國立臺灣大學理學院數學系

碩士論文

Department of Mathematics

College of Science

National Taiwan University

Master Thesis

橢圓曲線上有理點的質階數

The Prime Order of Rational Points on Elliptic Curves

蘇邦彥

Ban-Yan Su

指導教授：陳其誠 教授

Advisor: Ki-Seng Tan, Prof.

中華民國 99 年 1 月

January, 2010

誌謝

首先在此感謝我的指導教授陳其誠教授，在我完成論文的期間能夠不厭其煩的一而再、再而三的講解我不清楚的部分，並且給予許多不管是在學習上或是生活上的建議，以及感謝各位口試委員能夠抽空前來參與我的論文口試。最後要感謝我的家人與朋友在這段期間給我的許多生活上的協助以及建議。

中文摘要

本論文考慮的問題是：考慮一個橢圓曲線上的有理點，若此有理點的階數是質數，則此質數可能是哪些？最後的結論是 2、3、5、7 或 13。

第一章我們簡單介紹這個問題的來源，而在第二章和第三章我們回顧一些在證明中所需要用到的橢圓曲線性質以及 Class Group 的理論，並且在第四章證明這件事情。

Abstract

In this thesis, our goal is to answer the question: Given an elliptic curve defined over Q, suppose it has a rational point of prime order, then what may this prime be? The conclusion is 2,3,5,7 or 13.

In chapter 1, we give an introduction of this question. Then we review some properties of elliptic curves and class group in chapter 2 and chapter 3, and give a proof of the above fact in chapter 4.

Contents

Chapter 1

Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$. By definition, E poses a structure of abelian group ([1], chap. III, § 2), and according to Mordell-Weil Theorem (loc.cit., chap. VIII), the Mordell-Weil group $E(\mathbb{Q})$ that consists of rational points of E over $\mathbb{Q}$ is a finitely generated abelian group. Moreover, the fascinating theorem of Mazur ([2], chap. III, § 5) tells us that the torsion subgroup of $E(\mathbb{Q})$ must be isomorphic to one of the following 15 groups:

$$\mathbb{Z}/N\mathbb{Z}, \text{ for } 1 \leq N \leq 10 \text{ or } N = 12 \ ;$$

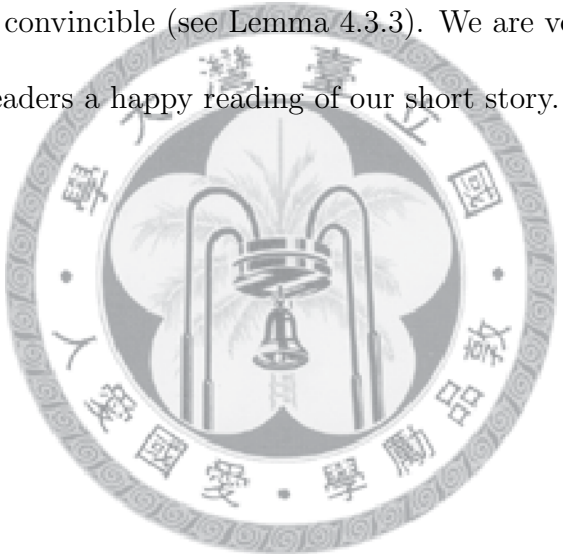
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \text{ for } 1 \leq N \leq 4.$$

The main step to prove Mazur's theorem is the following:

Theorem I: *Let E be an elliptic curve defined over $\mathbb{Q}$. Then E contains no $\mathbb{Q}$-rational point of prime order p, unless $p = 2, 3, 5, 7,$ or 13.*

Judging from the content of the paper [2], one might think that this theorem is still too much technically involved to be the subject of study for even an advanced master-degree thesis. However, by more careful readings of documents, we have

persuaded ourselves that it is possible to write an article explaining the proof of Theorem I, based on background knowledge understandable to normal graduate students, as long as we organize our story in a way that some of the main characters are either well known or convincible, and hence they can be introduced without much elaboration. Thus, the main theme of this thesis is set in such fashion. It turns out that in our story there will be two "characters" introduced without giving proofs of their "validation". One is Faltings theorem (see Section 4.1), which we considered as well-known, and the other is Mazur's unramified theorem, Theorem 4.3.2, which we shall try to make convincible (see Lemma 4.3.3). We are very satisfied with the work and wish the readers a happy reading of our short story.



