Number Fields Generated by Torsion Points on Elliptic Curves

Kevin Liu

under the direction of

Chun Hong Lo
Department of Mathematics
Massachusetts Institute of Technology

Research Science Institute
July 31, 2018

Abstract

Let E be an elliptic curve over $\mathbb{Q}$ and p be an odd prime. Assume that E does not have a p-adic point of order p, i.e. $E(\mathbb{Q}_p)[p] = 0$. For each positive integer n, define $K_n := \mathbb{Q}(E[p^n])$. Finding the class number of general number fields is a difficult problem in number theory, and we investigate the specific case of the class number of K_n. There is an injective homomorphism mapping $\mathrm{Gal}(K_n/\mathbb{Q})$ to $GL_2(\mathbb{Z}/p^n\mathbb{Z})$. We determine a lower bound on the order of the p-Sylow subgroup of the class group of K_n in terms of the Mordell-Weil rank of E in cases where this homomorphism is not necessarily surjective.

Summary

Elliptic curves are special curves in the plane, and their study has fascinated mathematicians in the last century. Number fields are sets of numbers where one can add, subtract, multiply, and divide numbers in the field. The class number is an important property of number fields. It is an interesting and difficult problem to compute the class number of general number fields. These mathematical objects can be linked by studying number fields associated with certain elliptic curves. Given an elliptic curve satisfying certain conditions, we show a constraint on the class numbers of the associated number fields.

1 Introduction

The study of elliptic curves arose from the study of Diophantine equations, or polynomial equations solved over the integers or the rational numbers. The study of cubic Diophantine equations in two variables is of particular interest, as they are among the simplest nontrivial examples of Diophantine equations. An early example is the Diophantine equation

$$y^2 - x^3 = c, \tag{1}$$

where c is a fixed integer. Equation (1) was extensively studied by Bachet in the early 1600s [7], and in 1621 he discovered a *duplication formula*, which allows one to take a rational solution to Equation (1) and obtain another rational solution.

The study of these equations was revolutionized by Descartes' development of analytic geometry in the seventeenth century. Analytic geometry gives us a natural geometric interpretation of equations such as Equation (1). In particular, we consider the set of solutions to Equation (1) as a curve in the xy-plane. Bachet's duplication formula manifests by drawing the tangent line to the curve at the point corresponding to our original rational solution, and taking the other intersection of this line and the curve.

Significant progress has been made on the solution of these Diophantine equations in the last century. In 1923, Mordell [5] showed that the group $E(\mathbb{Q})$ of rational points of an elliptic curve E with rational coefficients is finitely generated; that is, there exists a finite set of points on $E(\mathbb{Q})$ such that every point on $E(\mathbb{Q})$ can be expressed as a linear combination of points in this set. Even so, the behavior of integer and rational solutions to cubic equations is not fully understood.

Define K_n to be the number field generated by adjoining the coordinates of the p^n-torsion points $E[p^n]$, i.e. points that become the identity when multiplied by p^n, to $\mathbb{Q}$. We denote this by $K_n := \mathbb{Q}(E[p^n])$. We look at the class number of this number field, which measures how far the ring of integers is from satisfying unique factorization. For example, the Fundamental

Theorem of Arithmetic states that $\mathbb{Z}$ has unique factorization, so its field of fractions $\mathbb{Q}$ has class number 1. On the other hand,

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

so $\mathbb{Z}[\sqrt{-5}]$ does not satisfy unique factorization, and its field of fractions $\mathbb{Q}(\sqrt{-5})$ has class number 2. In general, number fields whose rings of integers do not satisfy unique factorization will have class numbers greater than 1. Due to a relative lack of techniques for computing effective bounds, class numbers are difficult to compute for general number fields, so it is useful to have a nontrivial bound on the class number of certain number fields. In 2018, Hiranouchi [2] showed a lower bound on the class number of K_n when the conditions

(**Full**) $\mathrm{Gal}(K_1/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/p\mathbb{Z})$, and

(**Tor**) $E(\mathbb{Q}_p)[p] = 0$

are satisfied. We investigate the behavior of K_n when (**Full**) does not hold, and attempt to derive a result similar to Hiranouchi's in cases where $\mathrm{Gal}(K_1/\mathbb{Q})$ is instead a proper subgroup of $GL_2(\mathbb{Z}/p\mathbb{Z})$.

The study of elliptic curves is not without applications, and has been applied to fields such as cryptography. For example, Lenstra's algorithm to factor large numbers utilizes elliptic curves and is one of the best factoring algorithms known.

