

# REPORT

University of Georgia  
Department of Mathematics  
Sungkon Chang

[schang@math.uga.edu](mailto:schang@math.uga.edu)

# Contents

1	Introduction . . . . .	2
2	The $p$ -descent on an elliptic curve $E/\mathbb{Q}$ . . . . .	3
	2.1 Definition of the $m$ -Selmer Group . . . . .	3
	2.2 Schaefer's Algorithm . . . . .	4
3	The Étale Algebras . . . . .	6
	3.1 The étale algebra $A$ . . . . .	6
	3.2 The étale algebra $B$ . . . . .	9
	3.3 The main theorem of the $p$ -descent on an elliptic curve . . . . .	11
	3.4 Notes on Schaefer-Stoll's description . . . . .	12
4	Implementation of Finding the Generators of $H^1(\mathbb{Q}, E[3])_S$ . . . . .	14
	4.1 Generators of $A(S, 3)$ . . . . .	14
	4.2 Performing the section map in <code>gp-pari</code> . . . . .	15
	4.3 Checking the conditions (6) with <code>gp-pari</code> . . . . .	15
5	Local Conditions . . . . .	16
	5.1 Local condition at $q \neq 3$ . . . . .	17
	5.2 Local condition at $q = 3$ . . . . .	19
6	Program: <code>selmer3333.gp</code> . . . . .	22
	6.1 Other Outputs . . . . .	23
	6.2 Running <code>selmer3333.gp</code> . . . . .	23
	6.3 Known bugs . . . . .	24

## 1 Introduction

Let  $K$  be a field of characteristic 0. An elliptic curve  $E/K$  is a nonsingular projective curve given by the equation:  $zy^2 = x^3 + az^2x + bz^3$  where  $a$  and  $b$  are elements of  $K$ . An elliptic curve is an abelian variety, i.e., a smooth projective variety with algebraic group law. For a(n) (algebraic) field extension  $L$  of  $K$ , we will denote by  $E(L)$  the subgroup of  $E(\bar{K})$  consisting of the points which are *defined over*  $L$ . The following theorem is well-known:

**Theorem 1.1 (Mordell-Weil Theorem)** *Let  $K$  be a number field, and  $E/K$  be an elliptic curve. Then,  $E(K)$  is a finitely generated abelian group, i.e.,*

$$E(K) \cong \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_n \oplus E(K)_{\text{tor}}. \tag{1}$$

The number of copies of  $\mathbb{Z}$  in (1) is called the *rank of the elliptic curve*. Neither a formula or a terminative algorithm for computing the rank of an elliptic curve has been known. The rank of an elliptic curve  $E/K$  can be computed from  $E(K)/mE(K)$ , and the *m-Selmer group of an elliptic curve  $E/K$* , which is introduced in Section 2, has been a standard computable (finite) group which contains  $E(K)/mE(K)$ ; the *m-Selmer group* is denoted by  $\text{Sel}^{(m)}(E/K)$ . The procedure of computing the *m-Selmer group* of an elliptic curve  $E/K$  is called the *m-descent*.

In Section 2, the definition of the *m-Selmer group* of an elliptic curve  $E/K$  is introduced. In Section 3, introduced is a way of computing the 3-Selmer group, developed by Edward Schaefer, of an elliptic curve  $E/\mathbb{Q}$  given by  $y^2 = x^3 + b$ . In Sections 4 and 5, I show how some of the key computations of the 3-descent were done by myself. The implementation of the 3-descent is done with `gp-pari`<sup>1</sup>, which is a high-level C-based computer language designed for heavy arithmetic computation. In the last section, I briefly explain about the `gp-script selmer3333.gp`.

The computer program `mwrnk` written by John Cremona performs the 2-decent on general elliptic curves  $E/\mathbb{Q}$ , and often finds the generators of the *Mordell-Weil group*  $E(\mathbb{Q})$ , and hence, the rank of the elliptic curve; however, occasionally it fails to find the generators. My original motivation for implementing the 3-descent was to hopefully determine the (correct) rank of elliptic curves which `mwrnk` couldn't find. For example, suppose that `mwrnk` computes:  $\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(E/\mathbb{Q}) = 1$ , but not the rank of the elliptic curve. If `selmer3333.gp` computes  $\dim_{\mathbb{F}_3} \text{Sel}^{(3)}(E/\mathbb{Q}) = 0$ , then we can conclude that the rank of  $E/\mathbb{Q}$  is 0.

Another use of `selmer3333.gp` can be to compute the 3-part of the *Tate-Shafarevich group of the elliptic curve  $E/\mathbb{Q}$* , denoted by  $\text{III}(E/\mathbb{Q})[3]$  (see Chapter 10, [5]). For example, if `mwrnk` computes the rank  $r$  of an elliptic curve  $E/\mathbb{Q}$  and  $E(\mathbb{Q})$  does not contain a nontrivial 3-torsion point, then  $\dim_{\mathbb{F}_3} \text{III}(E/\mathbb{Q})[3] = \dim_{\mathbb{F}_3} \text{Sel}^{(3)}(E/\mathbb{Q}) - r$ .

## 2 The $p$ -descent on an elliptic curve $E/\mathbb{Q}$

Edward Schaefer developed a practical algorithm of performing the  $p$ -descent using  $\overline{\mathbb{Q}}(E)$ , the rational functions on an elliptic curve  $E/\mathbb{Q}$ . Let  $E[p]$  denote the  $p$ -torsion of  $E(\overline{\mathbb{Q}})$ , and  $G_{\mathbb{Q}}$ , the absolute Galois group  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ . In the theory of Schaefer's algorithm, he finds a neat concrete description of the first Galois cohomology  $H^1(G_{\mathbb{Q}}, E[p])$  (see Chapter 10, [4] for the definition of the Galois cohomology), and this description makes his algorithm very practical.

The description of  $H^1(G_{\mathbb{Q}}, E[3])$  for the elliptic curve  $E : y^2 = x^3 + b$  is found in Schaefer-Stoll's paper [3], Section 10.2: *How to do a  $p$ -descent on an elliptic curve*. I followed their algorithm to implement the descent with `gp-pari`.

### 2.1 Definition of the $m$ -Selmer Group

The short exact sequence:  $0 \rightarrow E[m] \rightarrow E \xrightarrow{[m]} E \rightarrow 0$ , yields the following long exact sequence (see Chapter 10, [4]): denote  $H^1(G_{\mathbb{Q}}, M)$  by  $H^1(\mathbb{Q}, M)$  for  $G_{\mathbb{Q}}$ -module  $M$ :

$$\begin{aligned} 0 &\longrightarrow E[m] \longrightarrow E(\mathbb{Q}) \longrightarrow E(\mathbb{Q}) \longrightarrow H^1(\mathbb{Q}, E[m]) \longrightarrow H^1(\mathbb{Q}, E) \longrightarrow \dots \\ &0 \longrightarrow E(\mathbb{Q})/mE(\mathbb{Q}) \xrightarrow{\delta} H^1(\mathbb{Q}, E[m]) \longrightarrow H^1(\mathbb{Q}, E)[m] \longrightarrow 0 \end{aligned} \quad (2)$$

---

<sup>1</sup><http://pari.math.u-bordeaux.fr>

The same sort of the sequence (2) is obtained when  $E$  is considered as  $E(\overline{\mathbb{Q}_q})$  where  $\mathbb{Q}_q$  is the  $q$ -adic field, i.e., take the group cohomology with group  $G_{\mathbb{Q}_q}$ . The inclusion of  $\mathbb{Q}$  into  $\mathbb{Q}_q$  induces a map from the *weak Mordell-Weil group*  $E(\mathbb{Q})/mE(\mathbb{Q})$  to  $E(\mathbb{Q}_q)/mE(\mathbb{Q}_q)$ . and the restriction of the 1-cocycles down to the decomposition group of  $G_{\mathbb{Q}}$  at  $q$  induces a map:  $H^1(\mathbb{Q}, E[m]) \rightarrow H^1(\mathbb{Q}_q, E[m])$ . The following diagram summarizes the maps explained here, and the definition of the  $m$ -Selmer group is given:

$$\begin{array}{ccccc}
E(\mathbb{Q})/mE(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[m]) & \longrightarrow & \\
\downarrow & & \downarrow \text{res}_q & & \\
E(\mathbb{Q}_q)/mE(\mathbb{Q}_q) & \xrightarrow{\delta_q} & H^1(\mathbb{Q}_q, E[m]) & \longrightarrow & \\
\text{Sel}^{(m)}(E/\mathbb{Q}) = \{\xi \in H^1(\mathbb{Q}, E[m]) : \text{res}_q \xi \in \text{Im } \delta_q, \text{ for all places } q\} & & & & (3)
\end{array}$$

While  $H^1(\mathbb{Q}, E[m])$  is infinite, the  $m$ -Selmer group is finite, and the weak Mordell-Weil group injects to the  $m$ -Selmer group.

In practice, only a finite number of local computations are necessary, which is explained in Theorem 2.1. Let us introduce the definition of the subgroup  $H^1(\mathbb{Q}, E[m])_S$  *unramified outside*  $S$ .

### Definition 2.1

- (a) Throughout this report,  $S$  will be a finite set of places containing all the infinite places.
- (b) The *unramified subgroup* of  $H^1(\mathbb{Q}_q, E[m])$  is the kernel of the restriction:

$$H^1(G_{\mathbb{Q}_q}, E[m]) \longrightarrow H^1(I_q, E[m]),$$

where  $I_q$  is the inertia group.

- (c)  $\xi \in H^1(\mathbb{Q}, E[m])$  is *unramified at*  $q$  if  $\text{res}_q \xi$  is contained in the unramified subgroup of  $H^1(\mathbb{Q}_q, E[m])$ .
- (d) The subgroup of  $H^1(\mathbb{Q}, E[m])$  *unramified outside*  $S$ , denoted by  $H^1(\mathbb{Q}, E[m])_S$ , is the subgroup consisting of elements unramified at all  $q$  not contained in  $S$ .

**Theorem 2.1** *Let  $S$  be the set of places consisting of all infinite places,  $p$ , and places of bad reduction. Then,  $H^1(\mathbb{Q}, E[m])_S$  is finite, and the weak Mordell-Weil group injects into  $H^1(\mathbb{Q}, E[m])_S$ ; moreover,  $\text{Im } \delta_q$  for all  $q \notin S$  is equal to the unramified subgroup of  $H^1(\mathbb{Q}_q, E[m])$ , and hence,*

$$\text{Sel}^{(m)}(E/\mathbb{Q}) = \{\xi \in H^1(\mathbb{Q}, E[m])_S : \text{res}_q \xi \in \text{Im } \delta_q, \text{ for all } q \in S\} \quad (4)$$

Therefore, we can compute the  $m$ -Selmer group by checking the local conditions (4) at the places of  $S$  for the finite group  $H^1(\mathbb{Q}, E[m])_S$ .

## 2.2 Schaefer's Algorithm

Schaefer-Stoll's paper [3] provides an explicit description of  $H^1(\mathbb{Q}, E[3])$  for an elliptic curve given by  $y^2 = x^3 + b$ . I shall outline their ideas, and elaborate the descriptions (5) and (6) to show how the algebras in (5) arise.

Let me introduce some notations used in (5). The étale algebra  $\mathbb{Q}[X]/(X^2 - b)$  over  $\mathbb{Q}$  is denoted by  $\mathbb{Q}(\sqrt{b})$ . So, if  $\sqrt{b} \in \mathbb{Q}$ , then  $\mathbb{Q}(\sqrt{b}) \cong \mathbb{Q} \times \mathbb{Q}$ . Let  $f(x)$  be a polynomial of degree 6 (defined over)  $\mathbb{Q}$  with

$(-1)^i \sqrt{-3b} + \sqrt[3]{4b} \zeta^j$  as zeros where  $\zeta$  is a primitive third root of unity, and  $i = 0, 1$  and  $j = 0, 1, 2$ . Then, the étale algebra  $\mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b})$  over  $\mathbb{Q}$  is defined to be  $\mathbb{Q}[X]/f(X)$ . If  $\sqrt[3]{4b} \in \mathbb{Q}$ , then  $\mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) \cong \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) \times \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b} \zeta)$ . Likewise, the meaning of the notation of the étale algebras over  $\mathbb{Q}$ ,  $B$  and  $D$  in (5) is understood. For example, let  $g(x)$  be a polynomial of degree 12 (defined over  $\mathbb{Q}$ ) with  $(-1)^i \sqrt{b} + (-1)^j \sqrt{-3b} + \sqrt[3]{4b} \zeta^k$  as zeros where  $i, j = 0, 1$  and  $k = 0, 1, 2$ . Then,  $\mathbb{Q}(\sqrt{b}, \sqrt{-3b}, \sqrt[3]{4b})$  denotes  $\mathbb{Q}[X]/g(X)$ .

We define the étale algebras over  $\mathbb{Q}$ ,  $A$ ,  $A_+$ ,  $B$ , and  $D$  to be as follows:

$$\begin{aligned} A &= A_1 \times A_2 = \mathbb{Q}(\sqrt{b}) \times \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) \\ A_+ &= A_{+,1} \times A_{+,2} = \mathbb{Q} \times \mathbb{Q}(\sqrt[3]{4b}) \\ B &= B_1 \times B_2 = \mathbb{Q}(\sqrt{-3b}) \times \mathbb{Q}(\sqrt{b}, \sqrt[3]{4b}) \\ D &= \mathbb{Q}(\sqrt{b}, \sqrt{-3b}, \sqrt[3]{4b}) \end{aligned} \quad (5)$$

The first Galois cohomology  $H^1(\mathbb{Q}, E[3])$  is described in terms of the elements of the algebras defined in (5).