Chapter 2

Properties of Elliptic Curves

The material of this chapter can be found in [1], chap. III and chap. VII

2.1 The Weil Pairing

Let E be an Elliptic curve defined over a number field K, and let $E[n]$ denotes the n-torsion subgroup of $E(\bar{K})$ for n$\in \mathbb{N}$. Here $\bar{K}$ denote the separable closure of K. The structure of $E[n]$ is well known:

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

Let μ_n denote the group of n'th roots of unity.

Proposition 2.1.1: *There exists the Weil pairing*

$$e_n : E[n] \times E[n] \longrightarrow \mu_n$$

that satisfies

(a) *Bilinear:* $e_n(S_1+S_2, T) = e_n(S_1, T)e_n(S_2, T)$, *and* $e_n(S, T_1+T_2) = e_n(S, T_1)e_n(S, T_2)$

(b) *Alternating:* $e_n(T, T)=1$

(c) *Non-degenerate: If* $e_n(S,T) = 1$, *for all* $S \in E[n]$, *then* $T = 0$

(d) *Galois invariant:* ${}^{\sigma}e_n(S,T) = e_n({}^{\sigma}S, {}^{\sigma}T)$ *for all* $\sigma \in \mathrm{Gal}(\bar{K}/K)$

To define the Weil pairing, we need the following lemma. Let $[n]$ denote the multiplication by n on E.

Lemma 2.1.2: *Suppose* $P_i \in E(\bar{K})$, *for* $i = 1, ..., k$ *then the divisor* $\Sigma_{i=1}^{k} n_i \cdot (P_i)$ *is the divisor of a rational function on* E *if and only if the integer* $\Sigma_{i=1}^{k} n_i = 0$ *and the point* $\Sigma_{i=1}^{k}[n_i]P_i = 0$.

By the above lemma, for each $T \in E[n]$, there exit a rational function f such that

$$div(f) = n(T) - n(O).$$

Also, for a point $T' \in E(\bar{K})$ with $[n]T' = T$, there exit a rational function g such that

$$div(g) = \Sigma(T' + R) - (R), \ where \ R \in E[n].$$

Then, for each $S \in E[n]$, the Weil pairing is defined as

$$e_n(S,T) = g(X+S)/g(X) \in \mu_n.$$

Corollary 2.1.3: *If* $E[n]$ *is contained in* $E(K)$, *then* $\mu_n \subset K^*$.

Proof. The non-degenerate property of the pairing implies the surjectivity, and hence there exist points $S,\ T \in E[n]$ so that $e_n(S,T)$ is a primitive n'th root of unity. Since $e_n(S,T) = e_n({}^{\sigma}S, {}^{\sigma}T) = {}^{\sigma}e_n(S,T)$, we conclude that $e_n(S,T) \in K^*$. □

2.2 Elliptic curves over local fields

In this section we assume that E is an elliptic curve defined over a local field K that is complete with respect to a discrete valuation ν. Let R denotes the ring of integers of K, π denote an uniformizer of R and $\mathbb{F}_K$ denote the residue field of R.

We assume that E is defined by a minimal Weierstrass equation

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

for each i let $\tilde{a}_i$ denote the reduction of a_i modulo π, and set the reduction of E modulo π as

$$\tilde{E} : y^2 + \tilde{a_1}xy + \tilde{a3}y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

The cubic curve $\tilde{E}$ contains at most one singular point which, if exists, is rational over $\mathbb{F}_K$. We say that E has good (resp. multiplicative, additive) reduction, if $\tilde{E}(\mathbb{F}_K)$, and hence $\tilde{E}$, contains no singular point (resp. a node, a cusp). Furthermore, E has split (resp. non-split) multiplicative reduction, if it has multiplicative reduction and the two tangent lines at the node are rational (resp. not rational) over $\mathbb{F}_K$. In any case, the set of non-singular points, denoted by $\tilde{E}_{ns}(k)$, still form a group. If E has god reduction, then $\tilde{E}$ is an elliptic curve. In general, if $\mathbb{F}_K(\sqrt{d})$ denotes the quadratic extension of $\mathbb{F}_K$, then we have

$$\tilde{E}_{ns}(k) \simeq \begin{cases} \mathbb{F}_K^*, & \text{if } E \text{ has split multiplicative reduction;} \\ \mathbb{F}_K(\sqrt{d})^*/\mathbb{F}_K^*, & \text{if } E \text{ has non-split multiplicative reduction;} \\ \mathbb{F}_K, & if\ E \text{ has additive reduction.} \end{cases} \tag{2.1}$$

