification at the cusps. This is defined by extending the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$, as follows

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} [x : y] \mapsto [ax + by : cx + dy]\,.$$

Proposition 5.12. *There exists a smooth projective curve $X_0(N)/\mathbb{Q}$ and a bijection*

$$j_{N,0} : \mathbb{H}^*/\Gamma_0(N) \longrightarrow X_0(N)(\mathbb{C})$$

with the following property: let $\tau \in \mathbb{H}/\Gamma_0(N)$, and let $K = \mathbb{Q}(j_{N,0}(\tau))$. Then τ corresponds to a pair (E, C) where E/K is an elliptic curve and $C \subset E$ is a cyclic subgroup of order N also defined over K.

Proof. See [23], section 6.7. □

The other important idea is a modular interpretation for the points of $X_0(N)$ corresponding to $\mathbb{P}^1(\mathbb{Q}) \subset \mathbb{H}^*$. Whenever N is an odd prime one can easily check that $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$ consists of two points, which are sometimes called 0 and ∞. These points are named the cusps of $X_0(N)$ and, in some sense, they correspond to curves defined by singular Weierstrass equations.

To fix ideas, let $E/\mathbb{Q}$ be an elliptic curve with multiplicative reduction at some prime p, let $\mathcal{E}$ be a Néron model for E over $\mathbb{Z}$, and let $C \subseteq E(\mathbb{Q})_{\mathrm{tors}}$ be a cyclic subgroup of order p. Then the reduction of E mod p is not an elliptic curve, and then the pair (E, C) corresponds to one of the cusps when reduced mod p. The key fact is the following:

1. If $C \subset \mathcal{E}(\mathbb{F}_p)^0$, then (E, C) corresponds to 0.
2. If $C \not\subset \mathcal{E}(\mathbb{F}_p)^0$, then (E, C) corresponds to ∞.

The following proposition is key to the proof of the following theorem, which is the key to prove Mazur's theorem. Indeed, it is in some sense the heart of Mazur's proof of his Theorem.

Proposition 5.13. (Mazur). *Let N be an odd prime. There exists an abelian variety J and a surjective morphism $f : X_0(N) \longrightarrow J$ such that $J(\mathbb{Q})$ is a torsion group. Further, if the cusps $0, \infty \in X_0(N)$ satisfy $f(0) = f(\infty)$, then $N \leq 13$.*

Proof. See [16], pages 148-150. □

The following theorem is the key point in the proof of Mazur's theorem. The article [16] is devoted to its difficult and technical proof.

Theorem 5.14. (Mazur). *Let $E/\mathbb{Q}$ be an elliptic curve with a point $P \in E(\mathbb{Q})_{\text{tors}}$ of prime order $p > 13$. If E has bad reduction at a prime q, then the subscheme generated by the point P satisfies $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \not\subset \mathcal{E}(\mathbb{F}_q)^0$.*

Proof. By lemma 5.9, we know that E has multiplicative reduction at q. By proposition 5.5, it follows that

$$\mathcal{E}(\mathbb{F}_{q^2})^0 \cong \mathbb{F}_{q^2}^*,$$

a cyclic group of order $q^2 - 1$. So, $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \subseteq \mathcal{E}(\mathbb{F}_q)^0$ can only occur if p divides $q^2 - 1$. In particular this inclusion does not hold if $q \in \{2, 3, p\}$.

Now, consider, for contradiction, that $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \subseteq \mathcal{E}(\mathbb{F}_q)^0$ and, by the previous paragraph, we can (and do) assume that $q \neq 2, 3$ or p.

We consider S the scheme $\operatorname{Spec}\mathbb{Z}[1/2p]$ and let x be the S-valued point of $X_0(p)$ determined by the pair $(E_S, (\mathbb{Z}/p\mathbb{Z})_S)$, that is $x = j_{p,0}(E_S, (\mathbb{Z}/p\mathbb{Z})_S)$.