**Case:**  $\sqrt[3]{4b} \notin \mathbb{Q}$ . Let  $\sigma$  be the automorphism of order 3 on the algebra  $D$  such that  $\sigma \sqrt[3]{4b} = \sqrt[3]{4b} \zeta$  where  $\zeta = (-1 + \sqrt{-3})/2$  and  $\sqrt{-3} = \sqrt{-3b}/\sqrt{b}$ .

$$\begin{aligned} H^1(\mathbb{Q}, E[3]) &\cong \{(\alpha_1, \alpha_2) \in A_1^*/(A_1^*)^3 \times A_2^*/(A_2^*)^3 : \\ &N_{A_1/\mathbb{Q}}(\alpha_1) \in (\mathbb{Q}^*)^3, N_{A_2/A_{+,2}}(\alpha_2) \in (A_{+,2}^*)^3, \\ &i_{B_2/A_1}(\alpha_1) N_{L/B_2}(\alpha_2^\sigma) \in (B_2^*)^3, N_{A_2/B_2}(\alpha_2) \in (B_1^*)^3\} \end{aligned} \quad (6)$$

**Case:**  $\sqrt[3]{4b} \in \mathbb{Q}$ . The choice of  $\zeta$  is the same as in the previous case. Let  $\tau_1$  be the automorphism of order 2 on the algebra  $\mathbb{Q}(\sqrt{b}, \zeta)$  such that  $\tau_1 \sqrt{b} = -\sqrt{b}$  and  $\tau_1 \zeta = \zeta$ , and  $\tau_2$ , the automorphism of order 2 such that  $\tau_2 \sqrt{b} = \sqrt{b}$  and  $\tau_2 \zeta = \zeta^2$ . The algebras  $A_2$  and  $B_2$  in (5) split further as shown below.  $A_{+,2}$  also splits, but since  $N_{A_2/A_{+,2}}$  is meaningful, we keep it this way for this norm map:

$$A_2 = A_{21} \times A_{22} = \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) \times \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b} \zeta), \quad (7)$$

$$B_2 = B_{21} \times B_{22} = \mathbb{Q}(\sqrt{b}, \sqrt[3]{4b}) \times \mathbb{Q}(\sqrt{b}, \sqrt[3]{4b} \zeta). \quad (8)$$

Denote the algebra  $\mathbb{Q}(\sqrt{b}, \sqrt{-3b}, \sqrt[3]{4b}\zeta)$  by  $D'$ . Then,

$$\begin{aligned} H^1(\mathbb{Q}, E[3]) &\cong \{(\alpha_1, \alpha_{21}, \alpha_{22}) \in A_1^*/(A_1^*)^3 \times A_{21}^*/(A_{21}^*)^3 \times A_{22}^*/(A_{22}^*)^3 : \\ &N_{A_1/\mathbb{Q}}(\alpha_1) \in (\mathbb{Q}^*)^3, N_{A_2/A_{+,2}}(\alpha_2) \in (A_{+,2}^*)^3, \\ &i_{B_{22}/A_1}(\alpha_1) N_{D'/B_{22}}(\alpha_{22}) \in (B_{22}^*)^3, i_{B_{21}/A_1}(\alpha_1) \alpha_{21} \alpha_{22}^{\tau_1} \in (B_{21}^*)^3, \\ &N_{A_2/B_1}(\alpha_2) \in (B_1^*)^3\} \end{aligned} \quad (9)$$

**Remark:** The description of  $H^1(\mathbb{Q}, E[3])$  which appeared in [3], Section 10.2 is slightly different from the above. Firstly, they wrote  $N_{L/B_2}(\alpha_2^{\sigma^2})$  but  $N_{L/B_2}(\alpha_2^\sigma)$  is correct as in (6). Secondly, when  $\sqrt[3]{4b} \in \mathbb{Q}$ , their description of  $H^1(\mathbb{Q}, E[3])$  deserves some clarification which is given in (9).

As seen in (4), if one has the generators of  $H^1(\mathbb{Q}, E[3])_S$ , computing  $\text{Sel}^{(3)}(E/\mathbb{Q})$  is practical. Schaefer-Stoll states in [3] that using Tate's algorithm, we can take

$$S = \{3\} \cup \{q : 4b \in (\mathbb{Q}_q^*)^2, v_q(4b) \not\equiv 0 \pmod{6}\}. \quad (10)$$

To interpret the generators of  $H^1(\mathbb{Q}, E[3])_S$  in terms of elements of  $A$ , let us introduce *the subgroup of  $A$  unramified outside  $S$*  denoted by  $A(S, 3)$ . Let  $K$  be a number field, and  $\langle S \rangle$  be the subgroup of the group of ideals  $I_K$  generated by the prime ideals lying above the places of  $S$ . *The subgroup of  $K$  unramified outside  $S$* , denoted by  $K(S, 3)$ , is defined by

$$K(S, 3) = \{\alpha \in K^*/(K^*)^3 : \alpha \mathcal{O}_K = \mathfrak{a}^3 \text{ for some } \mathfrak{a} \in \langle S \rangle\}. \quad (11)$$

If  $A \cong A_1 \times A_2$  where  $A_1$  and  $A_2$  are fields, we define  $A(S, 3) = A_1(S, 3) \times A_2(S, 3)$ , and if  $A$  splits further, the subgroup  $A(S, 3)$  is defined similarly. We identify the generators of  $H^1(\mathbb{Q}, E[3])_S$  as follows:

$$H^1(\mathbb{Q}, E[3])_S = H^1(\mathbb{Q}, E[3]) \cap (A_1(S, 3) \times A_2(S, 3)), \quad (12)$$

Once we have the elements of  $H^1(\mathbb{Q}, E[3])_S$ , in order to finish computing  $\text{Sel}^{(3)}(E/\mathbb{Q})$ , we need to check the local condition:  $\text{res}_q \xi \in \text{Im } \delta_q$  where  $\xi \in H^1(\mathbb{Q}, E[3])_S$  for  $q \in S$ . The local cohomology  $H^1(\mathbb{Q}_q, E[3])$  has a description similar to that of  $H^1(\mathbb{Q}, E[3])$ , but the étale algebras over  $\mathbb{Q}_q$  split further. The following lemma shows how they split, and finds the generators of  $\text{Im } \delta_q$  for  $q \neq 3$ .

**Lemma 2.1** (Schaefer-Stoll) *Let  $q \in S \setminus \{3\}$ , and let  $\zeta$  be the primitive cube root of unity defined by  $\zeta = (-1 + \sqrt{-3})/2$  and  $\sqrt{-3} = \sqrt{-3b}/\sqrt{b}$ . The image of  $\delta_q$  is a one-dimensional  $\mathbb{F}_3$ -vector space, and a generator is represented by*

$$\text{Im } \delta_q = \begin{cases} \langle \langle 4b, 2b^2, \zeta^2 \rangle \rangle \subset A_q^*/(A_q^*)^3, & q \equiv 2 \pmod{3} \\ \langle \langle 4b, 2b^2, \zeta^2, \zeta \rangle \rangle \subset A_q^*/(A_q^*)^3, & q \equiv 1 \pmod{3} \end{cases} \quad (13)$$

where

$$A_q = A \otimes \mathbb{Q}_q = \begin{cases} \mathbb{Q}_q \times \mathbb{Q}_q \times \mathbb{Q}_q(\sqrt{-3}, \sqrt[3]{4b}), & q \equiv 2 \pmod{3} \\ \mathbb{Q}_q \times \mathbb{Q}_q \times \mathbb{Q}_q(\sqrt[3]{4b}) \times \mathbb{Q}(\sqrt[3]{4b}), & q \equiv 1 \pmod{3} \end{cases}. \quad (14)$$

Hence, with these generators, one can check the local condition (4).

However, in general, at  $q = 3$ , there is not an explicit description of the generators of  $\text{Im } \delta_3$ ; nevertheless, its size is easily computed:  $\dim_{\mathbb{F}_3} E(\mathbb{Q}_3)[3] + 1$ . I found a procedure of finding the generators of  $\text{Im } \delta_3$ , which uses the group of components, but I implemented a random search for the purpose of finding the generators because it runs quickly for all cases I tried. So, in `selmer3333.gp`, a random search is performed to find the generators.

The main computation of a random search are performing 3-divisibility test, i.e., we need to check if points found are not divisible by 3. The 3-divisibility test could be done quickly using the  $F$ -map which is introduced in [3], Section 5.

### 3 The Étale Algebras

This section is to help the reader understand more about the étale algebras appearing in the algorithm as concrete objects to work with. The reader may skip this section if not interested. Readers who are interested in more than what is introduced in this report should read Schaefer's paper [2]: *Computing a Selmer group of a Jacobian using functions on the curve*. All the theoretical works of the beautiful description of  $H^1(\mathbb{Q}, E[p])$  are credited to E. Schaefer and M. Stoll, and the rest of this section is my attempt to briefly show how the algebras arise.

#### 3.1 The étale algebra $A$

Let  $X$  be the set of the nontrivial points of  $E[p](\overline{\mathbb{Q}})$ , and  $m = p^2 - 1$ . Put  $X = \{R_1, \dots, R_m\}$ .

##### Definition 3.1

- (a) The affine coordinate ring of  $E/\mathbb{Q}$  defined over  $\overline{\mathbb{Q}}$  is denoted by  $\overline{\mathbb{Q}}[E]$ .
- (b) The étale algebra over  $\overline{\mathbb{Q}}$  corresponding to  $X$ , denoted by  $A$ , is the set of  $\overline{\mathbb{Q}}$ -valued set-theoretic functions on  $X$ . That is,

$$\overline{A} \cong \underbrace{\overline{\mathbb{Q}} \times \cdots \times \overline{\mathbb{Q}}}_{p^2-1}.$$

- (c) A line in  $E[p](\overline{\mathbb{Q}})$  is the set  $\{[m]P_1 + P_0 : m \in \mathbb{Z}\}$  for some  $P_0, P_1 \in E[p](\overline{\mathbb{Q}})$ , and denote by  $Z$  the set of lines in  $E[p](\overline{\mathbb{Q}})$  passing through the origin  $O$ . The étale algebra over  $\overline{\mathbb{Q}}$  corresponding to  $Z$ , denoted by  $\overline{A}_+$ , is the subalgebra of  $\overline{A}$

$$\{\phi \in \overline{A} : \phi(P) = \phi(Q) \text{ for all } P, Q \in \ell, \text{ for all } \ell \in Z\}.$$

That is,  $\overline{A}_+$  is the subalgebra of  $\overline{A}$  consisting of regular functions of  $\overline{\mathbb{Q}}[E]$  restricted to  $X$ , which are constant on the lines of  $Z$ .

$$\overline{A}_+ \cong \underbrace{\overline{\mathbb{Q}} \times \cdots \times \overline{\mathbb{Q}}}_{p+1}.$$

- (d) The action of the absolute Galois group  $G_{\mathbb{Q}}$  on  $\overline{A}$  is defined as follows: for  $\sigma \in G_{\mathbb{Q}}$  and  $\phi \in \overline{A}$ ,

$$(\sigma * \phi)(P) = \sigma \phi(P^{\sigma^{-1}}), \quad (15)$$

and this action induces an action on  $\overline{A}_+$ . The  $G_{\mathbb{Q}}$ -invariants  $\overline{A}^{G_{\mathbb{Q}}}$  and  $\overline{A}_+^{G_{\mathbb{Q}}}$  are denoted by  $A$  and  $A_+$ , respectively. We call  $A$  and  $A_+$  étale algebras over  $\mathbb{Q}$  associated with the  $p$ -descent on the elliptic curve  $E$ .

- (e) Let  $P$  be a point of  $E[p](\overline{\mathbb{Q}})$ , and  $\ell$  be a line in  $E[p](\overline{\mathbb{Q}})$  passing through the origin. The number field generated by the coordinates of  $P$  is denoted by  $\mathbb{Q}(P)$ .
- (f) Let  $H_{\ell}$  be the subgroup of  $G_{\mathbb{Q}}$  consisting of automorphisms which set-wise fix a line  $\ell$  in  $E[p](\overline{\mathbb{Q}})$ , and  $K_{\ell}$  be the number field generated by the coordinates of the points contained in  $\ell$ . Denoted by  $\mathbb{Q}(\ell)$  is the subfield of  $K_{\ell}$  fixed by  $H_{\ell}$ , i.e.,  $\mathbb{Q}(\ell) = K_{\ell}^{H_{\ell}}$ .

**Remark:** The number field  $K_\ell$  is not necessarily Galois, but the action of the subgroup  $H_\ell$  is well-defined: an element  $\sigma$  of  $H_\ell$  set-wise fixes the line  $\ell$ , and hence,  $\sigma(K_\ell) = K_\ell$ . In short, there is the restriction map:  $H_\ell \rightarrow \text{Aut}_{\mathbb{Q}}(K_\ell)$ .

**Proposition 3.1** *Let  $\bar{A}$  and  $\bar{A}_+$  be the étale algebras corresponding to  $X$  and  $Z$  defined in Definition 3.1.*

- (a) *The étale algebras  $\bar{A}$  and  $\bar{A}_+$  can be interpreted as follows:*
- (i)  *$\bar{A}$  is equal to the affine coordinate ring  $\overline{\mathbb{Q}}[E]$  restricted to  $X$ .*
  - (ii)  *$\bar{A}_+$  is equal to the subring of  $\overline{\mathbb{Q}}[E]$  restricted to  $X$  consisting of functions constant on lines in  $X$  passing through the origin.*
- (b) *If  $\phi \in A$  and  $P \in E[p](\overline{\mathbb{Q}})$ , then  $\phi(P)$  is contained in the number field  $\mathbb{Q}(P)$ .*
- (c) *Let  $X_i$ ,  $i = 1, \dots, s$  be the  $G_{\mathbb{Q}}$ -orbits in  $X$ , and  $P_i$  be a representative of the orbit  $X_i$  for each  $i$ . Denote the number field  $\mathbb{Q}(P_i)$  by  $A_i$ . Then, the followings are true:*
- (i) *For each  $i$ , the action of  $G_{\mathbb{Q}}/G_{A_i}$  on  $X_i$  is simple.*
  - (ii) *Define the map  $\psi : A \rightarrow \prod_{i=1}^s A_i$  by  $\phi \mapsto (\phi(P_1), \dots, \phi(P_s))$ . Then,  $\psi$  is an isomorphism.*
- (d) *If  $\phi \in A_+$  and  $\ell$  is a line passing through the origin, then  $\phi(\ell)$  is contained in the number field  $\mathbb{Q}(\ell)$ .*
- (e) *Let  $Z_i$ ,  $i = 1, \dots, t$  be the  $G_{\mathbb{Q}}$ -orbits in  $Z$ , and  $\ell_i$  be a representative of the orbit  $Z_i$  for each  $i$ . Denote the number field  $\mathbb{Q}(\ell_i)$  by  $A_{+,i}$ . Then, the followings are true:*
- (i) *For each  $i$ , the action of  $G_{\mathbb{Q}}/H_{\ell_i}$  on  $Z_i$  is simple.*
  - (ii) *Define the map  $\psi_+ : A_+ \rightarrow \prod_{i=1}^t A_{+,i}$  given by  $\phi \mapsto (\phi(\ell_1), \dots, \phi(\ell_t))$ . Then,  $\psi_+$  is an isomorphism.*

**proof:** Restricting functions of  $\overline{\mathbb{Q}}[E]$  is equivalent to taking the following quotient: let  $M_i$  be the maximal ideal corresponding to the point  $R_i \in X$ .  $\overline{\mathbb{Q}}[E]/M_1 \cdots M_m \cong \overline{\mathbb{Q}}[E]/M_1 \oplus \cdots \oplus \overline{\mathbb{Q}}[E]/M_m \cong \bar{A}$ .