For a point $P \in E(K)$, let $\tilde{P}$ denote its reduction modulo π, and set

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\}$$

$$E_1(K) = \{P \in E(K) : \tilde{P} = 0\}.$$

Then both $E_0(K)$ and $E_1(K)$ are subgroup of $E(K)$ and we have the exact sequence of abelian groups

$$0 \to E_1(K) \to E_0(K) \to \tilde{E}_{ns}(k) \to 0, \tag{2.2}$$

where the right-hand map is reduction modulo π. Certainly, $E(K)/E_0(K)$ is trivial, if E has good reduction. On the other hand, we have

Lemma 2.2.1: *If E has either non-split multiplicative reduction or additive reduction, then the order of $E(K)/E_0(K)$ is at most 4. If E has split multiplicative reduction, then $E(K)/E_0(K)$ is a finite cyclic group.*

There is associated a formal group law $\mathfrak{F}$, so that for each $k = 1, ...,$ the set $\mathfrak{F}(\pi^k \cdot R)$ form a group with

$$\mathfrak{F}(\pi \cdot R) \simeq E_1(K) \tag{2.3}$$

and

$$\mathfrak{F}(\pi^k \cdot R)/\mathfrak{F}(\pi^{k+1} \cdot R) \simeq \mathbb{F}_K. \tag{2.4}$$

We shall identify $\mathfrak{F}(\pi \cdot R)$ with $E_1(K)$ using (2.3) and denote $E_k(K) = \mathfrak{F}(\pi^k \cdot R)$. Thus, we have the filtration:

$$\cdots E_{k+1}(K) \subset E_k \subset \cdots \subset E_1(K) \subset E_0(K) \subset E(K), \tag{2.5}$$

so that the decomposition factors are described as above.

Lemma 2.2.2: *If E has good reduction and p is prime to the characteristic of $\mathbb{F}_K$, then the extension $K(E[p])$ is unramified over K.*

Lemma 2.2.3: *Suppose E is defined over $\mathbb{Q}_p$ with good reduction and $P \in E(\mathbb{Q}_p)$ is a point of order p. Then $P \notin E_1(\mathbb{Q}_p)$.*

Proof. Write $P = (x, y)$. Then we have

$$p^{2r}x(P),\ p^{3r}y(P) \in \mathbb{Z}_p,\ \text{with } r = [\frac{1}{p-1}] = 0.$$

In other words, both $x, y \in \mathbb{Z}_p$, and hence $\tilde{x} \neq \infty$ and $\tilde{y} \neq \infty$.

□

2.3 Isogenies

In this, section, assume that E is an elliptic curve defined over a field extension of $\mathbb{Q}$. Suppose E'/K is another elliptic curve and $\varphi : E \longrightarrow E'$ is an isogeny of degree n. Then $\ker(\varphi)$ is a subgroup of $E[n]$ of order n. Furthermore, it is in fact defined over K stable. In other words, the action of the Galois group $\mathrm{Gal}(\bar{K}/K)$ stable $\ker(\varphi)$. The converse is also true. If Λ is a subgroup of $E[n]$ stable under the action of $\mathrm{Gal}(\bar{K}/K)$ with $|\Lambda| = n$, then there is a degree n isogeny $\varphi : E \longrightarrow E'$ defined over K with $\ker(\varphi) = \Lambda$.