By lemma 5.10, we know that E has multiplicative reduction at 2 and 3 and

$$\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_2) \not\subset \mathcal{E}(\mathbb{F}_2)^0$$

and

$$\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_3) \not\subset \mathcal{E}(\mathbb{F}_3)^0.$$

Therefore, we can conclude that the value of x lying over 2 and 3 is ∞, while the value of x lying over q is 0, because $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \subset \mathcal{E}(\mathbb{F}_q)^0$. Figure 3 shows the scheme-theoretic diagram where ∞ and 0 are the cuspidal sections over S.

Now we consider the natural projection to the Eisenstein quotient $f : X_0(p)/S \longrightarrow J/S$. One has $f(x) = (x) - (\infty)$. By proposition 5.13 one has that $J(S) = J(\mathbb{Q})$ is a torsion group.

Since S is an open subscheme of $\operatorname{Spec}\mathbb{Z}$ over which 2 is invertible, if A is any abelian scheme over S, and ℓ any rational prime representing a closed point of S, then the specialization map $A(S)_{\text{tors}} \longrightarrow A(\mathbb{F}_\ell)$ is injective (see proposition 5.4). Applying this fact to $A = J$, the specialization

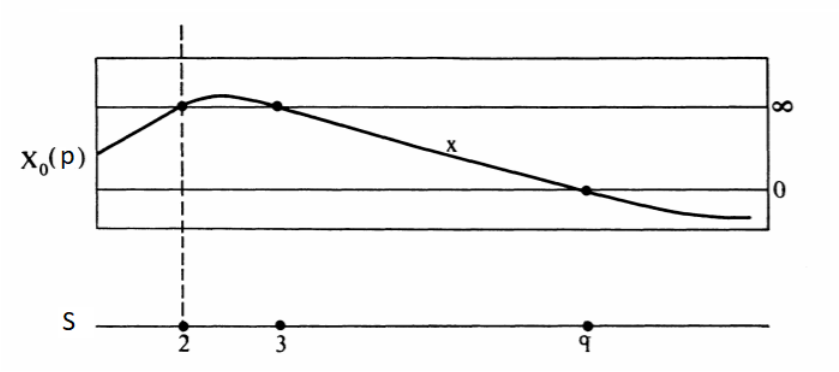

Figure 3: Scheme-theoretic diagram.

map $J(S) \longrightarrow J(\mathbb{F}_\ell)$ is injective. With $\ell = 3$, we see that $(x) - (\infty)$ is the neutral point in $J(S)$. With $\ell = q$, we see that $(x) - (\infty) = (0) - (\infty)$ in $J(S)$.

Hence $(0) - (\infty)$ must be the divisor of function on $X_0(p)$, and we have that

$$f(0) = f(\infty).$$

Now, by proposition 5.13 we obtain that $p \leq 13$, which is a contradiction (the ultimate reason is that for $p > 13$ the modular curve $X_0(p)$ has genus ≥ 1 and we get a contradiction with the Riemann-Roch theorem). Therefore, we can conclude that $\mathbb{Z}/p\mathbb{Z}(\mathbb{F}_q) \not\subset \mathcal{E}(\mathbb{F}_q)^0$. □

6. Appendix

1. Mazur's theorem ensures that elliptic curves over $\mathbb{Q}$ do not have a rational torsion point of primer order $p > 13$. The case $p = 11$ is also excluded in the list of possible torsion subgroups. The reason is as follows. The modular curve $X_1(11)$ classifying elliptic curves with a point of order 11 has genus one. In fact, it can be seen that $X_1(11)$ is our elliptic curve 11B in the introduction, given by the Weierstrass equation:

$$y^2 + y = x^3 - x^2\,.$$

The five rational torsion points corresponds to the rational cusps of $X_1(11)$. The elliptic curve 11A in the introduction corresponds to the modular curve $X_0(11)$ (see [9] for more information).

2. The Lutz-Nagell theorem gives an efficient algorithm to compute the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$. This theorem is more modest than Mazur's theorem, but still forceful enough to make it possible to determine the torsion group of any specific elliptic curve, at least if one knows a Weierstrass equation for it. So the point of departure is an elliptic curve over $\mathbb{Q}$ with an integral Weierstrass equation:

$$y^2 = x^3 + ax + b\,,$$

where a and b are in $\mathbb{Z}$. Any Weierstrass equation can be brought onto this form by an admissible change of coordinates. The discriminant $\Delta = 27b^2 + 4a^3$ plays a prominent role in the theorem.