The subalgebra  $\bar{A}_+$  corresponds to the set of  $m$ -tuples  $(a_1, \dots, a_m)$  such that  $a_i = a_j$  if  $R_i$  and  $R_j$  form a line in  $Z$ .

By definition, if  $\phi \in A$ , then  $\sigma\phi(P^{\sigma^{-1}}) = \phi(P)$  for all  $\sigma \in G_{\mathbb{Q}}$  and all  $P \in X$ , i.e.,  $\phi(P^{\sigma^{-1}}) = \sigma^{-1}\phi(P)$ . Let  $K$  be the number field  $\mathbb{Q}(P)$ . If  $\sigma \in G_K$ , then  $P^{\sigma^{-1}} = P$ , i.e.,  $\phi(P) = \phi(P^{\sigma^{-1}}) = \sigma^{-1}\phi(P)$ . Hence,  $\phi(P) \in K$ .

The action of  $G_{\mathbb{Q}}/G_{A_i}$  on  $X_i$  is obviously simple. If  $\sigma \in G_{\mathbb{Q}}/G_{A_i}$  fixes all elements of  $X_i$ , then  $\sigma$  fixes all elements of  $A_i$ , in particular.

Let  $A_i$  be the number field  $\mathbb{Q}(P_i)$ , and define the evaluation maps  $\psi_i : A \rightarrow A_i$  given by  $\psi_i(\phi) = \phi(P_i)$ . We define  $\psi : A \rightarrow \prod_1^s A_i$  by  $\psi = (\psi_1, \dots, \psi_s)$ .

The injectivity of  $\psi$ : Suppose that  $\psi(\phi) = 0$  for some  $\phi \in A$ . For any nontrivial point  $P$  of  $E[p](\overline{\mathbb{Q}})$ , there is some  $X_i$  such that  $P \in X_i$ , so that  $P = P_i^\sigma$  for some  $\sigma \in G_{\mathbb{Q}}$ . The function  $\phi$  being in  $A$  implies that  $\phi(P_i^\sigma) = \sigma\phi(P_i)$ , i.e.,  $\phi(P) = 0$ .

The surjectivity of  $\psi$ : Suppose that  $\alpha = (\alpha_1, \dots, \alpha_s) \in \prod_1^s A_i$ . Since  $\bar{A}$  splits completely as shown in (a), define a function  $\phi$  on  $X$  by  $\phi(P_i) = \alpha_i$  for all  $i$  and by  $\phi(P) = \sigma\alpha_i$  if  $P = P_i^\sigma$  for some  $i$  and some  $\sigma \in G_{\mathbb{Q}}$ . The function  $\phi$  is well-defined because the action of  $G_{\mathbb{Q}}/G_{A_i}$  on  $X_i$  is simple, i.e., for any

two automorphisms  $\sigma, \tau \in G_{\mathbb{Q}}/G_{A_i}$  such that  $P_i^\sigma = P_i^\tau$ , the images  $\sigma\alpha_i$  and  $\tau\alpha_i$  are equal to each other since  $\alpha_i \in A_i$ . Claim that  $\phi \in A$ . Note that for any  $\tau \in G_{\mathbb{Q}}$ , there is some  $P_i$  such that  $P = P_i^\sigma$ . Then,  $\phi(P^\tau) = \phi(P_i^{\sigma\tau}) = \tau\sigma\phi(P_i) = \tau\phi(P)$ .

Recall the definition of  $\mathbb{Q}(\ell)$ . Let  $\phi$  be an element of  $A_+$  identified as an element of  $A$ . For any  $\tau \in G_{K_\ell}$  and  $R \in \ell$ , we have  $\phi(R) = \phi(R^\tau) = \tau\phi(R)$ , i.e.,  $\phi(R) \in K_\ell$  for all nontrivial  $R \in \ell$ . On the other hand,  $\phi$  is constant on  $\ell$ . For any  $\tau \in H_\ell$  and a nontrivial point  $R \in \ell$ , we have  $\phi(R) = \phi(R^\tau) = \tau\phi(R)$ , i.e.,  $\phi(R) \in \mathbb{Q}(\ell)$ .

Let  $A_{+,i}$  be the number field  $\mathbb{Q}(\ell_i)$ , and define  $\psi_{+,i} : A_+ \rightarrow A_{+,i}$  given by  $\psi_{+,i}(\phi) = \phi(\ell_i)$ . We define  $\Psi_+ = (\Psi_{+,1}, \dots, \Psi_{+,s})$ .

The definition of  $H_\ell$  states that the action of  $G_{\mathbb{Q}}/H_\ell$  on  $Z_i$  is obviously simple.

The injectivity of  $\Psi_+$ : Suppose that  $\Psi_+(\phi) = 0$  for some  $\phi \in A_+$ , i.e.,  $\phi(\ell_i) = 0$  for all  $i$ . For any line  $\ell$  of  $Z$ , there is a line  $\ell_i$  such that  $\ell = \ell_i^\sigma$  for some  $\sigma \in G_{\mathbb{Q}}$ . Thus, we have  $\phi(\ell) = \phi(\ell_i^\sigma) = \sigma\phi(\ell_i) = 0$ .

The surjectivity of  $\Psi_+$ : Suppose that  $\alpha = (\alpha_1, \dots, \alpha_t) \in \prod_1^t A_{+,i}$ . Define a function  $\phi$  on  $Z$  by  $\phi(\ell_i) = \alpha_i$  for all  $i$  and by  $\phi(\ell) = \sigma\alpha_i$  if  $\ell = \ell_i^\sigma$  for some  $i$  and some  $\sigma \in G_{\mathbb{Q}}$ . Claim that the function  $\phi$  is well-defined. Note that the action of  $G_{\mathbb{Q}}/H_\ell$  on  $Z_i$  is simple. Suppose that there are two automorphisms  $\sigma, \tau \in G_{\mathbb{Q}}$  such that  $\ell = \ell_i^\sigma = \ell_i^\tau$ , i.e.,  $\sigma\tau^{-1} \in H_\ell$ . Note that  $\phi(\ell_i^\sigma) = \phi(\ell) = \sigma\alpha_i = \sigma\phi(\ell_i)$ , and similarly,  $\phi(\ell_i^\tau) = \tau\phi(\ell_i)$ . Since  $\phi(\ell_i) \in \mathbb{Q}(\ell_i) = K_{\ell_i}^{H_\ell}$ , we have  $\tau^{-1}\sigma\phi(\ell_i) = \phi(\ell_i)$ , i.e.,  $\sigma\phi(\ell_i) = \tau\phi(\ell_i)$ , i.e.,  $\phi(\ell_i^\sigma) = \phi(\ell_i^\tau)$ .

Claim that  $\phi \in A_+$ . Note that for any  $\tau \in G_{\mathbb{Q}}$ , there is some  $\ell_i$  such that  $\ell = \ell_i^\sigma$ . Then,  $\phi(\ell^\tau) = \phi(\ell_i^{\sigma\tau}) = \tau\sigma\phi(\ell_i) = \tau\phi(\ell)$ .  $\square$

### Example

Let  $E/\mathbb{Q}$  be an elliptic curve defined over  $\mathbb{Q}$  given by an equation:  $y^2 = x^3 + b$ , and  $\zeta$  be a primitive third root of unity. Then, the following points are the nontrivial 3-torsion points of  $E(\overline{\mathbb{Q}})$ .

$$\{(0, \sqrt{b}), (0, -\sqrt{b})\} \cup \{(-\sqrt[3]{4b}\zeta^i, (-1)^j\sqrt{-3b}) : i = 0, 1, 2, \text{ and } j = 0, 1\}. \quad (16)$$

**The Generic Case** If  $E[3](\mathbb{Q})$  is trivial for the case of an elliptic curve considered, then the elliptic curve is said to be *of the generic case*, and if  $E[3](\mathbb{Q}) \neq \{O\}$ , *of the special cases*.

For the generic case of an elliptic curve, the set  $\{(0, \sqrt{b}), (-\sqrt[3]{4b}, \sqrt{-3b})\}$  forms a complete set of representatives of the  $G_{\mathbb{Q}}$ -orbits in  $X$  where  $X = E[3](\overline{\mathbb{Q}}) \setminus \{O\}$ . Proposition 3.1 says:  $A_1 = \mathbb{Q}(\sqrt{b})$  and  $A_2 = \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b})$ , and

$$A \cong \mathbb{Q}(\sqrt{b}) \times \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) \quad (17)$$

Let  $\ell_1$  be the line generated by the point  $P_1 = (0, \sqrt{b})$ , and  $\ell_2$ , generated by the point  $P_2 = (-\sqrt[3]{4b}, \sqrt{-3b})$ . Then, the set  $Z$  of lines in  $X$  passing through the origin has two  $G_{\mathbb{Q}}$ -orbits:  $\ell_1$  represents one orbit, and  $\ell_2$  represents the other: if  $\sigma$  is an automorphism of  $G_{\mathbb{Q}}$  such that  $\sqrt[3]{4b} \mapsto \sqrt[3]{4b}\zeta$ , then  $\{\ell_2, \ell_2^\sigma, \ell_2^{\sigma^2}\}$  forms a  $G_{\mathbb{Q}}$ -orbit. Then,  $K_{\ell_1} = \mathbb{Q}(\sqrt{b})$  and  $K_{\ell_2} = \mathbb{Q}(\sqrt[3]{4b}, \sqrt{-3b})$ . Note that for any  $\tau \in G_{\mathbb{Q}}$ , the point  $P_1^\tau$  is either  $P_1$  or  $[2]P_1 = (0, -\sqrt{b})$ , i.e.,  $A_{+,1} = \mathbb{Q}$ . Elements of  $H_{\ell_2}$  should fix  $\sqrt[3]{4b}$ ; otherwise,  $\ell_2$  cannot be fixed under the action of  $H_{\ell_2}$ . It is easy to see that  $K_{\ell_2}^{H_{\ell_2}} = \mathbb{Q}(\sqrt[3]{4b})$ .

**The Special Cases** The special case:  $\sqrt[3]{4b} \in \mathbb{Q}$  is worth considering as the description of  $H^1(\mathbb{Q}, E[3])$  in (9) is treated differently. Let  $X$  and  $Z$  be the sets defined in Definition 3.1, and  $X_i$  and  $Z_i$  be the  $G_{\mathbb{Q}}$ -orbits

as introduced in Proposition 3.1. If  $Q$  is a point in  $X$ , we denote by  $\langle Q \rangle$  the line of  $Z$  passing through  $Q$ . Assume for simplicity that  $\sqrt{b}, \sqrt{-3b} \notin \mathbb{Q}$ . The points in  $X$  are denoted as follows, then we find  $X_i$ 's and  $Z_i$ 's.

$$\begin{aligned} P &= (0, \sqrt{b}) & \ell &= \langle P \rangle \\ R_0 &= (-\sqrt[3]{4b}, \sqrt{-3b}) & \ell_0 &= \langle R_0 \rangle \\ R_1 &= (-\sqrt[3]{4b} \zeta, \sqrt{-3b}) & \ell_1 &= \langle R_1 \rangle \\ R_2 &= (-\sqrt[3]{4b} \zeta^2, \sqrt{-3b}) & \ell_2 &= \langle R_2 \rangle \end{aligned} \tag{18}$$

$$\begin{aligned} X_1 &= \{P, [2]P\}, & A_1 &= \mathbb{Q}(\sqrt{b}), & Z_1 &= \{\ell\}, \\ X_2 &= \{R_0, [2]R_0\}, & A_2 &= \mathbb{Q}(\sqrt{-3b}), & Z_2 &= \{\ell_0\}, \\ X_3 &= \{R_1, R_2, [2]R_1, [2]R_2\} & A_3 &= \mathbb{Q}(\sqrt{-3b}, \zeta) & Z_3 &= \{\ell_1, \ell_2\} \end{aligned} \tag{19}$$

$$\begin{aligned} K_\ell &= \mathbb{Q}(\sqrt{b}), & \mathbb{Q}(\ell) &= \mathbb{Q}, \\ K_{\ell_0} &= \mathbb{Q}(\sqrt{-3b}), & \mathbb{Q}(\ell_0) &= \mathbb{Q}, \\ K_{\ell_1} &= \mathbb{Q}(\sqrt{-3b}, \zeta) & \mathbb{Q}(\ell_1) &= \mathbb{Q}(\zeta) \end{aligned} \tag{20}$$

The splitting of the algebras  $A$  and  $A_+$  is as follows:

$$A \cong \mathbb{Q}(\sqrt{b}) \times \mathbb{Q}(\sqrt{-3b}) \times \mathbb{Q}(\sqrt{-3b}, \zeta) \tag{21}$$

$$A_+ \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}(\zeta) \tag{22}$$

## 3.2 The étale algebra $B$

### Definition 3.2

Let  $Y$  be the set of lines in  $E[p](\overline{\mathbb{Q}})$  missing the origin  $O$ . The set  $Y$  contains  $(p^2 - 1)$  elements.