In Section 2, we recall the theory of elliptic curves and define a field extension L_n of K_n, building up to the result of Hiranouchi [2]. In Section 3, we provide examples showing that Hiranouchi's result no longer holds when the condition (**Full**) is dropped. Section 4 contains bounds on the class number of K_1 when $\mathrm{Gal}(K_1/\mathbb{Q})$ contains certain subgroups of $GL_2(\mathbb{Z}/p\mathbb{Z})$. In Section 5, we show a bound on the class number of K_n for any positive integer n, assuming that $\mathrm{Gal}(K_n/\mathbb{Q})$ contains all diagonal matrices in $GL_2(\mathbb{Z}/p^n\mathbb{Z})$. Section 6 describes some avenues of future research to improve or build on the results of this paper.

2 Preliminaries

2.1 Addition and Torsion Points on Elliptic Curves

An elliptic curve over the rational numbers $\mathbb{Q}$ is a smooth plane curve that can be defined by an equation of the form

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

where the a_i are rational numbers. Examples are shown in Figure 1.

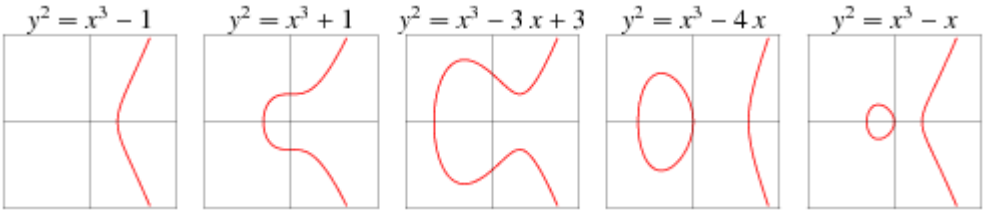

Figure 1: Various elliptic curves [8]

Consider an elliptic curve E with rational coefficients. The points of E are equipped with an addition operation, shown in Figure 2. To add points A and B on E, draw the line through A and B, and reflect the third intersection of this line with E over the x-axis. The third intersection must exist because an elliptic curve has degree 3, but it may lie in the projective plane. This gives the point $C = A + B$. This addition operation is commutative, associative, and has identity $\mathcal{O}$, the point at infinity in the vertical direction. Furthermore, any point and its image upon reflection about the x-axis are inverses.

Let K be a field, and let $E(K)$ denote the set of points on E with coordinates in K. Using Vieta's formulae, one can show that the sum of two points in $E(K)$ must also be in $E(K)$. Thus, the points of $E(K)$ form an additive group.

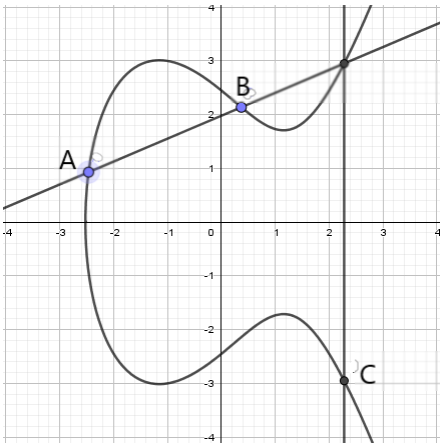

Figure 2: Adding two points on an elliptic curve

By Mordell's theorem [5], $E(\mathbb{Q})$ is finitely generated, so there exists a unique nonnegative integer r and prime powers $q_1, \ldots, q_m$ such that

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus \mathbb{Z}/q_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/q_m\mathbb{Z}.$$

We define the *rank* of E to be r.

For an odd prime p and positive integer n, let $E[p^n]$ be the set of p^n-*torsion points*, i.e. the points R, possibly with complex coordinates and including the identity $\mathcal{O}$, satisfying

$$[p^n]_E R := \underbrace{R + \cdots + R}_{p^n \text{ times}} = \mathcal{O}.$$

It is well known (Proposition 6.4 of [7]) that as additive groups,

$$E[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z}) \oplus (\mathbb{Z}/p^n\mathbb{Z}).$$

Therefore, we can identify the automorphisms of $E[p^n]$ with the group $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ of invertible 2×2 matrices with entries in $\mathbb{Z}/p^n\mathbb{Z}$.

2.2 The Fields K_n and L_n

The field K_n is defined as $\mathbb{Q}(E[p^n])$, and is a Galois extension of $\mathbb{Q}$ (Proposition 6.5(b) of [7]). In other words, every field homomorphism $\sigma : K_n \to \mathbb{C}$ that fixes $\mathbb{Q}$ has image equal to K_n. This allows us to consider $\mathrm{Gal}(K_n/\mathbb{Q})$, the group of all such homomorphisms. Then

the following theorem on the structure of this group holds ([7], Theorem 6.7).

Theorem 2.1. *There is an injective group homomorphism* $\mathrm{Gal}(K_n/\mathbb{Q}) \hookrightarrow GL_2(\mathbb{Z}/p^n\mathbb{Z})$.

