AN INVESTIGATION ON THE ALGEBRAIC AND ANALYTIC PROPERTIES OF ELLIPTIC CURVES
URA FOR 2006-2007

HAOKUN XU

ADVISOR: DR. NICHOLAS ROGERS

Contents

1. General Introduction

The theory of elliptic curves developed out of deep questions posed by Greek mathematicians. For example, the Greeks sought to find all integer solutions to the Pythagorean equation $a^2 + b^2 = c^2$. By transforming the problem of algebra into one of geometry, one can easily find all rational points on the unit circle $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$ by taking the intersection of the circle with all lines of rational slope through the point $(-1, 0)$, which is itself on the circle. After finding all such points, we multiply back the denominators to conclude that all primitive solutions to the Pythagorean equation are of the form

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

where both m and n are integers.

Using such geometrical techniques, we can find the integer solutions of polynomial equations by studying the rational points on the curves in affine space defined by our equation. It turns out that these curves can be categorized with respect to a certain topological property called the genus. The technique described in the paragraph above provides a complete solution to the curves of genus 0. Once we find a rational point on the curve, then intersection of all lines of rational slope through that point with our curve will give us the set of all rational points on that curve. Our problem then boils down to determining the existence of a single rational solution to our polynomial equation, which the Hasse-Minkowski Theorem and Hensel's Lemma will settle in Sections 3.1 and 3.2.

As for curves of genus greater than or equal to 2, Gerd Faltings proved in 1983 a conjecture by Mordell that such curves can only have finitely many rational points. The intermediate case, and the focus of our project, are the curves of genus 1, popularly known as the elliptic curves.

What makes the problem difficult is that some elliptic curves have only finitely many rational points or none at all while some curves have infinitely many rational points without an obvious method for categorizing the points. The modern theory of elliptic curves begins with the group structure of an elliptic curve in Section 2. From there we will be able to categorize all points of finite order using results of the Nagell-Lutz Theorem and find through Mordell's Theorem that the group of rational points of every elliptic curves is finitely generated.

Ramifications from Mordell's Theorem then lead to a method in Section 3 to compute the number of generators of the points of infinite order on a curve, often called the *rank* of an elliptic curve. However, the calculation of the rank of an elliptic curve is very computationally intensive and sometimes nearly impossible to carry out. A more approachable problem is to find upper bounds on the ranks of families of quadratic

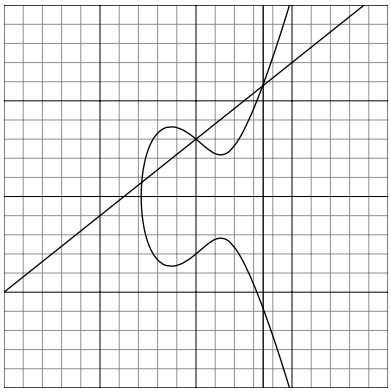
twists of an elliptic curve. Using the reciprocity theorems in Section 3.3 and Hensel's Lemma in Section 3.2 we will find explicit bounds on the ranks of the prime quadratic twists for the curve $E_1^p : py^2 = x^3 - x$ in Section 4.

2. Introduction to Elliptic Curves and the Group Law

Weierstrass showed in the late 19th century that all non-singular elliptic curves can be written in the form

$$E : y^2 = f(x), \qquad f(x) = x^3 + ax + b$$

where a, b are integers such that $f(x)$ has no double roots. The focus of this project is to study the set rational points (points with rational coordinates) on an elliptic curve, denoted $E(\mathbb{Q})$. Define the "addition" of two points P and Q to be the point $P + Q$ on the elliptic curve whose reflection across the x-axis is collinear with P and Q (see figure below).



This definition of addition is obviously commutative and can be shown to be associative, a fairly tricky proposition. Furthermore, define the "identity" as $\mathcal{O}$, the point at infinity, and the "inverse" of a point to be its reflection across the x-axis. Under those definitions, $E(\mathbb{Q})$ under our addition law becomes an abelian group.

The two most famous theorems, the Nagell-Lutz Theorem and Mordell's Theorem, in the theory of elliptic deals with points of finite order and points of infinite order, respectively.

Theorem 1 (Nagell-Lutz)**.** *Let $E : y^2 = x^3 + ax^2 + bx + c$ be a non-singular elliptic curve, where $a, b \in \mathbb{Z}$. Define*

$$D = -4a^3 + a^2b^2 + 18abc - 4b^3 - 27c^2$$

to be the discriminant of the cubic. If (r, s) is a rational point of finite order on E, then $r, s \in \mathbb{Z}$ and $s^2 | D$.

Proof. See [ST92] □

The Nagell-Lutz Theorem provides a method to find all points of finite order very quickly. The categorization of points of infinite order, however, is a much harder problem.

Theorem 2 (Mordell)**.** *Let $E : y^2 = x^3 + ax^2 + bx$ be a non-singular elliptic curve, where $a, b \in \mathbb{Z}$. The group of rational points $E(\mathbb{Q})$ is then finitely generated.*

Proof. See [ST92] □

Thus, the group of rational points on an elliptic curve is of the form

$$E(\mathbb{Q}) = E_{tors}(\mathbb{Q}) \oplus \mathbb{Z}^r,$$

where $E_{tors}(\mathbb{Q})$ is the torsion subgroup of points with finite order and r is called the rank of the elliptic curve.