- (a) The étale algebra over  $\overline{\mathbb{Q}}$  corresponding to  $Y$  is defined by the set of all set-theoretic  $\overline{\mathbb{Q}}$ -valued functions on  $Y$ , i.e.,

$$\overline{B} \cong \underbrace{\overline{\mathbb{Q}} \times \cdots \times \overline{\mathbb{Q}}}_{p^2-1} \tag{23}$$

- (b) The action of the absolute Galois group  $G_{\mathbb{Q}}$  on  $\overline{B}$  is defined as follows: for  $\sigma \in G_{\mathbb{Q}}$  and  $\theta \in \overline{B}$ ,

$$(\sigma * \theta)(\ell) = \sigma \theta(\ell^{\sigma^{-1}}). \tag{24}$$

The  $G_{\mathbb{Q}}$ -invariants  $\overline{B}^{G_{\mathbb{Q}}}$  is denoted by  $B$ . We call  $B$  an étale algebras over  $\mathbb{Q}$  associated with the  $p$ -descent on the elliptic curve  $E$ .

- (c) We define  $H_\ell, K_\ell$ , and  $\mathbb{Q}(\ell)$  as in Definition 3.1, (f).

**Proposition 3.2** For each  $\theta \in \overline{B}^*$ , there is a function  $\phi \in \overline{A}^*$  such that

$$\theta(\ell) = \prod_{P \in \ell} \phi(P). \tag{25}$$

Conversely, if  $\phi$  is an element of  $\overline{A}^*$ , then we have a map  $u : \overline{A}^* \rightarrow \overline{B}^*$  given by

$$\phi \mapsto (\ell \mapsto \prod_{P \in \ell} \phi(P)). \tag{26}$$

**proof:** Note that the number of lines in  $Y$  is equal to the number of points in  $X$ . Let  $Q_i$ ,  $i = 1, \dots, p^2 - 1$  be the points in  $X$ ,  $\phi$  be an element of  $\bar{A}^*$ , and  $x_i$ ,  $i = 1, \dots, p^2 - 1$  be the variables which represent the (non-zero) values of a function  $\phi \in \bar{A}$ . If the condition (25) is satisfied, then we have the following  $(p^2 - 1)$  equations: let  $v_i$ ,  $i = 1, \dots, p^2 - 1$  be the lines in  $Y$ , and  $T_i$ ,  $i = 1, \dots, p^2 - 1$  be the set  $\{j \in \mathbb{Z} : Q_j \in v_i\}$ .

$$\prod_{j \in T_i} x_j = \theta(v_i), \text{ for } i = 1, \dots, p^2 - 1. \quad (27)$$

In other words, we need to show that the following map is surjective:

$$\begin{aligned} \mathbb{G}_m(\bar{\mathbb{Q}}) \times \dots \times \mathbb{G}_m(\bar{\mathbb{Q}}) &\longrightarrow \mathbb{G}_m(\bar{\mathbb{Q}}) \times \dots \times \mathbb{G}_m(\bar{\mathbb{Q}}) \\ \text{given by } (x_1, \dots, x_{p^2-1}) &\mapsto (\dots, \prod_{j \in T_i} x_j, \dots). \end{aligned} \quad (28)$$

Change the variables:  $y_i = \ln x_i$ , and  $\beta_i = \ln \theta(v_i)$ . Then, the system of equations (27) yields a system of linear equations:

$$\sum_{j \in T_i} y_j = \beta_i, \text{ } i = 1, \dots, p^2 - 1. \quad (29)$$

The solvability of this equation depends upon the determinant of the  $(p^2 - 1) \times (p^2 - 1)$  matrix  $M = [a_{ij}]$  where

$$a_{ij} = \begin{cases} 1, & \text{if } j \in T_i, \\ 0, & \text{if } j \notin T_i. \end{cases}$$

The proof of the statement:  $\det M \neq 0$  is quite involved, so I include it in Appendix. Once we establish that  $\det M \neq 0$ , the system of the linear equations has a unique solution in the following form:

$$\ln x_i = y_i = \sum b_{ij} \beta_j = \ln \prod \theta(v_i)^{b_{ij}}, \text{ for some } b_{ij} \in \mathbb{Q}, \quad (30)$$

so that we can find the corresponding values for  $x_i$  in  $\bar{\mathbb{Q}}$   $\square$

**Proposition 3.3** *Let  $\bar{B}$  be the étale algebra corresponding to  $Y$  defined in Definition 3.2.*

- (a) *If  $\theta \in B$  and  $\ell \in Y$ , then  $\theta(\ell)$  is contained in the number field  $\mathbb{Q}(\ell)$ .*
- (b) *Let  $Y_i$ ,  $i = 1, \dots, s$  be the  $G_{\mathbb{Q}}$ -orbits in  $Y$ , and  $\ell_i$  be a representative of the orbit  $Y_i$  for each  $i$ . Denote the number field  $\mathbb{Q}(\ell_i)$  by  $B_i$ . Then, the followings are true:*
  - (i) *For each  $i$ , the action of  $G_{\mathbb{Q}}/G_{B_i}$  on  $Y_i$  is simple.*
  - (ii) *Define the map  $\Phi : B \rightarrow \prod_{i=1}^s B_i$  by  $\theta \mapsto (\theta(\ell_1), \dots, \theta(\ell_s))$ . Then,  $\Phi$  is an isomorphism.*

**proof:** Recall the definitions of  $H_\ell$ ,  $K_\ell$ , and  $\mathbb{Q}(\ell)$ . Let  $\theta$  be an element of  $B$ , and  $\ell$  be a line of  $Y$ . For any  $\tau \in G_{K_\ell}$ , we have  $\theta(\ell) = \theta(\ell^\tau) = \tau \theta(\ell)$ , i.e.,  $\theta(\ell) \in K_\ell$ . Suppose that  $\sigma$  is an element of  $H_\ell$ , i.e.,  $\ell^\sigma = \ell$ , i.e.,  $\theta(\ell) = \theta(\ell^\sigma) = \sigma \theta(\ell)$ .

The well-definedness and the injectivity of the map  $\Phi$  is quite similar to that of  $\psi$  and  $\psi_+$ . To show the surjectivity, suppose that  $(\beta_1, \dots, \beta_s)$  is an element of  $\prod_{i=1}^s B_i$ . Define a function  $\theta$  on  $Y$  given by  $\theta(\ell_i) = \beta_i$  and by  $\theta(\ell) = \sigma \theta(\ell_i)$  for some  $\sigma \in G_{\mathbb{Q}}$  and some  $i$  with  $\ell_i^\sigma = \ell$ . Claim that the function  $\theta$  is well-defined. Suppose that  $\tau \in G_{\mathbb{Q}}$  fixes the line  $\ell_i$ , i.e.,  $\tau \in H_{\ell_i}$ . Then,  $\theta(\ell_i) = \theta(\ell_i^\tau)$ , and  $\theta(\ell_i) = \tau \theta(\ell_i)$  because  $\theta(\ell_i) \in \mathbb{Q}(\ell_i)$ . That is,  $\sigma \tau \theta(\ell_i) = \sigma \theta(\ell_i)$ , which establishes the well-definedness because the choice of

$\sigma$  in the definition of  $\theta$  is made from the (lef) coset  $\sigma H_{\ell_i}$ . Moreover, by the definition of  $\theta$ , we have  $\theta(\ell^\sigma) = \sigma \theta(\ell)$  for all  $\ell \in Y$  and all  $\sigma \in G_{\mathbb{Q}}$ , i.e.,  $\theta \in B$   $\square$

In the subsection 3.4, we shall take the elliptic curve:  $y^2 = x^3 + b$ , and compute the splitting of the étale algebra  $B$ .

### 3.3 The main theorem of the $p$ -descent on an elliptic curve

I will state the theorem which shows the use of the étale algebras introduced in this section.

**The  $w$ -map** Consider the Weil pairing  $e_p : E[p](\overline{\mathbb{Q}}) \times E[p](\overline{\mathbb{Q}}) \rightarrow \mu_p(\overline{\mathbb{Q}})$  where  $\mu_p(\overline{\mathbb{Q}})$  is the group of the  $p$ -th roots of unity in  $\overline{\mathbb{Q}}$  (see Chapter 3, [5]). Let  $\mu_p(\overline{A})$  be the group of the  $p$ -th roots of unity in  $\overline{A}$ , and define the  $G_{\mathbb{Q}}$ -module map  $w : E[p](\overline{\mathbb{Q}}) \rightarrow \mu_p(\overline{A})$  given by  $P \mapsto \phi_P$  where

$$\phi_P(Q) = e_p(P, Q). \quad (31)$$

The map  $w$  induces the map  $\tilde{w} : H^1(\mathbb{Q}, E[p]) \rightarrow H^1(\mathbb{Q}, \mu_p(\overline{A})) \cong A^*/(A^*)^p$  where the last isomorphism is obtained from considering the Kummer sequence for  $A$ :

$$1 \rightarrow \mu_p(\overline{A}) \rightarrow \overline{A}^* \xrightarrow{x^p} \overline{A}^* \rightarrow 1.$$

The map  $\tilde{w}$  is in fact injective (see Proposition 6.4 in [3]).

Finally, the description of  $H^1(\mathbb{Q}, E[p])$  follows.

**Theorem 3.1** (Proposition 7.10, [3]) *Let  $E$  be an elliptic curve, and  $A, A_+$ , and  $B$  be the étale algebras over  $\mathbb{Q}$  associated with the  $p$ -descent on  $E$ , defined in the subsections (3.1) and (3.2). Define the map  $u : A^*/(A^*)^p \rightarrow B^*/(B^*)^p$  induced from the map defined in (26). Then, the followings are true:*

- (a) *The automorphism group  $\text{Aut}(A/A_+)$  is a cyclic group of order  $p-1$ .*
- (b) *The cyclic group  $(\mathbb{Z}/p)^*$  simply transitively acts on  $A$  fixing  $A_+$ , and the action is given by*

$$n * \phi = \phi \circ [n]$$

*for  $n \in (\mathbb{Z}/p)^*$  and  $\phi \in A$ . Thus, there is a canonical isomorphism:  $(\mathbb{Z}/p)^* \cong \text{Aut}(A/A_+)$ . Let  $g \in \mathbb{Z}$  be a primitive root mod  $p$ , and  $\sigma_g$  be the automorphism in  $\text{Aut}(A/A_+)$ , corresponding to the integer  $g$  under the canonical isomorphism.*

- (c) *Define the map  $(g - \sigma_g) : A^*/(A^*)^p \rightarrow A^*/(A^*)^p$  given by  $\phi \mapsto \phi^g / \sigma_g \phi$ , i.e.,  $(g - \sigma_g)(\phi)(P) = \phi(P)^g / (\sigma_g \phi)(P) = \phi(P)^g / \phi([g]P)$ . Then,*

$$H^1(\mathbb{Q}, E[p]) \cong \ker(g - \sigma_g) \cap \ker u. \quad (32)$$

*If  $p = 3$ , this simply means*

$$H^1(\mathbb{Q}, E[3]) \cong \ker(N_{A/A_+} : A^*/(A^*)^3 \rightarrow A_+^*/(A_+^*)^3) \cap \ker u. \quad (33)$$

Putting together these two kernel conditions in (33), one can obtain the four conditions appearing in the description (6), for  $p = 3$  and elliptic curves:  $y^2 = x^3 + b$ .

### 3.4 Notes on Schaefer-Stoll's description

For the rest of this section, I will elaborate the condition (6) and (9) in order to make a couple of corrections on the description  $H^1(\mathbb{Q}, E[3])$  which appeared in Schaefer-Stoll's paper [3].

The étale algebra  $B$  over  $\mathbb{Q}$  defined in (3.2) splits into a product of fields as shown in Proposition 3.3. Let  $Z$  be as in by the same principle that  $A$  splits. Let  $Z$  be as in Definition 3.2, then  $Z$  has 8 elements (or lines). Let us recall the notations for some points of  $X$ , and define the automorphisms  $\sigma$ ,  $\tau_1$ , and  $\tau_2$  for the generic case of an elliptic curve.

$$\begin{aligned} P &= (0, \sqrt{b}) & R_0 &= (-\sqrt[3]{4b}, \sqrt{-3b}) & \sigma\sqrt[3]{4b} &= \sqrt[3]{4b}\zeta \\ R_1 &= (-\sqrt[3]{4b}\zeta, \sqrt{-3b}) & \tau_1\sqrt{b} &= -\sqrt{b} & \tau_1\zeta &= \zeta \\ R_2 &= (-\sqrt[3]{4b}\zeta^2, \sqrt{-3b}) & \tau_2\zeta &= \zeta^2 & \tau_2\sqrt{b} &= \sqrt{b} \end{aligned} \quad (34)$$

The automorphism  $\sigma$  is the one of order 3 on the field  $L = \mathbb{Q}(\sqrt{b}, \sqrt{-3b}, \sqrt[3]{4b})$ ,  $\tau_1$ , of order 2, and  $\tau_2$ , of order 2. All 8 points of  $X$  are written in terms of  $P, R_i$ 's.