Let $E(\mathbb{Q})_{\mathrm{tors}}$ be the subgroup consisting of the torsion points of $E(\mathbb{Q})$, that is, the points R such that $[m]_E R = \mathcal{O}$ for some nonzero integer m. As before, $[m]_E$ denotes the multiplication-by-m map on E. Since $E(\mathbb{Q})$ is finitely generated with rank r, it has a subgroup A such that $A \simeq \mathbb{Z}^r$ and

$$A + E(\mathbb{Q})_{\mathrm{tors}} = E(\mathbb{Q}).$$

Let $P_1, \ldots, P_r$ be generators of A. For each $1 \leq j \leq r$, let T_j be a point on $E(\mathbb{C})$ such that

$$[p^n]_E T_j = P_j.$$

We now define the field extension $L_n = K_n(T_1, \ldots, T_r)$ to be the field generated by adjoining the coordinates of $T_1, \ldots, T_r$ to K_n. An element σ of $\mathrm{Gal}(L_1/K_1)$ has an action on points of $E(L_1)$ defined by ${}^{\sigma}(x, y) := (\sigma(x), \sigma(y))$. There exists an injective homomorphism

$$\Phi_n : \mathrm{Gal}(L_n/K_n) \to E[p^n]^r$$

sending σ to $({}^{\sigma}T_1 - T_1, \ldots, {}^{\sigma}T_r - T_r)$. Thus, the degree $[L_n : K_n]$ is a power of p.

2.3 The First Cohomology Group

Consider a group G and a G-module M. Define the *1-cocycles* $Z^1(G, M)$ to be the additive group of maps $f : G \to M$ satisfying

$$f(ab) = f(a) + a \cdot f(b)$$

for all $a, b \in G$, and the *1-coboundaries* $B^1(G, M)$ to be the additive group of maps $f : G \to M$ such that for some $m \in M$,

$$f(a) = a \cdot m - m$$

for all $a \in G$. The first cohomology group $H^1(G, M)$ is the quotient $Z^1(G, M)/B^1(G, M)$.

The following result on the first cohomology group is Theorem 5.1 of [3].

Theorem 2.2. *Let G be a group and let M be a G-module. Let α be in the center of G. Then $H^1(G, M)$ is annihilated by the map $x \mapsto \alpha x - x$ on M. In particular, if this map is an automorphism of M, then $H^1(G, M) = 0$.*

In particular, letting $G = \mathrm{Gal}(K_n/\mathbb{Q})$ and $M = E[p^n]$, if $\alpha = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ is in G, then the map $x \mapsto \alpha x - x$ is the identity. This map is clearly an automorphism of M, so $H^1(G, M) = 0$.

2.4 Bounding the Class number of K_n Assuming (Full)

Suppose E is an elliptic curve with rank r satisfying (**Full**). The following theorem is Corollary 2.5 in [6].

Theorem 2.3 (Sairaiji & Yamauchi)**.** *The map $\Phi_n : \mathrm{Gal}(L_n/K_n) \to E[p^n]^r$ sending σ to $({}^{\sigma}T_1 - T_1, \ldots, {}^{\sigma}T_r - T_r)$ is an isomorphism for all positive integers n. In particular, the equation $[L_n : K_n] = p^{2nr}$ holds for all n.*

Given a number field K, a fractional ideal I of its ring of integers $\mathcal{O}_K$ is an $\mathcal{O}_K$-submodule of K, which has the form $I = \frac{1}{\alpha}J$, where J is an ideal in $\mathcal{O}_K$ and α is a nonzero element of $\mathcal{O}_K$. A principal fractional ideal is a fractional ideal that is generated by exactly one nonzero element. Let J_K denote the multiplicative group of fractional ideals of $\mathcal{O}_K$, and let P_K denote the subgroup of principal fractional ideals. Then the class group of K is defined as the quotient J_K/P_K, and the class number of K is the order of the class group.

Denote by $\#\,\mathrm{Cl}_p(K_n)$ the size of the p-Sylow subgroup of the class group of K_n. In particular, $\#\,\mathrm{Cl}_p(K_n) = p^{\kappa_n}$ is the largest power of p that divides the class number of K_n. Now let E be an elliptic curve with minimal discriminant Δ satisfying (**Full**) and (**Tor**). Let ord_p denote the p-adic valuation, and define

$$\nu_\ell := \begin{cases} \min\{\mathrm{ord}_p(\mathrm{ord}_\ell(\Delta)), n\}, \text{ if } E \text{ has split multiplicative reduction at } \ell, \\ n, \text{ if } E \text{ has additive reduction at } \ell, \text{ and } c_\ell = 3, \\ 0, \text{ otherwise,} \end{cases}$$

where c_ℓ is the Tamagawa number at ℓ. In Theorem 3.3 of [2], Hiranouchi proved the following.