Theorem 6.1. (Lutz-Nagell). *If the elliptic curve $E/\mathbb{Q}$ has the integral Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$ and $P = (x, y) \in E(\mathbb{Q})$ is a nonzero torsion point. Then x and y are integers, and either $y = 0$ or y^2 is a divisor in the discriminant Δ , that is $y^2|\Delta$.*

Proof. See [4], page 221. □

3. The following is a list of elliptic curves with each possible torsion subgroup. The web page of Tom Womack contains PARI code that lists elliptic curves over $\mathbb{Q}$ with each of the fifteen possibilities of torsion subgroups. We can obtain more information in [7], page 4.

Curve	$E(\mathbb{Q})_{\text{tors}}$
$y^2 = x^3 - 2$	$\{0\}$
$y^2 = x^3 + 8$	$\mathbb{Z}/2\mathbb{Z}$
$y^2 = x^3 + 4$	$\mathbb{Z}/3\mathbb{Z}$
$y^2 = x^3 + 4x$	$\mathbb{Z}/4\mathbb{Z}$
$y^2 - y = x^3 - x^2$	$\mathbb{Z}/5\mathbb{Z}$
$y^2 = x^3 + 1$	$\mathbb{Z}/6\mathbb{Z}$
$y^2 = x^3 - 43x + 166$	$\mathbb{Z}/7\mathbb{Z}$
$y^2 + 7xy = x^3 + 16x$	$\mathbb{Z}/8\mathbb{Z}$
$y^2 + xy + y = x^3 - x^2 - 14x + 29$	$\mathbb{Z}/9\mathbb{Z}$
$y^2 + xy = x^3 - 45x + 81$	$\mathbb{Z}/10\mathbb{Z}$
$y^2 + 43xy - 210y = x^3 - 210x^2$	$\mathbb{Z}/12\mathbb{Z}$
$y^2 = x^3 - 4x$	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
$y^2 = x^3 + 2x^2 - 3x$	$(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
$y^2 + 5xy - 6y = x^3 - 3x^2$	$(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$
$y^2 + 17xy - 120y = x^3 - 60x^2$	$(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

We calculate, for example, the torsion points of the curve

$$E_1 : y^2 + xy + y = x^3 - x^2 - 14x + 29$$

If we look at the table, we see that E_1 is isomorphic to $\mathbb{Z}/9\mathbb{Z}$. So we will have 9 torsion points.

Torsion points of $E_1(\mathbb{Q})$		
$(0 : 1 : 0)$	$(-3 : 7 : 1)$	$(9 : -29 : 1)$
$(1 : 3 : 1)$	$(3 : -5 : 1)$	$(3 : 1 : 1)$
$(1 : -5 : 1)$	$(9 : 19 : 1)$	$(-3 : -5 : 1)$

We can calculate the torsion points of the curve

$$E_2 : y^2 + 5xy - 6y = x^3 - 3x^2$$

If we look at the table, we see that E_2 is isomorphic to $(\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$. So we will have 12 torsion points.

Torsion points of $E_2(\mathbb{Q})$		
$(0:1:0)$	$(0:6:1)$	$(3:0:1)$
$(-6:18:1)$	$(3:-9:1)$	$(0:0:1)$
$(2:-2:1)$	$(-3:3:1)$	$(12:-72:1)$
$(3/4:9/8:1)$	$(12:18:1)$	$(-3:18:1)$

4. Barry Mazur formulated the Strong Uniform Boundedness Conjecture, asserting that the cardinality of $E(K)_{tors}$ can be bounded above by a constant which depends only on the degree of $K/\mathbb{Q}$. This conjecture was proved in 1994 by Loïc Merel. He proved the following generalization of Mazur's theorem (see [8]):

Theorem 6.2. (Merel 1994). *For all $d \in \mathbb{Z}$, $d \geq 1$ there exists a constant $B(d) \geq 0$ such that for all elliptic curves E over a number field K with $[K:\mathbb{Q}] = d$ then*

$$|E(K)_{\text{tors}}| \leq B(d).$$

References

[1] B. Schwartz (2004), Thesis: *Elliptic Curves, Group Schemes, and Mazur's Theorem*. Harvard University, Cambridge, Massachusetts.