Let  $Y$  be the set in Definition 3.2, and denote a line in  $Y$  by a triple of points  $(Q_1, Q_2, Q_3)$ . Then the  $G_{\mathbb{Q}}$ -action on  $Y$  is described in the following diagrams:

$$\begin{array}{ccc} (P, R_0, 2R_1) & \xrightarrow{\tau_1} & (2P, 2R_0, R_1) & & (P, R_1, 2R_2) & \xrightarrow{\tau_1} & (2P, 2R_1, R_2) \\ \downarrow \tau_2 & & \downarrow \tau_2 & \xrightarrow{\sigma} & \downarrow \tau_2 & & \downarrow \tau_2 \end{array} \quad (35)$$

$$\begin{array}{ccc} (P, 2R_0, R_2) & \xrightarrow{\tau_1} & (2P, R_0, 2R_2) & & (P, 2R_2, R_1) & \xrightarrow{\tau_1} & (2P, R_2, 2R_1) \\ & & (R_0, R_1, R_1) & \xrightarrow{\tau_1} & (2R_0, 2R_1, 2R_2) & & \\ & & \downarrow \tau_2 & & \downarrow \tau_2 & & \\ & & (2R_0, 2R_2, 2R_1) & \xrightarrow{\tau_1} & (R_0, R_2, R_1) & & \end{array} \quad (36)$$

The first two squares have six distinct lines, i.e., the 6 lines form one orbit, and the other two lines form another. According to the way Schaefer-Stoll wrote the description of  $H^1(\mathbb{Q}, E[3])$  in [3], they must have chosen  $(P, R_1, 2R_2)$  and  $(R_0, R_1, R_2)$  as representatives of the orbits. Let  $\ell_1$  be  $(R_0, R_1, R_2)$ , and  $\ell_2$  be  $(P, R_1, 2R_2)$ . Then, some elements of  $H_{\ell_1}$  map the elements of  $K_{\ell_1}$  as follows:  $\sqrt[3]{4b} \mapsto \sqrt[3]{4b}\zeta$ , i.e.,  $B_1 = \mathbb{Q}(\sqrt{-3b})$ . Some elements of  $H_{\ell_2}$  map the elements of  $K_{\ell_2}$  as follows:  $\zeta \mapsto \zeta^2$  and  $\sqrt{-3b} \mapsto -\sqrt{-3b}$ . Hence,  $B_2 = \mathbb{Q}(\sqrt{b}, \sqrt[3]{4b})$ . Now,  $B$  is identified as follows:

$$B \longrightarrow \mathbb{Q}(\sqrt{-3b}) \times \mathbb{Q}(\sqrt{b}, \sqrt[3]{4b}) \quad (37)$$

$$\theta \mapsto (\theta(R_0, R_1, R_2), \theta(P, R_1, 2R_2)), \quad (38)$$

We justify the third condition of (6) as it slightly differs from [3], Section 10.2.

$$i_{B_2/A_1}(\alpha_1)N_{L/B_2}(\alpha_2^\sigma) \in (B_2^*)^3.$$

Let the elliptic curve  $E$  be of the generic case. Recall that the maps  $\psi$  and  $\Phi$  defined in Proposition 3.1 and 3.3. The representatives of the orbits in  $X$  and  $Y$  are chosen as follows:

$$\begin{aligned} P_1 &= P & \ell_1 &= (R_0, R_1, R_2) \\ P_2 &= R_1 & \ell_2 &= (P, R_1, 2R_2) \end{aligned} \quad (39)$$

A function  $\phi \in A$  can be identified as  $(\alpha_1, \alpha_2) \in A_1 \times A_2$  with  $\alpha_1 = \phi(P_1)$  and  $\alpha_2 = \phi(P_2)$ . Recall the map  $u : A \rightarrow B$  defined in (26). If  $\phi \in \ker u$ , then

$$\phi(P)\phi(R_1)\phi(2R_2) = \phi(P)\phi(R_1)\phi(R_1^{\tau_2}) = \phi(P) N_{L/B_2} \phi(R_1) = \phi(P) N_{L/B_2} \phi(R_0)^\sigma = \alpha_1 N_{L/B_2} \alpha_2^\sigma \in (B_2^*)^3.$$

In [3], they state  $N_{L/B_2} \alpha_2^{\sigma^2}$ . This must be a typo.

We can also prove the fourth condition of (6). If  $\phi \in \ker u$ , then  $\phi(R_0)\phi(R_1)\phi(R_2) = N_{A_2/B_1} \phi(R_0) = N_{A_2/B_1} \alpha_2 \in (B_1^*)^3$ .

When we consider special cases such as  $\sqrt{b} \in \mathbb{Q}$  but  $\sqrt{-3b} \notin \mathbb{Q}$ ,  $\sqrt[3]{4b} \notin \mathbb{Q}$ , the norm maps of (6) have the obvious meanings. For example, when  $\sqrt{b} \in \mathbb{Q}$ ,  $A_1 = \mathbb{Q} \times \mathbb{Q}$  and  $N_{A_1/\mathbb{Q}}(x) = x_1 x_2$  where  $x = (x_1, x_2)$ . The first condition of (6) means  $x_1 x_2 \in (\mathbb{Q}^*)^3$ , i.e.,  $x_2$  is determined by  $x_1$  up to  $(\mathbb{Q}^*)^3$ , so that we could begin with  $H^1(\mathbb{Q}, E[3])$  as a subgroup of  $\mathbb{Q}^*/(\mathbb{Q}^*)^3 \times A_2^*/(A_2^*)^3$ , not as a subgroup of  $\mathbb{Q}^*/(\mathbb{Q}^*)^3 \times \mathbb{Q}^*/(\mathbb{Q}^*)^3 \times A_2^*/(A_2^*)^3$ . So, for this special case, we can take  $A_1 = \mathbb{Q}$ , and skip the first condition of (6). Likewise, when  $\sqrt{-3b} \in \mathbb{Q}$ , we could begin with  $H^1(\mathbb{Q}, E[3])$  as a subgroup of  $A_1^*/(A_1^*)^3 \times A_2^*/(A_2^*)^3$  where  $A_2' = \mathbb{Q}(\sqrt[3]{4b})$ , skipping the second condition of (6).

However, when  $\sqrt[3]{4b} \in \mathbb{Q}$ , we do not have the automorphism  $\sigma$  defined in (34), and hence, we need to write a description of  $H^1(\mathbb{Q}, E[3])$  for this special case.

As described in Proposition 3.1, the fields appearing in the splitting of the algebra  $A$  correspond to a choice of the representatives of the  $G_{\mathbb{Q}}$ -orbits in  $X$ . For this special case of an elliptic curve, we can choose the points  $P, R_0$  and  $R_1$  as representatives; see (34), and recall the definitions of the field automorphisms  $\tau_1$  and  $\tau_2$ . Let  $A_1$  be  $\mathbb{Q}(\sqrt{b})$ ,  $A_{21}$  be  $\mathbb{Q}(\sqrt{-3b})$ , and  $A_{22}$  be  $\mathbb{Q}(\sqrt{-3b}, \zeta)$ ; the fields were indexed in this way to indicate that the étale algebra  $A_2 = \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) \cong A_{21} \times A_{22}$ .

$$\begin{aligned} A &\rightarrow A_1 \times A_{21} \times A_{22} \\ \phi &\rightarrow (\phi(P), \phi(R_0), \phi(R_1)) \end{aligned} \quad (40)$$

To describe explicitly the condition of  $\phi$  being in  $\ker u$ , count the number of  $G_{\mathbb{Q}}$ -orbits in the set of 8 lines in (35). Since the automorphism  $\sigma$  does not exist for this case, we have three orbits. Let us choose the line  $\ell_1 = (R_0, R_1, R_2)$  as a representative of the first orbit,  $\ell_{21} = (P, R_0, 2R_1)$ , of the second, and  $\ell_{22} = (P, R_1, 2R_2)$ , of the third. Recall the definition of  $\mathbb{Q}(\ell)$  for a line  $\ell$  from Definition 3.2. Then,  $\mathbb{Q}(\ell_1) = \mathbb{Q}(\sqrt{-3b})$ ,  $\mathbb{Q}(\ell_{21}) = \mathbb{Q}(\sqrt{b}, \zeta)$ , and  $\mathbb{Q}(\ell_{22}) = \mathbb{Q}(\sqrt{b})$ ; let  $B_1, B_{21}$ , and  $B_{22}$  denote these fields, respectively. The étale algebra  $B$  splits as follows:

$$B \rightarrow B_1 \times B_{21} \times B_{22}. \quad (41)$$

Then, the condition that  $\phi$  is contained in  $\ker u$  means

$$\begin{aligned} \phi(R_0)\phi(R_1)\phi(R_2) &= \phi(R_0)\phi(R_1)\phi(R_1)^{\tau_1 \tau_2} \\ &= \alpha_{21} N_{A_{22}/B_1} \alpha_{22} = N_{A_2/B_1}(\alpha_{21}, \alpha_{22}) \in (\mathbb{Q}(\sqrt{-3b})^*)^3 \end{aligned} \quad (42)$$

$$\phi(P)\phi(R_0)\phi(2R_1) = \phi(P)\phi(R_0)\phi(R_1)^{\tau_1} = \alpha_1 \alpha_{21} \alpha_{22}^{\tau_1} \in (\mathbb{Q}(\sqrt{b}, \zeta)^*)^3 \quad (43)$$

$$\phi(P)\phi(R_1)\phi(2R_2) = \phi(P)\phi(R_1)\phi(R_1)^{\tau_2} = \alpha_1 \alpha_{22} \alpha_{22}^{\tau_2} \in (\mathbb{Q}(\sqrt{b})^*)^3 \quad (44)$$

Now, we have the following as a description of  $H^1(\mathbb{Q}, E[3])$  for this special case:

Let  $L'$  be the field  $\mathbb{Q}(\sqrt{b}, \sqrt{-3b}, \sqrt[3]{4b\zeta}) = \mathbb{Q}(\sqrt{b}, \zeta)$ .

$$\begin{aligned} H^1(\mathbb{Q}, E[3]) \cong & \{(\alpha_1, \alpha_{21}, \alpha_{22}) \in A_1^*/(A_1^*)^3 \times A_{21}^*/(A_{21}^*)^3 \times A_{22}^*/(A_{22}^*)^3 : \\ & N_{A_1/\mathbb{Q}}(\alpha_1) \in (\mathbb{Q}^*)^3, N_{A_2/A_{+2}}(\alpha_2) \in (A_{+,2}^*)^3, \\ & i_{B_{22}/A_1}(\alpha_1) N_{L/B_{22}}(\alpha_{22}) \in (B_{22}^*)^3, \\ & i_{B_{21}/A_1}(\alpha_1) \alpha_{21} \alpha_{22}^{\tau_1} \in (B_{21}^*)^3, \\ & N_{A_2/B_1}(\alpha_2) \in (B_1^*)^3\} \end{aligned}$$

## 4 Implementation of Finding the Generators of $H^1(\mathbb{Q}, E[3])_S$

### 4.1 Generators of $A(S, 3)$

In the definition (4), the Selmer group is described as a subgroup of  $H^1(\mathbb{Q}, E[3])_S$ , and we identify  $H^1(\mathbb{Q}, E[3])_S$  as a subgroup of  $A^*/(A^*)^3$  as in (6) and (9). Recall the definition (11) of the subgroup of the étale algebra over a number field *unramified outside the set*  $S$ . The corresponding image of  $H^1(\mathbb{Q}, E[3])_S$  in  $A^*/(A^*)^3$  is equal to the elements in  $A(S, 3)$  which satisfy the conditions appearing in (6) and (9).

For a number field  $K$ , the subgroup  $K(S, 3)$  is understood by the following short exact sequence:

$$1 \longrightarrow U_S/(U_S)^3 \longrightarrow K(S, 3) \xrightarrow{f} \text{Cl}_S(K)[3] \longrightarrow 1. \quad (45)$$

The  $S$ -unit group  $U_S$  defined by  $\{x \in \mathcal{O}_K : v_p(x) = 0, \text{ for all } p \notin \tilde{S}\}$  where  $\tilde{S}$  is the set of places of  $K$  that lie above the places contained in  $S$ . The  $S$ -class group  $\text{Cl}_S(K)$  is defined by  $\text{Cl}(K)/\langle \tilde{S} \rangle$  where  $\langle \tilde{S} \rangle$  is the subgroup generated by  $\tilde{S}$ . When there is no confusion,  $\langle \tilde{S} \rangle$  will also mean that the subgroup of the (multiplicative) ideal group generated by  $\tilde{S}$ . Then, the map  $f$  of (45) is given by  $\alpha \mapsto \mathfrak{b}$  where  $\alpha \mathcal{O}_K = \mathfrak{a} \mathfrak{b}^3$  and  $\mathfrak{a} \in \langle \tilde{S} \rangle$ .

A general algorithm of finding the generators of the  $S$ -units of a given number field  $K$  has not been found, but the system `gp-pari` computes both the  $S$ -unit group and the  $S$ -class group when it can.

Once we have the generators of  $U_S$  and  $\text{Cl}_S(K)[3]$ , we can find the corresponding element in  $K(S, 3)$ . The first map of (45) is just an inclusion, so the  $S$ -unit group can be used a part of the generators of  $K(S, 3)$ . To find the rest of the generators, we use a section of the second map. Define a section  $\Theta$  as follows:

$$\Theta : \text{Cl}_S(K)[3] \longrightarrow K(S, 3) \quad (46)$$

$$\text{given by } \mathfrak{b} \rightarrow \alpha \text{ if } \mathfrak{b}^3 = \alpha \mathfrak{a} \text{ for some } \mathfrak{a} \in \langle \tilde{S} \rangle. \quad (47)$$

**Lemma 4.1** *The map  $\Theta$  is well-defined, and  $\Theta \circ f = \text{id}_{K(S,3)}$ .*

**proof:** It is clear that the image, under  $\Theta$ , of an ideal  $\mathfrak{b} \in \text{Cl}_S(K)[3]$  is contained in  $K(S, 3)$ . Suppose that  $\mathfrak{b}' = \mathfrak{b}$  in  $\text{Cl}_S(K)$  and  $\mathfrak{b} = \alpha \mathfrak{a}$ . Then, there is  $y \in K^*$  and  $\mathfrak{a} \in \langle \tilde{S} \rangle$  such that  $\mathfrak{b}' = y \mathfrak{a}' \mathfrak{b}$ . It follows that  $(\mathfrak{b}')^3 = (y^3 (\mathfrak{a}')^3 \alpha) \mathfrak{a} = (y^3 \alpha) ((\mathfrak{a}')^3 \mathfrak{a})$ . Since  $y^3 \alpha$  and  $\alpha$  represent the same element in  $K(S, 3)$ , the map  $\Theta$  is well-defined.

Suppose that  $\alpha$  represents an element of  $K(S, 3)$ , so  $\alpha = \mathfrak{a} \mathfrak{b}^3$  for some ideals  $\mathfrak{a} \in \langle \tilde{S} \rangle$  and  $\mathfrak{b}$ . The map  $f$  sends  $\alpha \mapsto \mathfrak{b}$ . We have  $\mathfrak{b}^3 = \alpha \mathfrak{a}^{-1}$ , i.e.,  $\Theta(\mathfrak{b}) = \alpha$ . We proved  $\Theta \circ f(\alpha) = \alpha$   $\square$

## 4.2 Performing the section map in gp-pari

The system gp-pari has the command `bnfisprincipal` that writes a given ideal  $\mathfrak{c}$  as follows:

$$\mathfrak{c} = \beta \prod_{i=1}^s \mathfrak{P}_i^{r_i},$$

where  $\beta \in K^*$  and  $\mathfrak{P}_i$ 's are the generators of  $\text{Cl}(K)$ . Recall the definition of the map  $\Theta$ . To perform the map  $\Theta$  with `bnfisprincipal`, we have to find  $\mathfrak{a} \in \langle \tilde{S} \rangle$ .