Theorem 2.4 (Hiranouchi)**.** *For all $n \in \mathbb{Z}_{\geq 1}$, the exponent κ_n of $\#\,\mathrm{Cl}_p(K_n) = p^{\kappa_n}$ satisfies*

$$\kappa_n \geq 2n(r-1) - 2 \sum_{\ell \neq p,\, \ell \mid \Delta} \nu_\ell.$$

The following lemma is used in the proof of Theorem 2.4.

Lemma 2.5.

$$\#\,\mathrm{Cl}_p(K_n) \cdot p^{2n} \cdot p^{2\sum_{\ell \neq p, \ell \mid \Delta} \nu_\ell} \geq [L_n : K_n]$$

*for any elliptic curve satisfying (**Tor**).*

A direct substitution of Theorem 2.3 into Lemma 2.5 implies Theorem 2.4.

3 Examples Showing (Full) is Necessary

We now give an example in which Theorem 2.4 does not hold when (**Full**) is not satisfied. The following computations are given by SAGE. Consider the elliptic curve defined by $y^2 = x^3 - x^2 - 935133x - 397141863$, with Cremona label 50700b2, satisfying (**Tor**) but not (**Full**). It has rank 2, and letting $p = 3$ and $n = 1$,

$$2n(r-1) - 2 \sum_{\ell \neq p,\, \ell \mid \Delta} \nu_\ell = 2,$$

but the class number of K_1 is 192, so $\kappa_1 = 1$. This contradicts the bound given by Theorem 2.4.

Let

$$b = 2n(r-1) - 2\sum_{\ell \neq p,\, \ell \mid \Delta} \nu_\ell.$$

Table 1 lists some elliptic curves satisfying (**Tor**) but not (**Full**) such that $\kappa_n < b$ when $p = 3$ and $n = 1$. Therefore, Theorem 2.4 is no longer necessarily true when the condition (**Full**) is not satisfied.

Cremona label	b	κ_n
50700b2	2	1
63075n2	2	1
145200bp3	2	1
145200bp4	2	1

Table 1: Elliptic curves satisfying (**Tor**) but not the bound given in Theorem 2.4

4 The Class Number of K_n When $n = 1$

Other than the exceptional subgroups, every subgroup of $GL_2(\mathbb{Z}/p\mathbb{Z})$ is contained in one of five subgroups: Borel, split Cartan, normalizer of the split Cartan, non-split Cartan, and normalizer of the non-split Cartan [1]. The split Cartan subgroup is contained within the Borel and normalizer of the split Cartan subgroups, and the non-split Cartan subgroup is contained within the normalizer of the non-split Cartan subgroup.

4.1 The Split Cartan Subgroup

Let $C_s(p)$ denote the split Cartan subgroup of $GL_2(\mathbb{Z}/p\mathbb{Z})$, that is, the subgroup of diagonal matrices of $GL_2(\mathbb{Z}/p\mathbb{Z})$. In the case that $\mathrm{Gal}(K_1/\mathbb{Q}) \simeq C_s(p)$, the matrix $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$ is in $\mathrm{Gal}(K_1/\mathbb{Q})$. It follows from Theorem 2.2 that

$$H^1(\mathrm{Gal}(K_1/\mathbb{Q}), E[p]) = 0. \tag{2}$$

We now obtain the following bounds on the degree of the extension $[L_1 : K_1]$.

Theorem 4.1. *If* $\mathrm{Gal}(K_1/\mathbb{Q}) \simeq C_s(p)$*, we have* $p^r \leq [L_1 : K_1] \leq p^{2r}$*.*

Proof. We follow the method of the proof given by Sairaiji & Yamauchi in Theorem 2.4 of [6]. Recall that A is defined as the free subgroup of $E(\mathbb{Q})$ with rank r. For each P in A, take $T \in E(L_1)$ such that $[p]_E T = P$, and define the map $\delta_P : \mathrm{Gal}(L_1/K_1) \to E[p]$ by $\sigma \mapsto {}^{\sigma}T - T$.

We show that δ_P is trivial if and only if P is in $[p]_E A$. Clearly the reverse implication is true. Now suppose δ_P is trivial. Then T is in $E(K_1)$, so the map

$$\mathrm{Gal}(K_1/\mathbb{Q}) \to E[p] : \sigma \to {}^{\sigma}T - T$$

is an element of $H^1(\mathrm{Gal}(K_1/\mathbb{Q}), E[p])$. By Equation (2), there exists T' in $E[p]$ such that

$${}^{\sigma}T - T = {}^{\sigma}T' - T'$$

for each $\sigma \in \mathrm{Gal}(K_1/\mathbb{Q})$. Therefore, $T - T'$ is in $E(\mathbb{Q})$.