Lemma 2.3.2: *Suppose φ is an endomorphism of an elliptic curve E defined over $\mathbb{R}$. If φ is also defined over $\mathbb{R}$, then $\varphi \in \mathbb{Z}$.*

Proof. Let E and φ have the property as assumption. We can choose a suitable lattice $\Lambda \subset \mathbb{C}$ such that $E \cong \mathbb{C}/\Lambda$ related by Weierstrass $\mathfrak{p}$-function and Λ is an ideal of $\mathfrak{R}$, where $\mathfrak{R}$ is a ring of integer of a quadratic imaginary field. The endomorphism φ corresponds to complex multiplication by $\alpha \in \mathfrak{C}$, that is, for $z \in \mathbb{C}/\Lambda$ corresponds to a point $P \in E$, then αz corresponds to $\varphi(P)$. Also, since elements in Λ has the form

$$\mathbb{Z} + \mathbb{Z}\sqrt{-d} \text{ or } \frac{\mathbb{Z} + \mathbb{Z}\sqrt{-d}}{2}$$

, we have $\overline{\Lambda} = \Lambda$, therefore

$$\mathfrak{p}(\overline{z};\Lambda) = \frac{1}{\overline{z}^2} + \sum_{\omega \neq 0 \in \Lambda} \frac{1}{(\overline{z}-\omega)^2} - \frac{1}{\omega^2} = \overline{\mathfrak{p}(z;\Lambda)}$$

, similarly $\mathfrak{p}'(\overline{z}) = \overline{\mathfrak{p}'(z)}$, thus $\overline{z}$ will correspond to $\overline{P}$. By above discussion, we have that $\alpha\overline{z}$ corresponds to $\varphi(\overline{P})$, and $\overline{\alpha z}$ corresponds to $\overline{\varphi(P)}$. But $\varphi(\overline{P}) = \overline{\varphi(P)}$ since φ is defined over $\mathbb{R}$. This force $\alpha\overline{z} = \overline{\alpha z}$ for arbitrary $z \in \mathbb{C}$, thus $\alpha \in \mathbb{R}$. Meanwhile, α must send the lattice Λ to itself, thus $\alpha \in \mathbb{Z}$ and hence the proof. □

Chapter 3

The Class Group

The main reference of this chapter is [4], chap. V, and [3], §6.3

3.1 Ideal Class Group and Hilbert Class Field

In this section, we review a basic fact from the class field theory. Let K be a number field, and let R be the ring of integers of K. The equivalence class of nonzero ideals of R under the relation:

$$I \sim J, \text{ if } \alpha I = \beta J, \text{ for some non zero } \alpha,\ \beta \in R,$$

together with ideal multiplication as operation form a *finite abelian group* $\mathfrak{C}_K$ called **the ideal class group** of K. Its order of is called the **class number** of K, denoted as h_K. Also, the maximal abelian unramified extension of K, called **Hilbert class field**, satisfies the following property:

Proposition 3.1.1: *Let K be a number field and H be the Hilbert class field of*

K. Then H/K is a Galois extension with Gal(H/K) isomorphic to the ideal class group of K.

Suppose K/k is a finite Galois extension with $\mathrm{Gal}(K/k) = \Gamma$. Then Γ acts on $\mathfrak{C}_K$ via its action on the set of ideals of R. Furthermore, H/k is also a Galois extension and Γ acts on $\mathrm{Gal}(H/K)$ via the conjugation (in $\mathrm{Gal}(H/k)$) $g \mapsto \sigma g \sigma^{-1}$, for $g \in \mathrm{Gal}(H/K)$, $\sigma \in \Gamma$. Then the isomorphism in Proposition 3.1.1 respects these Γ actions.

3.2 Irregular Prime and Herbrand-Ribet Theorem

Let p be an odd prime number and let $K = \mathbb{Q}(\mu_p)$, the p'th cyclotomic field. Then p is an **irregular prime**, provided it divides the class number h_K. The celebrated theory of Kummer says that p is an irregular prime if and only if it divides the product

$$\prod_{k=1}^{\frac{p-3}{2}} B_{2k},$$

of Bernoulli numbers. Moreover, the question which Bernoulli numbers a irregular prime exactly divides is answered by the theorem Herbrand-Ribet quoted below.