For this purpose, I considered a transition matrix  $M$ . Suppose that  $\mathfrak{p}_i, i = 1, \dots, t$  generate  $\langle \tilde{S} \rangle$ , and  $\mathfrak{P}_j, j = 1, \dots, s$  are the independent generators of  $\text{Cl}(K)$ . Using `bnfisprincipal`, write each  $\mathfrak{p}_i = \beta_i \prod_{j=1}^s \mathfrak{P}_j^{m_{ij}}$ , and define  $M$  to be the transpose of the matrix  $[m_{ij}]$ . So, if we have an ideal  $\prod_{i=1}^t \mathfrak{p}_i^{r_i} \in \langle \tilde{S} \rangle$ , then

$$\prod_{i=1}^t \mathfrak{p}_i^{r_i} = \prod_{j=1}^s \mathfrak{P}_j^{v_j} \quad \text{in } \text{Cl}(K), \quad (48)$$

where  $v_j$  is the  $j$ -th entry of the column vector  $\mathbf{v} = M\mathbf{r}$  and  $\mathbf{r}$  is the column vector with the  $i$ -th entry  $r_i$ . To perform the section  $\Theta$  on  $\mathfrak{b} \in \text{Cl}_S(K)[3]$ , I did the followings:

- (a) Use `bnfisprincipal` to write:  $\mathfrak{b}^3 = \beta \prod_{j=1}^s \mathfrak{P}_j^{v_j}$ .
- (b) Solve  $M\mathbf{r} \equiv \mathbf{v} \pmod{\mathbf{n}}$  for  $\mathbf{r}$  where  $\mathbf{v}$  is as before and  $\mathbf{n}$  is the column vector with entries  $n_j$ , the order of  $\mathfrak{P}_j$  in  $\text{Cl}(K)$ , and put  $\mathfrak{a} = \prod_{i=1}^t \mathfrak{p}_i^{r_i}$ . Then we have  $\mathfrak{a} = \mathfrak{b}^3$  in  $\text{Cl}(K)$ .
- (c) Then,  $\alpha \mathcal{O}_K = \mathfrak{b}^3 \mathfrak{a}^{-1}$  for some  $\alpha \in K(S, 3)$ , and the  $\alpha$  is the image under the section map of (45).

The equation  $M\mathbf{r} \equiv \mathbf{v}$  is always solvable because  $\mathfrak{b}^3 = \mathfrak{a}$  in  $\text{Cl}(K)$  for some  $\mathfrak{a} \in \langle \tilde{S} \rangle$ , i.e., there are  $r_i$ 's such that (48) is satisfied.

## 4.3 Checking the conditions (6) with gp-pari

To check with gp-pari the conditions in (6), we need to redefine in gp the fields  $A_i$  defined in (3.1) as extensions of some intermediate fields. For example, for the generic case, the extension  $A_2$  of  $A_{+,2}$  is treated as follows. Note that  $A_2 = \mathbb{Q}(\sqrt{-3b} + \sqrt[3]{4b})$  and  $A_{+,2} = \mathbb{Q}(\sqrt[3]{4b})$ :

```
g=t^3-4*b; Aplus2=bnfinit(g);
aa=Mod(t,g);
f=(x-aa)^2-(-3*b);
z=Mod(x,f);
cc=subst(h,x,z);
    \\ h is a polynomial in x over the rational numbers
    \\     representing an element of the field A2.
norm(cc);
```

The gp-variable `aa` is the generator  $\sqrt[3]{4b}$  of  $A_{+,2}$ , and `z` is the generator  $\sqrt{-3b} + \sqrt[3]{4b}$  of  $A_2$ . In the second line of the script, with the `Mod` command, we implicitly define the field  $\mathbb{Q}[T]/g(T) \cong A_{+,2}$  in gp-pari. On top of it, we also implicitly define is the quadratic extension of  $A_{+,2}$ ,  $A_2 = A_{+,2}[X]/f(X)$  where  $f(X) = (X - \sqrt[3]{4b})^2 + 3b$ . Note that all elements of  $A_2$  can be represented by a polynomial  $h(X)$  over  $\mathbb{Q}$  where  $X$

corresponds to  $\sqrt{-3b} + \sqrt[3]{4b}$ . To compute in `gp-pari` the norm of the element represented by  $h(X)$  to  $A_{+,2}$ , substitute  $X$  with  $z$  which is  $X$  in  $A_{+,2}[X]/f(X)$  and take the `norm` command.

Using this technique, all the norms in (6) are computed. What is left is to determine whether or not a given element of a number field  $K$  is a cube. The procedure of checking this property is stated in the following quite trivial lemma:

**Lemma 4.2**  *$K$  is a number field, and  $\alpha$  is a non-zero element of  $K$ . Then,  $\alpha \in (K^*)^3$  iff  $\alpha$  satisfies the following two conditions:*

- (a)  $\alpha \mathcal{O}_K = \mathfrak{a}^3$  and  $\mathfrak{a} = \beta \mathcal{O}_K$  for some  $\beta \in K^*$ .
- (b)  $\alpha/\beta^3 \in (\mathcal{O}_K^*)^3$ .

**proof:** Suppose that  $\alpha = \gamma^3$  for some  $\gamma \in K^*$ , i.e.,  $\alpha \mathcal{O}_K = (\gamma \mathcal{O}_K)^3$ . If  $\beta$  is another generator of  $\gamma \mathcal{O}_K$ , then  $\beta = \gamma u$  for some  $u \in \mathcal{O}_K^*$ , i.e.,  $\alpha/\beta^3 = 1/u^3 \in (\mathcal{O}_K^*)^3$ . The converse is trivial since the condition (??) implies  $\alpha$  is a cube.  $\square$

The system `gp-pari` has the commands `idealfactor` for factoring ideals, `bnfisprincipal` for finding a principal generator, and `bnfisunit` for determining whether or not a given element is a unit; if so, it writes the element in terms of the fundamental units. As easily anticipated, factoring ideals is an expensive computation, and writing a given element in terms of the fundamental units is even more costly. In particular, when the field is “complicated,” e.g., the unit group and the class group are big, this part of computation takes long time. Indeed, when such complicated fields are involved, `selmer3333.gp` takes more than 20-30 seconds to finish the computation. For most cases with complicated fields involved, the level of real precision in `gp-pari` has to be increased to find the fundamental units and to run `bnfisunit`.

## 5 Local Conditions

Recalling the definition (4) of the Selmer group, we see that the next tasks are finding the generators of  $\text{Im } \delta_q$  and checking the condition of (4). For all cases, the lemma 2.1 computes the generators for  $q \in S$  not equal to 3.

However, at  $q = 3$ , there is not a simple formula. As mentioned in the beginning of this report, I implemented a random search in `gp-pari` since it finds the generators of  $\text{Im } \delta_3$  quickly. Both the random search and the terminating procedure of finding the generators will be explained in this section. Since this part is going to be a bit lengthier, let me proceed with the following subsection.

### 5.1 Local condition at $q \neq 3$

Once we have the generators of  $\text{Im } \delta_q$  in  $A^*/(A^*)^3$ , we need to check the condition of (4). We identified  $H^1(\mathbb{Q}, E[3])$  and  $H^1(\mathbb{Q}_q, E[3])$  as follows, and  $A_q$  is identified as in Lemma 2.1:

$$\begin{array}{ccc} H^1(\mathbb{Q}, E[3])_S & \xrightarrow{w} & A^*/(A^*)^3 \\ \text{res}_q \downarrow & & \pi \downarrow \\ H^1(\mathbb{Q}_q, E[3]) & \xrightarrow{w_q} & A_q^*/(A_q^*)^3 \end{array}, \quad (49)$$

where  $w$  and  $w_q$  are injective, and  $\pi(\alpha) = \alpha \otimes 1$ . Since the diagram is commutative, the condition (4) means that if  $w(\xi) = \alpha$  for  $\xi \in H^1(\mathbb{Q}, E[3])_S$ , then  $\pi(\alpha) \in w_q(\text{Im } \delta_q)$ . In practice, the map  $\pi$  means the following:

for the generic case and  $q \equiv 2 \pmod{3}$ , let  $z_0$  be an element of  $\mathbb{Q}_q$  such that  $z_0^2 - b = 0$ , and  $\pi_{ij}$  be the field isomorphisms defined below.

$$\mathbb{Q}(\sqrt{b}) \times \mathbb{Q}(\sqrt{-3b}, \sqrt[3]{4b}) \longrightarrow \mathbb{Q}_q \times \mathbb{Q}_q \times \mathbb{Q}_q(\sqrt{-3b}, \sqrt[3]{4b}), \quad (50)$$

$$\alpha = (\alpha_1, \alpha_2) \mapsto (\pi_{11}\alpha_1, \pi_{12}\alpha_1, \pi_2\alpha_2), \quad (51)$$

$$\text{where } \pi_{11}\sqrt{b} = z_0, \pi_{12}\sqrt{b} = -z_0, \pi_2(\sqrt{-3b} + \sqrt[3]{4b}) = \sqrt{-3} \cdot z_0 + \sqrt[3]{4b}. \quad (52)$$

The map involves a choice of  $\sqrt{b}$ ; just fix one once and for all.

For  $q \equiv 1 \pmod{3}$ , the map  $\pi$  is understood similarly. For this case, the algebra  $\mathbb{Q}_q(\sqrt{-3b}, \sqrt[3]{4b})$  splits further. Write  $\pi_2 = (\pi_{21}, \pi_{22})$ . We have  $\pi_2(\sqrt{-3b} + \sqrt[3]{4b}) = (\sqrt{-3} z_0 + \sqrt[3]{4b}, -\sqrt{-3} z_0 + \sqrt[3]{4b})$  (see Lemma 2.1). However, the map  $\pi_{21}$  will be the same as in the case:  $q \equiv 2 \pmod{3}$ . That is, rather than choosing  $\sqrt{-3} \in \mathbb{Q}_3$ , use the description of  $\zeta$  as in Lemma 2.1 so that we can avoid the ambiguity of choosing  $\zeta \in \mathbb{Q}_3$ , in practice. It is actually important to make only one choice (for  $\sqrt{b}$ ) and keep the other elements consistent with the choice.

It remains to check in gp if  $\pi(\alpha_1, \alpha_2) \in A_q^*/(A_q^*)^3$  is contained in  $\langle\langle 4b, 2b^2, \zeta^2 \rangle\rangle$  or  $\langle\langle 4b, 2b^2, \zeta^2, \zeta \rangle\rangle$  depending on the congruence relation of  $q$ . Hence, we need an algorithm to check if a given element is a cube in a finite extension of  $\mathbb{Q}_q$ . We will call this process *the local cube-test at  $q$* .

### Local cube-test at $q \neq 3$

The test uses Hensel's lemma for a special case:

**Lemma 5.1**  *$K$  is a number field generated by (an algebraic integer)  $\beta$  with the minimal polynomial  $f(x)$  defined over  $\mathbb{Q}$ , i.e.,  $K = \mathbb{Q}(\beta)$ . Let  $q \neq 3$  be a rational prime, and  $\mathfrak{q}$  be a prime ideal of  $\mathcal{O}_K$  lying above  $q$ . Then the local field  $K_{\mathfrak{q}}$  is generated by some  $\beta_{\mathfrak{q}} \in K_{\mathfrak{q}}$  such that  $f(\beta_{\mathfrak{q}}) = 0$ , i.e.,  $K_{\mathfrak{q}} = \mathbb{Q}_{\mathfrak{q}}(\beta_{\mathfrak{q}})$ .*

*Suppose that  $g(x)$  is a polynomial over  $\mathbb{Q}_{\mathfrak{q}}$ , and  $\pi_{\mathfrak{q}} \in K$  is a uniformizer of the local field  $K_{\mathfrak{q}}$ . If  $g(\beta_{\mathfrak{q}})$  is a unit of the  $\mathfrak{q}$ -adic integers of  $K_{\mathfrak{q}}$ ,  $g(\beta_{\mathfrak{q}})$  is a cube in  $K_{\mathfrak{q}}$  iff  $g(\beta_{\mathfrak{q}}) \equiv a^3 \pmod{\pi_{\mathfrak{q}} \mathcal{O}_{K_{\mathfrak{q}}}}$  for some  $a \in \mathcal{O}_{K_{\mathfrak{q}}}$ .*

**proof:** We have the field isomorphism  $K \cong \mathbb{Q}[x]/f(x)$ , and  $f(\beta) = 0$ . It follows that  $K \otimes \mathbb{Q}_p \cong \prod_{i=1}^s \mathbb{Q}_p[x]/f_i(x)$  where  $f(x) = \prod_{i=1}^s f_i(x)$  is a factorization into irreducible polynomials over  $\mathbb{Q}_p$ . These factors  $f_i(x)$  correspond to the prime ideals  $\mathfrak{q}_i$  lying above  $p$ , and  $K_{\mathfrak{q}_i} \cong \mathbb{Q}_p[x]/f_i(x)$ . Saying  $q = q_1$ , we can find  $\beta_{\mathfrak{q}} \in K_{\mathfrak{q}}$  such that  $f_1(\beta_{\mathfrak{q}}) = 0$ , and it is obvious that  $K_{\mathfrak{q}} = \mathbb{Q}_p(\beta_{\mathfrak{q}})$  and  $f(\beta_{\mathfrak{q}}) = 0$ .

The rest of the statement of the lemma is a standard application of Hensel's Lemma to the polynomial  $x^3 - a$   $\square$

As a matter of fact, performing Lemma 5.1 in gp-pari is not very convenient. Let me summarize in the following proposition how it was actually done in gp-pari.