Note that

$$P = [p]_E(T - T').$$

Since $T - T' \in E(\mathbb{Q})$, we can write $T - T' = Q_1 + Q_2$, where $Q_1 \in A$ and $Q_2 \in E(\mathbb{Q})_{\mathrm{tors}}$. However,

$$[p]_E(T - T') = [p]_E Q_1 + [p]_E Q_2 \in A,$$

so $[p]_E Q_2 = 0$ and $P = [p]_E(T - T') \in [p]_E(A)$. Therefore, δ_P is trivial if and only if P is in $[p]_E(A)$, so $\ker(P \mapsto \delta_P) = [p]_E(A)$.

Consider the injective map $\delta : A/[p]_E A \hookrightarrow H^1(\mathrm{Gal}(L_1/\mathbb{Q}), E[p])$ defined by $P \mapsto \delta_P$. By Equation (2), $H^1(\mathrm{Gal}(L_1/\mathbb{Q}), E[p]) \simeq \mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p])$. In particular, the image of δ lies in $\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p])$, so

$$\#\,\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p]) \geq \#A/[p]_E A = p^r.$$

Since $E[p]$ is $\mathrm{Gal}(K_1/\mathbb{Q})$-isomorphic to $\mathbb{F}_p^2$, $E[p]^r$ is $\mathrm{Gal}(K_1/\mathbb{Q})$-isomorphic to $\mathbb{F}_p^{2r}$. $\mathbb{F}_p$ is irreducible, and $\mathbb{F}_p^{2r}$ is a semisimple $\mathrm{Gal}(K_1/\mathbb{Q})$-module, so the image of Φ_1 is $\mathrm{Gal}(K_1/\mathbb{Q})$-

isomorphic to $\mathbb{F}_p^s$ for some nonnegative integer $s \leq 2r$. Now

$$\begin{aligned}\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p]) &\simeq \mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathbb{F}_p^s, \mathbb{F}_p^2) \\ &\simeq \mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathbb{F}_p, \mathbb{F}_p^2)^s,\end{aligned}$$

where the action of $\mathrm{Gal}(K_1/\mathbb{Q}) \simeq C_s(p)$ on $\mathbb{F}_p$ is given by

$$\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \cdot x = ax.$$

Suppose $f \in \mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathbb{F}_p, \mathbb{F}_p^2)$ maps 1 to $\langle u, v\rangle$. Then for any $x, a, b \in \mathbb{F}_p$,

$$\langle axu, bxv\rangle = f\left(\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \cdot x\right) = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \cdot f(x) = \langle axu, axv\rangle,$$

so $v = 0$. Therefore, $f(x) = \langle ux, 0\rangle$ for all x. Since u can be any element of $\mathbb{F}_p$,

$$\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathbb{F}_p, \mathbb{F}_p^2)^s \simeq (\mathbb{Z}/p\mathbb{Z})^s,$$

so $s \geq r$. Since $[L_1 : K_1] = p^s$, the result follows. □

It is possible that $\mathrm{Gal}(K_1/\mathbb{Q})$ has $C_s(p)$ as a proper subgroup, for example, if $\mathrm{Gal}(K_1/\mathbb{Q})$ is isomorphic to the Borel subgroup $B(p)$ of upper triangular matrices in $GL_2(\mathbb{Z}/p\mathbb{Z})$. In this case, the above argument still holds. This is because $\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p])$ is a subgroup of $\mathrm{Hom}_{C_s(p)}(\mathrm{Gal}(L_1/K_1), E[p])$, and since

$$\begin{aligned}p^s &= \#\,\mathrm{Hom}_{C_s(p)}(\mathrm{Gal}(L_1/K_1), E[p]) \\ &\geq \#\,\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p]) \\ &\geq \#A/[p]_E A = p^r,\end{aligned}$$

we can still conclude $s \geq r$. Recall that $[L_1 : K_1] = p^s$, so the following corollary holds.

Corollary 1. *If $C_s(p)$ is a subgroup of $\mathrm{Gal}(K_1/\mathbb{Q})$, then $p^r \leq [L_1 : K_1] \leq p^{2r}$.*

The combination of Theorem 4.1 and Lemma 2.5 gives the following result, analogous to Thereom 2.4:

Theorem 4.2. *Assume (**Tor**). If $\mathrm{Gal}(K_1/\mathbb{Q})$ contains $C_s(p)$, the inequality*

$$\kappa_1 \geq r - 2 - 2 \sum_{\ell \neq p,\, \ell \mid \Delta} \nu_\ell$$

holds.