For convenience, we choose a generator ζ of the group μ_p which is considered as a subgroup of $\mathbb{Z}[\zeta]$, the ring of integers of K. Let A be the p-Sylow subgroup of ideal class group of K and let Γ denote the Galois group $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Then A is a Γ-module and, since the order of Γ is prime to p, can be decomposed as a direct sum of eigen-spaces. Let $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \mu_{p-1}$ be the Teichmüller character

that is the inverse of the composition:

$$\mu_{p-1} \hookrightarrow \mathbb{Z}[\zeta] \longrightarrow \mathbb{Z}[\zeta]/(1-\zeta) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^{\times}.$$

Every (Dirichlet) character of $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is of the form ω^i for some $i = 0, 1, ..., p-2$. For each i, let

$$\epsilon_i = \frac{1}{p-1} \sum_{a=1}^{p-1} \omega^i(a)\sigma_a^{-1} \in \mathbb{Z}_p[G].$$

Then $\epsilon_i \cdot \epsilon_j = 0$, if $i \neq j$, $\epsilon_i \cdot \epsilon_i = 1$ and $\sum_{i=0}^{p-2} \epsilon_i = 1$. Also, if we identify Γ with $(\mathbb{Z}/p\mathbb{Z})^{\times}$, then $\sigma \cdot \epsilon_i = \omega^i(\sigma) \cdot \epsilon_i$. Thus, for each i, the subgroup $A_i := \epsilon_i \cdot A$ is the ω^i-eigen-space of A so that

$$A = \bigoplus_{i=0}^{p-2} A_i.$$

.

Theorem 3.2.1 (Herbrand-Ribet): *The eigen-space A_i is nontrivial, if and only if p divides B_{p-i}.*

We shall need to apply the "only if" part of the theorem, which is exactly the classical Herbrand theorem.

Corollary 3.2.2: *Suppose we are given a finite Galois extension L over k, which contains K so that L/K is a non-trivial everywhere unramified abelian p extension and the Galois group $Gal(L/K)$ is actually an ω^i-eigen-space under the conjugation action of Γ. Then p must divides B_{p-i}.*

Proof. We have the projection $\pi : \mathfrak{C}_K \xrightarrow{\sim} \mathrm{Gal}(H/K) \longrightarrow \mathrm{Gal}(L/K)$. Also, $\mathfrak{C}_K = A \times C$ with $|C|$ prime to p and the restriction of π to C is trivial. Therefore, the projection π sends A surjectively to $\mathrm{Gal}(L/K)$. This implies that A_i is non-trivial.

□

Chapter 4

The Proof of Theorem I

4.1 Faltings' theorem

Here we quote a famous theorem of Faltings.

Theorem (Faltings): *If X is an algebraic curve defined over a number field K with the genus greater than 1, then X contains only finitely many K-rational points.*

4.2 The modular curves $X_0(p)$ and $X_1(p)$

The following theorem is first proved in [2], chap. III.

Theorem 4.2.1: *If p is prime number and not equal to $2, 3, 5, 7$ or 13, then $X_0(p)$ contains only finitely many $\mathbb{Q}$-rational points.*

What we really need is the following, for which we give a proof using Faltings theorem.

Theorem 4.2.2: *If p is prime number and not equal to $2, 3, 5, 7$, then $X_1(p)$ contains only finitely many $\mathbb{Q}$-rational points.*

Proof. From [5],§ 9.1, the genus of $X_1(N)$ is 0 if $N \leq 4$, and for $N \geq 5$ the genus of $X_1(N)$ is given by

$$g = 1 + \frac{N^2}{24}\prod_{p|N}(1-p^{-2}) - \frac{N}{4}\prod_{p|N}[1-p^{-2}+\upsilon_p(N)(1-p^{-1})^2].$$

Thus for prime N, the genus of $X_1(N)$ is given by

$$g = 1 + \frac{N^2}{24}\prod_{p|N}(1-p^{-2}) - \frac{N}{4}\prod_{p|N}[1-p^{-2}+(1-p^{-1})^2] = \frac{(N-5)(N-7)}{24}.$$

We conclude that the genus of $X_1(p)$ is greater than 1 if $p \geq 13$. Then by Faltings' theorem, $X_1(p)$ contains only finitely many $\mathbb{Q}$-rational points if $N \geq 13$, i.e. $p \neq 2, 3, 5, 7, 11$. To complete the proof, it remains to check the case $p = 11$. For the case $p = 11$, the genus of $X_1(11) = 1$ which implies that it is an elliptic curve. From [6],§ 4.2, the minimal equation for $X_1(11)$ is

$$y^2 + y = x^3 - x^2$$

which has only 5 $\mathbb{Q}$-rational points, $\{O, (0,0), (0,-1), (1,0), (1,-1)\}$.