First, let me introduce a couple of definitions. Given a positive integer  $N$ , define the  $N$ -truncation map  $r_N : \mathbb{Q}_q \rightarrow \mathbb{Q}$  given by  $\sum_{n=m}^{\infty} a_n q^n \mapsto \sum_{n=m}^{N-1} a_n q^n$ , and  $R_N : \mathbb{Q}_q[x] \rightarrow \mathbb{Q}[x]$  given by  $\sum a_n x^n \mapsto \sum r_N(a_n) x^n$ ; call  $R_N$  the  $N$ -truncation map on polynomials.

**Proposition 5.1** *Assume the same context of Lemma 5.1. Put  $\tilde{g} = R_N(g)$  for some  $N$  so that  $\tilde{g} \neq 0$ . Then  $g(\beta_{\mathfrak{q}})$  is a cube in  $K_{\mathfrak{q}}^*$  iff  $\tilde{g}(\beta)$  is a cube in  $(\mathcal{O}_K/\mathfrak{q})^*$ .*

**proof:** Suppose that  $g(\beta_q)$  is a cube in  $K_q^*$ , and consider the embedding  $i$  of  $K$  into  $K_q$  which takes  $\beta \mapsto \beta_q$ . Note  $g(\beta_q) = \tilde{g}(\beta_q) + q^N y = \tilde{g}(i(\beta)) + q^N y$  for some  $y \in \mathcal{O}_{K_q}$ , i.e., for some  $a \in \mathcal{O}_{K_q}$ ,  $a^3 = g(\beta_q) \equiv \tilde{g}(i(\beta)) \pmod{\pi_q \mathcal{O}_{K_q}}$ , and  $\tilde{g}(i(\beta)) \not\equiv 0 \pmod{\pi_q \mathcal{O}_{K_q}}$ . Since  $\mathcal{O}_{K_q}/\pi_q \mathcal{O}_{K_q} \cong \mathcal{O}_K/\mathfrak{q}$ ,  $\tilde{g}(\beta) \equiv b^3 \pmod{\mathcal{O}_K/\mathfrak{q}}$  for some  $b \in \mathcal{O}_K$ .

By Hensel's lemma, the converse is easily proved: if  $\tilde{g}(\beta) \equiv a^3 \pmod{\mathfrak{q} \mathcal{O}_K}$  for some  $a \in \mathcal{O}_K$ , then the congruence remains valid modulo  $\pi_q K_q$ , and hence  $a^3 \equiv \tilde{g}(\beta_q) \equiv g(\beta_q) \pmod{\pi_q K_q}$  since  $\tilde{g}(\beta_q) = g(\beta_q) + q^N y$ .  $\square$

With this proposition, testing if a given element  $g(x) \in \mathbb{Q}[x]/f(x)$  is a cube modulo  $\pi_q \mathcal{O}_{K_q}$  is done by testing if  $\tilde{g}(x)$  modulo  $\mathfrak{q}$  is a cube, where  $x$  corresponds to the generators of  $K_q$  and  $K$ . Hence, the problem reduces to finding the cyclic generator of  $(\mathcal{O}_K/\mathfrak{q})^*$  with which it is easier to determine whether or not  $\tilde{g}(x)$  is a cube. The system `gp-pari` has the command `idealstar` which in general computes the structure and the generators of  $\mathcal{O}_K/\mathfrak{a}$  for an integral ideal  $\mathfrak{a}$ . So, using the generator  $\gamma$  of  $(\mathcal{O}_K/\mathfrak{q})^*$  that `gp-pari` finds, I created a list of cubes in  $(\mathcal{O}_K/\mathfrak{q})^*$ , i.e.,  $\{\gamma^{3k} : k = 1, \dots, m\}$  where  $3m$  is the order of  $(\mathcal{O}_K/\mathfrak{q})^*$ . With this list prepared, testing if  $\tilde{g}(x)$  is a cube modulo  $\mathfrak{q}$  is just *comparing*  $\tilde{g}(x)$  with the elements in the list. When we actually *compare* an element  $\tilde{g}(\beta)$  with the elements in the list, we compute the  $\mathfrak{q}$ -valuation of  $\tilde{g}(\beta) - \gamma^{3k}$  to see if  $\tilde{g}(\beta) \equiv \gamma^{3k} \pmod{\mathfrak{q}}$  for some  $k$ . The `gp-pari` command `nfeltval` computes such valuations.

**Example:** Recall the definition (5) of the fields  $A_1$  and  $A_2$ . I will show by an example how to actually determine whether an element  $\alpha = (\alpha_1, \alpha_2) \in A \cong A_1 \times A_2$  is mapped to  $\text{Im } \delta_q$  as required in (49) to be an element of the Selmer group. Suppose that  $q = 5$ , and that an element  $\alpha = (\alpha_1, \alpha_2) \in A_1 \times A_2$  is *represented by polynomials*  $g'_1(x)$  and  $g'_2(x)$  defined over  $\mathbb{Q}$ , i.e.,  $g'_1(\sqrt{b}) = \alpha_1$  and  $g'_2(\sqrt{-3b} + \sqrt[3]{4b}) = \alpha_2 \in A_2$ . To check the local condition at  $q$  (see Lemma 2.1), we need to see, for example, whether or not  $\pi_2 \alpha_2 \equiv (\zeta^2)^k \pmod{(A_2)_q^*/((A_2)_q^*)^3}$  for some  $k = 0, 1, 2$  where  $(A_2)_q = \mathbb{Q}_q(\sqrt{-3b}, \sqrt[3]{4b})$  and the map  $\pi_2$  is defined as in (50). For both cases:  $q \equiv 1, 2 \pmod{3}$ , we apply the following procedure:

- (a) Choose once and for all, a prime  $\mathfrak{q}$  lying above  $q$  using `idealprimedec` and  $\sqrt{b} = z_0 \in \mathbb{Q}_q$  using `polrootspadic`. We write  $\zeta$  in terms of  $z_0$  and  $\beta_q = \sqrt{-3b} + \sqrt[3]{4b} \in K_q$ :

$$\begin{aligned} \sqrt{-3b} &= (\beta_q^3 - 9b\beta_q - 4b)/(3\beta_q^2 - 3b), \\ \sqrt{-3} &= \sqrt{-3b}/z_0, \quad \zeta = (-1 + \sqrt{-3})/2. \end{aligned}$$

That is, we find a rational function  $f(x)$  over  $\mathbb{Q}_q$  such that  $\zeta = f(\beta_q)$ . Moreover, we can find a polynomial  $g(x)$  defined over  $\mathbb{Q}_q$  such that  $f(\beta_q)^{-1} = g(\beta_q)$ .

- (b) Take a *polynomial*  $g_2(x) = g'_2(x)g(x)^{2k}$  for  $k = 0, 1, 2$ , so that  $g_2(\beta_q) = g'_2(\beta_q)/(\zeta^2)^k$ . Use Proposition 5.1 to test if  $g_2(x)$  over  $\mathbb{Q}_q$  corresponds to a cube modulo  $\pi_q$ .

The maps  $\pi_{11}$  and  $\pi_{12}$  are easier to perform. Suppose that  $g'_1(x)$  is a polynomial defined over  $\mathbb{Q}$ , such that  $\alpha_1 = g'_1(\sqrt{b})$ . To see if  $\pi_{11}(w(\alpha_1)) \in w_q(\text{Im } \delta_q)$ , take the polynomial  $g_{11}(x) = g'_1(z_0)/(4b)^k$ , which is in fact an element of  $\mathbb{Q}_q$ . The local cube-test in  $\mathbb{Q}_q$  is easy. Since  $\pi_{11}A_1 \cong \pi_{12}A_1$ , the test for  $\text{Im } \pi_{12}$  is not necessary.

**Script** As an example of testing if  $g(x)$  is a cube in  $K_q$ , I include the user-defined `gp`-function of `selmer3333.gp`, which performs this task.

```

{ \\ w is in polmod,
  \\ mod Q-polynomial with coeff q-adic.
wiscubeatq(L,w,q)=
  local(P,T,pi,n,ans,ww,k);
  if(L==A1,T=SA1,SA2); \\ (1)
  P=picktheprime(T,q);
  pi=P[2];
  w=component(w,2);
  w=fitiT_q(w,q); \\ (2)
  w=nfalgtobasis(L,w);
  n=nfeltval(L,w,P);
  if(n%3!=0, ans=0,
    ww=nfeltpow(L,pi,n);
    w=nfeltdiv(L,w,ww);
    \\ w has valuation 0 at P.
    k=kthprime(S,q);
    if(L==A1,T=littlecubes[k],
      T=bigcubes[k]);
    ans=testit_q(L,w,P,T,q)
  );
  ans
}

```

The script is the definition of a user-defined function in `gp-pari`. `wiscubeatq` checks if  $w$  is a cube in the completion of a global field  $L$  at a prime ideal lying over  $q$ . `component`, `nfalgtobasis`, `nfeltval`, `nfeltpow`, and `nfeltdiv` are built-in `gp`-functions, and all other functions are user-defined.

In line (1) of the script, it determines whether the field is  $A_1$  or  $A_2$ , and chooses the corresponding  $\langle \tilde{S} \rangle$ , and `pi` is the uniformizer of  $q$ . The command `fitiT_q` performs the truncation map  $R_N$  where  $N$  is pre-defined, so  $w$  is a polynomial defined over  $\mathbb{Q}$  in line (2). If at this stage  $w$  is zero, then the error message: *padic precision low; try again* is displayed. If not, it carries on going to find the  $q$ -valuation  $n$  of  $w$ , and make  $w$  have  $q$ -valuation 0 by dividing it by  $\pi^n$  if  $n$  is divisible by 3. The command `testit_q` tests if the polynomial  $w$  is a cube in  $(\mathcal{O}_K/q)^*$ .

## 5.2 Local condition at $q = 3$

There is no simple formula for the generators of  $\text{Im } \delta_3$ , but in theory, finding the generator is a finite amount of computation with use of Hensel's lemma. Nevertheless,  $\dim_{\mathbb{F}_3} E(\mathbb{Q}_3)/3E(\mathbb{Q}_3) = \dim E[3](\mathbb{Q}_3) + 1$  is true for all elliptic curves (see [1]), and hence, we know the size of  $E(\mathbb{Q}_3)/3E(\mathbb{Q}_3)$  in advance.

The actual random search implemented in `selmer3333.gp` is a search of the generators of  $E(\mathbb{Q}_3)/3E(\mathbb{Q}_3)$ . To find the corresponding images in  $A^*/(A^*)^3$ , we need a concrete description of the map which takes  $E(\mathbb{Q}_3)/3E(\mathbb{Q}_3)$  to  $A^*/(A^*)^3$ . Schaefer describes this map very well in [2], called *the F-map*.

### F-map

#### Definition 5.1

- (a) Let  $E$  be an elliptic curve over  $\mathcal{Q}$ ,  $f \in \overline{\mathcal{Q}}(E)$ , and  $D \in \text{Div}(E)$ . If the support of the divisor  $D$  is disjoint with  $\text{div } f$ , we define  $f(D) = \prod_{P \in \text{Supp}(D)} f(P)^{n_P}$ , where  $D = \sum_{P \in \text{Supp}(D)} n_P(P)$ .
- (b) The  $F$ -map is defined as follows. First, consider the diagram:

$$\begin{array}{ccc}
 E(\mathbb{Q}) & \xrightarrow{F} & A^*/(A^*)^3 \\
 \iota \downarrow & & \downarrow \text{id} \\
 \text{Pic}^0(E)(\mathbb{Q}) & \xrightarrow{F'} & A^*/(A^*)^3
 \end{array} \tag{53}$$

where the maps  $\iota$ ,  $F'$  and  $F''$  are defined as follows.

- (i)  $\iota(P) = (P) - (O)$ .

- (ii) If the support of a divisor  $D \in \text{Div}(E)$  is defined over  $\mathbb{Q}$  and does not intersect  $E[3](\overline{\mathbb{Q}})$ , we call  $D$  a *good divisor*.
- (iii) Given a nontrivial point  $P \in E[3](\overline{\mathbb{Q}})$ , let  $f_P$  be an element of  $\overline{\mathbb{Q}}(E)$  with  $\text{div } f_P = 3(P) - 3(O)$  (see Corollary 3.5, Chapter 3 of [5]).
- (iv) For a good divisor  $D$ , define

$$F'(D) = \phi \in A, \text{ given by } \phi(Q) = \prod_{P \in \text{Supp}(D)} f_Q(P)^{n_P}.$$

- (v) Define  $F(P) = F'(\iota(P))$ .

The map  $F$  is a well-defined group homomorphism:  $E(\mathbb{Q})/3E(\mathbb{Q}) \rightarrow A^*/(A^*)^3$  (see Lemma 2.1 in [2]), i.e., there is a good divisor for all points of  $E(\mathbb{Q})$ , and at any good divisors  $D_1$  and  $D_2$  linearly equivalent to each other,  $F'(D_1) = F'(D_2)$ . For example, let  $P$  and  $R_0$  be the points of  $E[3](\overline{\mathbb{Q}})$  defined in (34), and  $T \in E$  with  $[6]T \neq O$ . We have  $(T) - (O) \sim (2T) - (T)$ , i.e.,  $(2T) - (T)$  is a good divisor. Noting that  $A \cong A_1^*/(A_1^*)^3 \times A_2^*/(A_2^*)^3$ , we can define  $F(T)$

$$F(T) = \left( \frac{f_P(2T)}{f_P(T)}, \frac{f_{R_0}(2T)}{f_{R_0}(T)} \right).$$

The  $F_q$ -map is similarly defined as a map:  $E(\mathbb{Q}_q)/3E(\mathbb{Q}_q) \rightarrow A_q^*/(A_q^*)^3$ .

## Random Search I

The task is to find one or two points of  $E(\mathbb{Q}_3)$  that are not divisible by 3. The structure of  $E(\mathbb{Q}_3)$  is understood in terms of  $E_0(\mathbb{Q}_3)$  and  $E_1(\mathbb{Q}_3)$  (see Chapter 4 of [5]). The standard definitions of  $E_0$  and  $E_1$  are given for a minimal model of  $E$ , but just to give the definition of these subgroups of  $E(\mathbb{Q}_3)$ , it is not necessary to put it in a minimal model.