Proof. By Theorem 4.1 and Lemma 2.5,

$$\kappa_1 + 2 + 2 \sum_{\ell \neq p,\, \ell | \Delta} \nu_\ell \geq r,$$

which is what we wanted to prove. □

4.2 The Non-split Cartan Subgroup

Define the non-split Cartan subgroup $C_{ns}(p)$ of $GL_2(\mathbb{Z}/p\mathbb{Z})$ to be the subgroup consisting of matrices of the form

$$\begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix},$$

where x and y are not both zero and ε is the smallest positive integer generating $(\mathbb{Z}/p\mathbb{Z})^\times$. Assume that $C_{ns}(p)$ is a subgroup of $\mathrm{Gal}(K_1/\mathbb{Q})$. Note that $C_{ns}(p)$ contains the matrix $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, so by Theorem 2.2, Equation (2) still holds. We obtain results similar to those proved in Section 4.1 using the same methods.

Theorem 4.3. *Suppose* $\mathrm{Gal}(K_1/\mathbb{Q})$ *contains the subgroup* $C_{ns}(p)$*. Then* $p^r \leq [L_1 : K_1] \leq p^{2r}$*.*

Proof. By the same argument given in the proof of Theorem 4.1,

$$\#\,\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p]) \geq \#A/[p]_E A = p^r.$$

Suppose that $E[p]$ has a $\mathrm{Gal}(K_1/\mathbb{Q})$-submodule generated by $\langle a, b\rangle$. In order for

$$\left(\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right) \langle a, b\rangle = \langle ax + \varepsilon by, ay + bx\rangle$$

to lie in the span of $\langle a, b\rangle$, we must have

$$b(ax + \varepsilon by) = a(ay + bx) \Leftrightarrow \varepsilon b^2 = a^2,$$

assuming $y \neq 0$. Since ε generates $(\mathbb{Z}/p\mathbb{Z})^\times$, it is not a quadratic residue modulo p, so this cannot happen. Therefore, $E[p]$ is an irreducible $\mathrm{Gal}(K_1/\mathbb{Q})$-module.

We have that $E[p]^r$ is a semisimple $\mathrm{Gal}(K_1/\mathbb{Q})$-module ([4], Chapter XVIII, Lemma 12.1). Therefore, the image of Φ_1 is $\mathrm{Gal}(K_1/\mathbb{Q})$-isomorphic to $E[p]^s$ for some nonnegative integer

$s \leq r$. In particular, $[L_1 : K_1] \leq p^{2r}$. We have

$$\begin{aligned}\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p]) &\simeq \mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(E[p]^s, E[p]) \\ &\simeq \mathrm{End}_{\mathrm{Gal}(K_1/\mathbb{Q})}(E[p])^s.\end{aligned}$$

However, $\mathrm{End}_{\mathrm{Gal}(K_1/\mathbb{Q})}(E[p])$ consists of all matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ which commute with all elements of $\mathrm{Gal}(K_1/\mathbb{Q})$. Note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} = \begin{pmatrix} ax + by & \varepsilon ay + bx \\ cx + dy & \varepsilon cy + dx \end{pmatrix},$$

$$\begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ax + \varepsilon cy & \varepsilon dy + bx \\ cx + ay & by + dx \end{pmatrix},$$

and the two can only be equal for all x, y not both zero if $a = d$ and $b = \varepsilon c$. This leaves at most p^2 choices of a, b, c, d, so

$$p^r \leq \#\,\mathrm{Hom}_{\mathrm{Gal}(K_1/\mathbb{Q})}(\mathrm{Gal}(L_1/K_1), E[p]) \leq p^{2s}.$$

Therefore, $[L_1 : K_1] = p^{2s} \geq p^r$, as desired. □

Theorem 4.4. *Assume (**Tor**). If* $\mathrm{Gal}(K_1/\mathbb{Q})$ *contains* $C_{ns}(p)$*, the inequality*

$$\kappa_1 \geq r - 2 - 2 \sum_{\ell \neq p,\, \ell \mid \Delta} \nu_\ell$$

holds.

Proof. Substitute Theorem 4.3 into Lemma 2.5 and repeat the proof of Theroem 4.2. □

4.3 Examples

Let E be the elliptic curve with rank 3 and Cremona label 398325j1, and let $p = 3$. $\mathrm{Gal}(K_1/\mathbb{Q})$ is isomorphic to $B(p)$, so by Theorem 4.2, $\kappa_1 \geq 1$, so the class number of K_1 must be divisible by 3. According to SAGE, K_1 is the splitting field of the polynomial

$$x^{12}-1280x^{11}-2461247x^{10}+2234131300x^9+2914089708235x^8-1034113846347200x^7-1691228805630598535x^6$$

$$-1409277007805920818 50x^5+3327368461788880039 49965x^4+1383923141372077003540258 50x^3$$

$$+2357169453926635484033521548 3x^2+1908113469772910231763941149710x+6099817328801710561544556082928 4,$$

and has class number 5184, which is indeed divisible by 3. Thus, the bound given in Theorem 4.2 is nontrivial.