□

4.3 The field generated by $E[p]$

From now on, we assume that E is an elliptic curve defined over $\mathbb{Q}$ and $P \in E(\mathbb{Q})$ is a point of order p. We choose another point $Q \in E[p]$ so that P and Q generate $E[p]$. Let $L = \mathbb{Q}(P, Q)$ be the field extension generated by (the coordinates of) P and Q. As before, let K denote the cyclotomic field $\mathbb{Q}(\mu_p)$ and let $\zeta = e_p(P, Q)$ that is a generator of μ_p (as e_p is non-degenerated). Then Corollary 2.1.3 implies that L is a field extension of K. Set G =Gal$(L/\mathbb{Q})$ and Γ =Gal$(K/\mathbb{Q})$. Then Γ acts on Gal(L/K) via the conjugation.

As G acts on $E[p]$ which is in fact a 2-dimensional $\mathbb{F}_p$-vector space with P and Q as basis, there is associated a representation

$$\rho : G \longrightarrow \mathrm{GL}_2(\mathbb{F}_p).$$

Since P is fixed by every $\sigma \in G$, we have

$$\rho(\sigma) = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$$

with $a \in \mathbb{F}_p, b \in \mathbb{F}_p^*$. Also,

$${}^{\sigma}\zeta = {}^{\sigma}e(P,Q) = e({}^{\sigma}P, {}^{\sigma}Q) = e(P, aP + bQ) = e(P,Q)^b = \zeta^b.$$

This implies the following lemma.

Lemma 4.3.1: *Let notation be as above. Then the restriction of Galois action*

$$G \longrightarrow \Gamma$$

is given by $\sigma \mapsto b$. Furthermore, the Galois group $\mathrm{Gal}(L/K)$ is either trivial or of order p.

Theorem 4.3.2: *If p is prime number and not equal to $2, 3, 5, 7$ or 13, then, the extension L/K is everywhere unramified.*

The theorem is proved by Mazur in [2]. We are not able to reproduce it here. However, we can treat the following cases. First, L/K is unramified at ∞, since we already have $K_\infty = \mathbb{C}$.

Lemma 4.3.3: *Suppose $p \neq 2, 3$. Then the extension L/K is unramified at a place v if v satisfies any of the following conditions:*

1. *E has good reduction at p and v is sitting over p.*

2. *E has good reduction at v and v is not sitting over p.*

3. *E has additive reduction at v and v is not sitting over p.*

4. *E has non-split multiplicative reduction at v.*

Proof. Suppose the lemma do not hold and L/K is ramified (and hence totally ramified). Let L_v and K_v denote the completion of L and K.

If E has good reduction at p, then by Lemma 2.2.3, $P \notin E_1(\mathbb{Q}_p)$, and since in this case the formal group law is stable over the field extension $L_v/\mathbb{Q}_p$, we have $P \notin E_1(L_v)$. Also, since the residual characteristic of L_v equals p, $\tilde{E}[p] \simeq \mathbb{Z}/p\mathbb{Z}$ and is generated by the reduction $\tilde{P}$. This means we can choose Q so that $\tilde{Q} = 0$ and hence $Q \in E_1(L_v)$. Now, $L_v/\mathbb{Q}_p$ is totally ramified with Galois group G and the group $E_1(L_v) \cap E[p]$, which is generated by Q, is stable under the action of G. Consequently, the representation ρ must be reducible and we shall have $G \simeq \Gamma$, a contradiction.

For the rest of the proof, we assume that v is not sitting over p. If E has good reduction at v, then $L_v/\mathbb{Q}_p$ is unramified by Lemma 2.2.2.

If E over L_v has either additive or non-split multiplicative reduction, then Lemma 2.2.1 together with (2.1) as well as the filtration (2.5) implies $E(L_v) \cap E[p]$ is either trivial or cyclic. This contradicts to the fact that $E[p] \subset E(L_v)$.

Finally, if E has additive reduction over K_v, while it has either good reduction or split multiplicative reduction over L_v, then the minimal Weierstrass equation of E over L_v must be changed due to the change of coordinate $(x', y') = (\pi_L^{-2r} \cdot x, \pi_L^{-3r} \cdot y)$.