### Definition 5.2

Let  $E$  be an elliptic curve given by  $y^2 = x^3 + b$  for  $b \in \mathbb{Z}$ .

- (a)  $E_1(\mathbb{Q}_3) = \{(x, y) \in E(\mathbb{Q}_3) : v_3(x) < 0\}$ , which is called the *kernel of reduction of  $E$  at 3* when it's in a minimal model.
- (b)  $E_0(\mathbb{Q}_3) = \{(x, y) \in E(\mathbb{Q}_3) : v_3(x) < 0, \text{ or } x \not\equiv -b \pmod{3}\}$  is called the *connected component of  $O$  of  $E(\mathbb{Q}_3)$* .

$E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3)$  is isomorphic to  $(\mathbb{F}_3, +)$ ;  $E$  is said to *have additive reduction at 3*. In general, this quotient group is isomorphic to either  $(\mathbb{F}_q, *)$  or  $(\mathbb{F}_q, +)$ ; see [6] for more of *type of reductions of elliptic curves*.

Coming back to our problem, we want to find a point of  $E(\mathbb{Q}_3)$  which is not divisible by 3. It is a well-known fact that

$$E_1(\mathbb{Q}_3) \stackrel{\phi}{\cong} (\mathbb{Z}_3, \mathcal{F}),$$

where  $\mathcal{F}$  is the two-variable power series over  $\mathbb{Z}$  which defines a group law on  $\mathbb{Z}_3$  endowed from the group structure of  $E(\mathbb{Q}_3)$ . Since this isomorphism  $\phi$  is well-understood and the filtrations:  $3^n E_1(\mathbb{Q}_3) \rightarrow 3^{n+1} E_1(\mathbb{Q}_3)$  are surjective, a nontrivial point  $T$  of  $E_1(\mathbb{Q}_3)/3E_1(\mathbb{Q}_3)$  generates  $E_1(\mathbb{Q}_3)$ , and assuming  $\phi^{-1}(3) =$

$T$  makes it easy to find one point, namely  $T$ . However,  $E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3) \cong \mathbb{Z}/3$  implies that such  $T$  might be divisible by 3. According to some of the computations I performed, there are cases:  $E_0(\mathbb{Q}_3) \rightarrow E_1(\mathbb{Q}_3)$  given by the multiplication-by-3 is not surjective, and there are cases: it is surjective.

For the same reason, a point in  $E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3)$  might be divisible by 3 when  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$  is  $\mathbb{Z}/3$ . Thus, trying to find points in  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$  reduces the chance of the points being divisible by 3.

**Lemma 5.2** *Suppose that  $E$  is an elliptic curve defined over  $\mathbb{Z}$  with  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3) \cong \mathbb{Z}/3$ . If  $T \in E(\mathbb{Q}_3)$  represents a nontrivial point of  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$ , then  $T$  is not divisible by 3.*

*Suppose that  $E$  is an elliptic curve defined over  $\mathbb{Z}$  with  $\#E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$  not divisible by 3. If  $T \in E_0(\mathbb{Q}_3)$  represents a nontrivial point of  $E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3)$ , then  $T$  is not divisible by 3.*

**proof:** Suppose that  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3) \cong \mathbb{Z}/3$ . If  $T$  is divisible by 3, i.e.,  $3T' = T$  for  $T' \in E(\mathbb{Q}_3)$ , then  $T$  must be in  $E_0(\mathbb{Q}_3)$ .

Suppose that  $\#E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$  not divisible by 3 and  $3T' = T$  for some  $T' \in E(\mathbb{Q}_3)$ .  $T'$  cannot represent a nontrivial point of  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$  because  $[3]$  is an automorphism on  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$ .  $T'$  cannot represent a nontrivial point of  $E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3)$  because it forces  $T$  to be contained in  $E_1(\mathbb{Q}_3)$ .  $\square$

The above lemma completes the theoretical description of a method of finding one point of  $E(\mathbb{Q}_3)$  that is not divisible by 3, but I find a random search performs the task far quicker, and with random search, it was easier to find a second point when  $E(\mathbb{Q}_3)/3E(\mathbb{Q}_3) \cong \mathbb{Z}/3 \oplus \mathbb{Z}/3$ .

## Random Search II

The actual random search in `selmer33333.gp` was done by finding points in  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$  regardless of the structure of  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$  which was distinguished in the lemma 5.2. One non-trivial computation we have to perform in this random search is checking the 3-divisibility. The 3-divisibility test can be done quickly using the  $F$ -map introduced earlier. From the diagram of the definition ??, we obtain the following computationally useful lemma:

**Lemma 5.3** *Suppose that  $T \in E(\mathbb{Q}_3)$ . Then,  $T \in 3E(\mathbb{Q}_3)$  iff  $F(T)$  is a cube in  $A_3$ .*

**proof:**  $E(\mathbb{Q}_3)/3E(\mathbb{Q}_3) \rightarrow A_3^*/(A_3^*)^3$  is an injective group homomorphism.  $\square$

Directly checking the 3-divisibility of a point of an elliptic curve over a local field is much more computation than checking if an element is a cube in  $A_3$ , which is explained in the next section.

To find points of  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$ , I considered different cases depending on the valuation of  $b$ . The followings are a couple of examples. When a second point has to be found, I applied the same random search until it finds one (independent of the first one):

**Case:**  $v_3(b) = 0$  and  $b \not\equiv 1, 8 \pmod{9}$ . It turns out that  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$  is the trivial group. Points of  $E(\mathbb{Q}_3)$  in form of  $(\alpha, \beta) \in \mathbb{Z}_3 \times \mathbb{Z}_3$  represents a nontrivial point of  $E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3)$ . Varying  $\alpha$  over  $\mathbb{Z}$ , we find many solutions for  $\beta \in \mathbb{Q}_3$ , and look for a point which passes the 3-divisibility condition for which we use Lemma 5.3.

**Case:**  $v_3(b) = 3$ . A point of  $E(\mathbb{Q}_3)$ , in form of  $(3\alpha, 3\beta) \in \mathbb{Z}_3 \times \mathbb{Z}_3$  represents a nontrivial point of  $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3)$ .

### Cube-test at $q = 3$ .

As shown in Lemma 5.3, to check the 3-divisibility of a point of  $E(\mathbb{Q}_3)$ , we need to check if an element is a cube in  $A_3$ . Since Lemma 5.1 on p.17 is not applicable, we need the following refined version:

**Lemma 5.4**  *$K$  is a number field, and  $\mathfrak{q}$  is a prime ideal of  $\mathcal{O}_K$  lying above 3, of ramification index  $e$ . Then,  $a \in (\mathcal{O}_{K_{\mathfrak{q}}}^*)^3$  iff  $x^3 - a \equiv 0 \pmod{\mathfrak{q}^N}$  is solvable where  $N = \lceil (3e + 1)/2 \rceil$ .*

**proof:** Let  $f(x) = x^3 - a = f(x_0) + 3x_0^2(x - x_0) + 3x_0(x - x_0)^2 + (x - x_0)^3$ ,  $N = \lceil (3e + 1)/2 \rceil$ , and  $\pi$  be a uniformizer of  $\mathfrak{q}$ . Suppose that  $n \geq N$ , and  $\alpha_n = b_0 + \cdots + b_{n-1}\pi^{n-1}$ ,  $b_0 \neq 0$  such that  $\alpha_n^3 - a \equiv 0 \pmod{\mathfrak{q}^n}$ , where  $b_i$  are one of the fixed representatives of  $\mathcal{O}_K/\mathfrak{q}$ . Then, we can find  $\alpha_{n+1} \pmod{\mathfrak{q}^{n+1}}$  such that  $\alpha_{n+1}^3 - a \equiv 0 \pmod{\mathfrak{q}^{n+1}}$ . Let:  $\alpha_{n+1} = \alpha_n + c\pi^{n-e}$  for  $c \in (\mathcal{O}_K/\mathfrak{q})^*$ .

$$f(\alpha_{n+1}) = f(\alpha_n) + 3\alpha_n^2(c\pi^{n-e}) + 3\alpha_n(c\pi^{n-e})^2 + (c\pi^{n-e})^3.$$

$v_\pi(3\alpha_n(c\pi^{n-e})^2) = 2n - e$ , and  $v_\pi((c\pi^{n-e})^3) = 3n - 3e$ .  $n \geq N \geq (3e + 1)/2 \geq e + 1$  implies  $2n - e \geq n + 1$  and  $3n - 3e \geq n + 1$ . Then  $0 \equiv (\alpha_n^3 - a) + (u\pi^e)\alpha_n^2c\pi^{n-e} \pmod{\mathfrak{q}^{n+1}}$  where  $3 = u\pi^e$ , i.e.,  $0 \equiv (\alpha_n^3 - a)/\pi^n + u\alpha_n^2c \pmod{\mathfrak{q}}$  which is solvable for  $c$  since  $\alpha_n^2u \in (\mathcal{O}_K/\mathfrak{q})^*$ .  $\square$

Using `idealstar`, we can prepare the list of cubes for  $\mathcal{O}_K/\mathfrak{q}^N$ . This cube-test at  $q = 3$  is also used to check the local condition of (4) in p.4 at  $q = 3$ . This concludes all the computation. The set of the elements of  $H^1(\mathbb{Q}, E[3])_S$  which passed all the local conditions is  $\text{Sel}^{(3)}(E/\mathbb{Q})$ .

## 6 Program: selmer3333.gp

`selmer3333.gp` displays only one quantity  $\dim_{\mathbb{F}_3} \text{Sel}^{(3)}(E/\mathbb{Q})$ , but a user can display the generators of  $H^1(\mathbb{Q}, E[3])_S$ .

I was interested in how the  $S$ -unit group and the 3-part of the  $S$ -class group of  $A$  contribute to  $\text{Sel}^{(3)}(E/\mathbb{Q})$ ; it's known that the  $S$ -unit group contributes at most by dimension 1. Such knowledge may not be mathematically useful because our set  $S$  is not necessarily "minimal." Using Tate's algorithm, our set  $S$  described in (10) in p.5 is already smaller than the standard choice described in Theorem 2.1 on p.4. The meaning of  $S$  being minimal could be the smallest set  $S$  of places such that for any smaller set  $S'$  contained in  $S$ ,

$$\begin{aligned} & \{ \xi \in H^1(\mathbb{Q}, E[m])_S : \text{res}_q \xi \in \text{Im } \delta_q, \forall q \in S \} \\ & \neq \{ \xi \in H^1(\mathbb{Q}, E[m])_{S'} : \text{res}_q \xi \in \text{Im } \delta_q, \forall q \in S' \}. \end{aligned} \tag{54}$$

However, from my experiments, for many cases, our set  $S$  is minimal, and for some cases,  $\emptyset$  is minimal. Up to this moment I haven't approached this problem mathematically.

### 6.1 Other Outputs

The following outputs are also computed after a run of `selmer(b, pN)`.

- (a) `VV` is a vector of length `nn` of the generators of  $A_1^*/(A_1^*)^3$ .
- (b) `WW` is a vector of length `mm` of the generators of  $A_2^*/(A_2^*)^3$ .
- (c) `WWW` is a vector of length `mmm` of the generators of  $A_{22}^*/(A_{22}^*)^3$  when  $\sqrt[3]{4b}$  is defined over  $\mathbb{Q}$ . (See the subsection 3.4 on p.12).

- (d) `Pass1` is a vector of the *exponential coordinates* for `VV` that passed the first condition of (6) in p.4. e.g., if `Pass1[2]` is `[1,2,0]` and  $y_i$  are the entries of `VV`, then the element  $y_1^1 y_2^2 y_3^0$  passed the norm condition.
- (e) `Pass2` is a vector of the *exponential coordinates* for `WW` or for `WW` and `WWW`, which passed the second and the fourth condition of (6).
- (f) `MGen` is a matrix with entries 0 and 1 whose rows represent `Pass1` and columns represents `Pass2`. e.g., `MGen[2,3]` being 1 means that an element of `A` corresponding to `Pass1[2]` and `Pass2[3]` passed the third condition of (6) and the local condition, and hence is an element of  $\text{Sel}^{(3)}(E/\mathbb{Q})$ .

## 6.2 Running `selmer3333.gp`

The gp-script `selmer3333.gp` is available at my website

<http://www.math.uga.edu/~schang/math/selmer3.html>

The script runs in the gp-calculator. The following is an example of loading `selmer3333.gp` in the gp-calculator and computing the size of  $\text{Sel}^{(3)}(E/\mathbb{Q})$  for  $E : y^2 = x^3 + 17$ :

```
\r selmer3333;
pN=70;
selmer(17,pN);
```

`pN` sets the level of precision for the local computation. When the level of precision is not sufficient for correct calculation, it displays: “padic precision low: try again.” Then simply reset the value of `pN`, and run it again.

## 6.3 Known bugs

There are two bugs are known to me.

- (a) When `pN` is large, the coefficients of the polynomials dealt in the local computation of the program are approximated by a large integers as it applies Proposition 5.1, but it results in, rather very rarely, `gp-pari` being unable to properly execute `bnfisunit`, which determines if a given element is a unit in a number field, displaying the message: *nonpositive argument in mplog*.
- (b) When the number fields are complicated as described at the end of Section 4.3 on p.15, `gp-pari` cannot find the full set of the fundamental units with the default real precision, which is 28 digits, displaying “insufficient real precision level.” By running `\p 100`, for example, it can be increased to 100 digits. For some complicated fields, it has to be increased up to 200 digits or more for `gp-pari` to find the fundamental units.

# Bibliography

- [1] Edward Schaefer. Class groups and selmer groups. *J. Number Theory*, 56, 1996.
- [2] Edward Schaefer. Computing a selmer group of a jacobian using functions on the curve. *Math. Ann.*, 310, 1998.
- [3] Edward Schaefer and Michael Stoll. How to do a  $p$ -descent on an elliptic curve. *Transactions of The American Mathematical Society*, 356, No.3, 2003.
- [4] Jean-Pierre Serre. *Local Fields*. Springer, 1979.
- [5] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.
- [6] Joseph H. Silverman. *Advanced Topics in The Arithmetic of Elliptic Curves*. Springer, 1994.