The following computations given by SAGE show that the bound given in Corollary 1 is tight. Let $p = 3$ and E be the elliptic curve of rank 1 with Cremona label 528g1. $\mathrm{Gal}(K_1/\mathbb{Q})$ is isomorphic to $B(p)$, which has $C_s(p)$ as a subgroup. The x-coordinate of T_1 is a root of the polynomial

$$x^9+54x^8+912x^7+6496x^6+81408x^5+695808x^4+2805760x^3+19046400x^2+121307136x+252444672,$$

which factors as

$$(x^3 - 2x^2 + 16x + 192)(x^6 + 56x^5 + 1008x^4 + 7424x^3 + 69376x^2 + 522240x + 1314816).$$

Therefore, $[L_1 : K_1] < 9$. However, $[L_1 : K_1]$ must be a power of p, so $[L_1 : K_1] = 3 = p^r$. This shows that the bound $[L_1 : K_1] \geq p^r$ cannot be improved without imposing further constraints.

5 Finding Bounds for all n

We obtain results analogous to Theorem 4.1 and Theorem 4.2 for any positive integer n. The proof method is similar.

Theorem 5.1. *Suppose* $\mathrm{Gal}(K_n/\mathbb{Q})$ *contains all diagonal matrices of* $GL_2(\mathbb{Z}/p^n\mathbb{Z})$. *Then* $p^{nr} \leq [L_n : K_n] \leq p^{2nr}$.

Proof. Note that

$$H^1(\mathrm{Gal}(K_n/\mathbb{Q}), E[p^n]) = 0$$

by Theorem 2.2. We repeat the argument given in the proof of Theorem 4.1, replacing L_1 and K_1 with L_n and K_n and replacing p with p^n. This gives that

$$\#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\mathrm{Gal}(L_n/K_n), E[p^n]) \geq \#A/[p^n]_E A = p^{nr}.$$

Recall that Φ_n is an injective map from $\mathrm{Gal}(L_n/K_n)$ to $E[p^n]^r \simeq (\mathbb{Z}/p^n\mathbb{Z})^{2r}$, which has

size p^{2nr}, so $[L_n : K_n] \leq p^{2nr}$ follows immediately. Also,

$$\#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\mathrm{Gal}(L_n/K_n), E[p^n]) = \#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\operatorname{Im}\Phi_n, E[p^n]).$$

A diagonal matrix $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ in $\mathrm{Gal}(K_n/\mathbb{Q})$ acts on an element $\langle x_1, y_1, \ldots, x_r, y_r\rangle$ of $E[p^n]^r$ by

$$\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \cdot \langle x_1, y_1, \ldots, x_r, y_r\rangle = \langle ax_1, by_1, \ldots, ax_r, by_r\rangle.$$

We define

$$G_x := \{\langle x_1, \ldots, x_r\rangle \mid \langle x_1, y_1, \ldots, x_r, y_r\rangle \in \operatorname{Im}\Phi_n\},$$

$$G_y := \{\langle y_1, \ldots, y_r\rangle \mid \langle x_1, y_1, \ldots, x_r, y_r\rangle \in \operatorname{Im}\Phi_n\},$$

so that G_x and G_y are subgroups of $(\mathbb{Z}/p^n\mathbb{Z})^r$ and $\operatorname{Im}\Phi_n = G_x \oplus G_y$. Since G_x is a finite abelian group, it is the direct sum of cyclic groups. However, the order of G_x is a power of p, so the order of each component cyclic group is also a power of p. Also, every element of G_x has order dividing p^n. Thus, we can write

$$G_x \simeq \mathbb{Z}/p^{f_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{f_m}\mathbb{Z}$$

for integers $1 \leq f_1, \ldots, f_m \leq n$. A homomorphism $f : G_x \to E[p^n]$ can be treated as m separate homomorphisms by considering each component cyclic group separately. Therefore,

$$\#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(G_x, E[p^n]) = \prod_{i=1}^{m} \#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\mathbb{Z}/p^{f_i}\mathbb{Z}, (\mathbb{Z}/p^n\mathbb{Z})^2).$$

Let $f \in \operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\mathbb{Z}/p^{f_i}\mathbb{Z}, (\mathbb{Z}/p^n\mathbb{Z})^2)$, and take a generator x of $\mathbb{Z}/p^{f_i}\mathbb{Z}$. If $f(x) = \langle u, v\rangle$,

$$\langle au, bv\rangle = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) f(x) = f\left(\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \cdot x\right) = f(ax) = \langle au, av\rangle$$

for all $a, b \in (\mathbb{Z}/p^n\mathbb{Z})^\times$, so $v = 0$. Also, we must have $p^{f_i}u = 0$ in $\mathbb{Z}/p^n\mathbb{Z}$. There are only p^{f_i} such u, and f is completely determined by $f(x)$, so

$$\#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\mathbb{Z}/p^{f_i}\mathbb{Z}, (\mathbb{Z}/p^n\mathbb{Z})^2) \leq p^{f_i}.$$