Again, Lemma 2.2.1, (2.1) and (2.5) tell us that $P \in E_0(K_v)$ and hence from the above change of coordinate, we should have $P \in E_1(L_v)$. But this is absurd, since, by (2.5), $E_1(L_v)$ is a q-group where q is the residual characteristic of v.

□

4.4 The proof

Now We complete the proof of Theorem I.

Proof. Assume that the theorem does not hold and there is an elliptic curve $E/\mathbb{Q}$ with a $\mathbb{Q}$-rational point P of order p for some p not equal $2, 3, 5, 7, 13$. Then keep the notation used in Section 4.3.

First, consider the case where $L \neq K$. Then, as $L/\mathbb{Q}$ is a Galois extension, $\mathrm{Gal}(L/K)$ is a Γ-module and hence, as it is of dimension 1 over $\mathbb{F}_p$, must be an eigen-space. In fact, from

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}^{-1} = \begin{pmatrix} 1 & b^{-1}x \\ 0 & 1 \end{pmatrix}$$

we can conclude that it is an ω^{-1}-eigen-space. Since $\omega^{-1} = \omega^{p-2}$, by Corollary 3.2.2, p must divide (the numerator of) $B_2 = 1/6$. This is impossible.

Therefore, we can assume that $K = L$, always. Then the representation ρ is reducible and there is a splits exact sequence of Gal $(\bar{\mathbb{Q}}/\mathbb{Q})$-modules:

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

where the left-hand map is the composition $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} < P > \hookrightarrow E[p]$ and the right-hand one is given by $T \mapsto e(T, P)$, with a section $\mu_p \longrightarrow E[p]$ given by $\zeta^l \mapsto lQ$.

Consider the isogeny

$$\varphi : E \longrightarrow E_1 = E/\mu_p$$

given by the quotient map. Then $P_1 = \varphi(P) \in E_1$ is a $\mathbb{Q}$-rational point of order p, and our assumption implies that $L_1 := \mathbb{Q}(E_1[p]) = K$, and hence $E_1[p]$ splits as the direct product of $\mathbb{Z}/p\mathbb{Z}$ with μ_p. Therefore, We can form the isogeny

$$\varphi_1 : E_1 \longrightarrow E_2 = E_1/\mu_p$$

and so on. Thus, we have obtained a sequence of μ_p-isogenies

$$E_0 = E \xrightarrow{\varphi} E_1 \xrightarrow{\varphi_1} E_2 \xrightarrow{\varphi_2} ....$$

with a non-trivial point $P_i \in E_i[p]$, for each $i = 0, 1, ...$ Each pair (E_i, P_i) gives rise to a $\mathbb{Q}$-rational point on $X_1(p)$. By Theorem 4.2.2, there are only finitely many such point, and hence we must have an isomorphism $\psi : E_i \simeq E_j$ for some i and $j > i$. Since, from our construction, the point P_i is not contained in the kernel of the composition $\psi_i : E_i \xrightarrow{\varphi_i} \cdots \xrightarrow{\varphi_{j-1}} E_j$, which is of degree p^{j-i}, the endomorphism $\psi^{-1} \circ \psi_i \in \mathrm{End}(E_i)$ cannot be contained in $\mathbb{Z}$. But, since $\psi^{-1} \circ \psi_i$ is defined over $\mathbb{Q}$, Lemma 2.3.2 says it must be contained in $\mathbb{Z}$. This is a contradiction.

□

Bibliography

[1] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer, 1986.

[2] B. Mazur, Modular curves and the Eisenstein ideal, Publications Mathématiques de L'IHÉS Volume 47, Number 1 (1977), 33-186.

[3] Lawrence C. Washington, Introduction to Cyclotomic Fields, Springer, 1982.

[4] Daniel A. Marcus, Number Fields, Springer, 1977.

[5] Fred Diamond and John Im, Modular forms and modular curves, Seminar on Fermat's last theorem : 1993-1994, the Fields Institute for Research in the Mathematical Sciences, Toronto, Ontario, Canada (1995), 39-133.

[6] Yifan Yang, Defining equations of modular curves, Advances in Mathematics Volume 204, Issue 2 (2006), 481-508.