[2] A. Néron (1964), *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux*, Publications Mathématiques de l'IHÉS, 21: 5–128, doi:10.1007/BF02684271, ISSN 1618-1913, MR 0179172.

[3] L. Magistrale (2004), Master Thesis: *The Néron-Ogg-Shafarevich Criterion*. Università Degli Studi di Padova.

[4] J. Silverman (2009), *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106, Springer-Verlag. University of California at Berkeley, CA 94720-3840. ISBN 978-0-387-09493-9.

[5] J. Silverman (1994), *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics 151, Springer-Verlag. Berkeley, CA 94720-3840. ISBN 978-0-387-94328-2.

[6] S. Lichtenstein (2011), *Néron Models.*. Stanford. `http://virtualmath1.stanford.edu/~conrad/mordellsem/Notes/L11.pdf`.

[7] W. Stain (2001), *Lecture 27: Torsion Points on Elliptic Curves and Mazur's Big Theorem.* Harvard University. Math 124. `https://wstein.org/edu/Fall2001/124/lectures/`.

[8] M. Rebolledo (2009), Thesis: *Merel's theorem on the boundedness of the torsion of elliptic curves*. Université Clermont Auvergne. `http://math.univ-bpclermont.fr/~rebolledo/page-fichiers/07-goettingen.pdf`.

[9] T. Weston (2001), *The Modular Curves $X_0(11)$ and $X_1(11)$*. Modular Forms, The University of Arizona. `https://www.math.arizona.edu/~swc/aws/2001/`.

[10] Z. Borevich and I. Shafarevich (1966), *Number Theory*. Academic Press INC, London LTD. Library of Congress Catalog Card Number: 65-28624.

[11] A. V. Sutherland (2012), *Torsion subgroups of elliptic curves over number fields*. Harvard University. `http://www.math.harvard.edu/~chaoli/MazurTorsionSeminar.html`.

[12] J. Tate (2006), *Algorithm for determining the type of a singular fiber in an elliptic pencil.* Modular Functions of One Variable IV, 1975, Volume 476. ISBN 978-3-540-07392-5.

[13] D. Kohel (1996), Thesis: *Endomorphism rings of elliptic curves over finite fields*. University of California, Berkeley. `http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf`.

[14] M. Kosters and R. Pannekoek (2017), *On the structure of elliptic curves over finite extensions of $\mathbb{Q}_p$ with additive reduction*. Corpus ID: 119131463.Archiv: 1703.07888v1 [math.AG].

[15] S. Dembner (2019), Thesis: *Torsion on Elliptic Curves and Mazur's Theorem.* `http://math.uchicago.edu/~may/REU2019/REUPapers/Dembner.pdf`.

[16] B. Mazur (1977), *Modular curves and the Eisenstein ideal*. IHES Publ. Math.47, 33-186. `http://www.numdam.org/item?id=PMIHES_1977__47__33_0`.

[17] B. Mazur (2010), *How can we construct abelian Galois extensions of basic number fields?*. Bulletin (New Series) of the American Mathematical Society. Volume 48, Number 2, Pages 155–209. S 0273-0979(2011)01326-X.

[18] B. Mazur (1978), *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*. In: Invent. Math. 44.2, pp. 129–162.

[19] J. Tate (1997), *Finite at group schemes. In Modular Forms and Fermat's Last Theorem*, pages 121-154. Springer.

[20] F. Najman (2011), *Torion of elliptic curves over quadratic cyclotomic fields*. Math. J. Okayama Univ. 53, 75–82.

[21] A. V. Sutherland (2011), *Constructing Elliptic Curves Over Finite Fields With Prescribed Torsion*. Volume 81, Number 278, Pages 1131–1147.

[22] E. Gonzalez and J. M. Tornero (2010), *On the ubiquity of trivial torsion on elliptic curves*. Arch. Math. 95, 135–141.

[23] G. Shimura (1971), *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton Univ. ISBN-10: 0691080925.

[24] F. Oort and J. Tate (1970), *Group schemes of prime order*. Ann. Sci. École Norm. Sup. (4) 3, 1-21.