Therefore,

$$\#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(G_x, E[p^n]) \leq \prod_{i=1}^{m} p^{f_i} = \#G_x.$$

Similarly,

$$\#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(G_y, E[p^n]) \leq \#G_y.$$

Finally,

$$\begin{aligned}
\#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(\operatorname{Im}\Phi_n, E[p^n]) &= \#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(G_x \oplus G_y, E[p^n]) \\
&= \#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(G_x, E[p^n]) \cdot \#\operatorname{Hom}_{\mathrm{Gal}(K_n/\mathbb{Q})}(G_y, E[p^n]) \\
&\leq \#G_x \cdot \#G_y \\
&= \#\operatorname{Im}\Phi_n \\
&= [L_n : K_n],
\end{aligned}$$

so $[L_n : K_n] \geq p^{nr}$ as desired. □

From this we obtain our main result.

Theorem 5.2. *If* $\mathrm{Gal}(K_n/\mathbb{Q})$ *contains all diagonal matrices in* $GL_2(\mathbb{Z}/p^n\mathbb{Z})$ *and (**Tor**) is satisfied, then*

$$\kappa_n \geq n(r-2) - 2\sum_{\ell \neq p,\, \ell \mid \Delta} \nu_\ell.$$

Proof. From Lemma 2.5 and Theorem 5.1 we have

$$\kappa_n + 2n + 2\sum_{\ell \neq p,\, \ell \mid \Delta} \nu_\ell \geq nr.$$

The result is now immediate. □

6 Conclusion and Future Work

We discussed p^n-torsion points on elliptic curves, and the number field $K_n = \mathbb{Q}(E[p^n])$. We studied a previous result proving a lower bound on the class number of K_n. Using this method, we showed a different lower bound on the class number of K_n assuming a weaker condition than in the previous result.

There are several possible directions of future research. One such direction is to extend the work in Section 4 to other subgroups of $GL_2(\mathbb{Z}/p\mathbb{Z})$, particularly those in which Theorem 2.2 does not apply. A simple example is the subgroup of $C_s(3)$ generated by the matrix

$\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. This subgroup does not contain the matrix $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, so we cannot immediately apply Theorem 2.2.

It may also be possible to improve upon the bounds on κ_n given in Sections 4 and 5. An alternative avenue of exploration would be to consider the p-isogeny field $F := \mathbb{Q}(P + Q)$, where P and Q are generators of $E[p]$. It may be possible to derive a result analogous to Theorem 2.4 by constructing an extension of F analogous to the extension L_n of K_n and modifying Theorem 2.3 and Lemma 2.5.

7 Acknowledgments

I would first like to thank my mentor, Chun Hong Lo. He introduced me to this project and proved to be invaluable in my research. I would like to thank Prof. Andrew Sutherland, who originally suggested this project and helped provide guidance. Our head mentor, Dr. Tanya Khovanova, also provided insight into this project and its presentation. My tutor, Dr. John Rickert, gave important advice in the making of my paper and presentation. I would like to acknowledge last-week TAs David Wu and Anne Blythe Davis, who helped edit this paper and provided useful comments. I would also like to thank MIT, CEE, and RSI for giving me the opportunity to conduct this research. Lastly, I would like to recognize my sponsors, Ms. Lisa Sodeika and Ms. Alexa Margalith, who made my experience at RSI possible.

References

[1] J. Cremona, A. V. Sutherland, J. Jones, and S. Anni. Image of mod p galois representation. `http://www.lmfdb.org/knowledge/show/ec.q.galois_rep_image`, June 2018.

[2] T. Hiranouchi. Local torsion primes and the class numbers associated to an elliptic curve over $\mathbb{Q}$. arXiv:1703.08275 [math.NT].

[3] S. Lang. *Elliptic Curves Diophantine Analysis*, volume 231. Springer-Verlag Berlin Heidelberg, 1978.

[4] S. Lang. *Graduate Texts in Mathematics: Algebra*. Springer, 2002.

[5] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Cambridge Philos. Soc.*, 21:179–192, 1922-23.

[6] F. Sairaiji and T. Yamauchi. On the class numbers of the fields of the pˆn-torsion points of certain elliptic curves over Q. arXiv:1307.7691 [math.NT].

[7] J. H. Silverman and J. T. Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992.

[8] E. W. Weisstein. Elliptic curve. `http://mathworld.wolfram.com/EllipticCurve.html`.