3. Calculating Bounds on the Rank of an Elliptic Curve

Through a rather long analysis, of which we will only state the results, there is an elegant formula for the rank r of the elliptic curve $E : y^2 = x^3 + ax^2 + bx$. Define a second elliptic curve $\bar{E} : y^2 = x^3 - 2a + (a^2 - 4b)x$, and the map

$$\alpha : E \to \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}, \qquad \begin{array}{ll} \alpha(x, y) = x & \mod \mathbb{Q}^{*2} \\ \alpha(0, 0) = b & \mod \mathbb{Q}^{*2} \end{array}.$$

The formula for the rank r of our curve E is then

$$2^r = \frac{\#\alpha(E) \cdot \#\alpha(\bar{E})}{4}.$$

The size of the group $\alpha(E)$ is the number of quartics of the form

$$z^2 = b_1 x^4 + a x^2 y^2 + b_2 y^4,$$

where $b_1 b_2 = b$, which have a non-trivial solution $(x, y, z) \in (\mathbb{Z})^3$ where x, y, z, b_1 are all pairwise relatively prime. A similar calculation gives the size of the group $\alpha(\bar{E})$. Thus, we have a tool to calculate the rank of an elliptic curve with a rational point of order 2.

However, determining the solvability of the quartics defined above is very difficult. Furthermore, the Hasse-Minkowski Theorem does not apply because the degree of the polynomial equation is greater than 2. However, since $\mathbb{Q}$ is a subset of all of the p-adic number fields $\mathbb{Q}_p$, if a polynomial has a non-trivial solution in the rational numbers, then it must have a non-trivial solution in $\mathbb{Q}_p$ for every $p \leq \infty$. Thus, a necessary condition for a quartic above to have a non-trivial solution in $\mathbb{Q}$ is to have a solution in all the

p-adic number fields. With that in mind, we present some tools, which in conjunction with Hensel's Lemma from Section 3.2, will provide the conditions for the necessity of solvability of the quartic, and hence a bound on the rank of the elliptic curve.

3.1. **The p-adic numbers, and the Hasse-Minkowski Theorem.** To understand the context of the Hasse-Minkowski Theorem, we shall delve into the world of p-adic numbers, which are different ways of measuring distances between rational numbers. First, we must abstract our understanding of the common notion of an absolute value:

Definition 1. An absolute value on a field $\mathbb{F}$ is a function $|\cdot| : \mathbb{F} \to \mathbb{R}$ such that

- $|x| \geq 0$ with equality if and only if $x = 0$
- $|xy| = |x|\,|y|$ for all $x, y \in \mathbb{F}$
- $|x + y| \leq |x| + |y|$ for all $x, y \in \mathbb{F}$

If the absolute value satisfies the further restriction that $|x + y| \leq \max\{|x|, |y|\}$, then we call $|\cdot|$ *non-archimedean*. Otherwise, the absolute value is called *archimedean*.

Clearly, the usual absolute value on $\mathbb{R}$

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

is an example of an absolute value. We also have the trivial absolute value $|x|_t = 1$ if $x \neq 0$ and $|0|_t = 0$. There are more absolute values than meets the eye:

Definition 2. Let p be a prime number. Define the p-adic absolute value $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ such that $|x|_p = p^{-\operatorname{ord}_p(x)}$, where $\operatorname{ord}_p(x)$ is the unique natural number such that $x = p^{\operatorname{ord}_p(x)} \cdot \frac{a}{b}$ such that $p \nmid ab$ and $\gcd(a, b) = 1$. Denote the usual absolute value on $\mathbb{R}$ to be $|\cdot|_\infty$.

Thus, a rational number is "small" is the p-adic sense if the numerator of its reduced fraction representation is divisible by a large power of p. Thus, 2^{32} is tiny in the 2-adic absolute value as $|2^{32}|_2 = 2^{-32} \approx 2.3 \times 10^{-10}$, while $2^{32} + 1$ has 2-adic absolute value 1. Straightforward calculations will realize that the p-adic absolute values are indeed genuine absolute values as defined above. Moreover, it follows from factorization and the distributive law that for all $x, y \in \mathbb{Q}$

$$\begin{aligned} \operatorname{ord}_p(xy) &= \operatorname{ord}_p(x) + \operatorname{ord}_p(y), \\ \operatorname{ord}_p(x + y) &\geq \min\{\operatorname{ord}_p(x), \operatorname{ord}_p(y)\}. \end{aligned}$$

We also define by convention that $\text{ord}_p(0) = \infty$. The p-adic absolute values also define a metric $d_p : \mathbb{Q} \times \mathbb{Q} \to \mathbb{R}$, where $d_p(x, y) = |x - y|_p$. It turns out that such absolute values described above are all possible absolute values for the field $\mathbb{Q}$, described by the following theorem:

Theorem 3 (Ostrowski)**.** *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to some absolute value $|\ |_p$, where p is a prime number or $p = \infty$; that is, for every non-trivial absolute value on $\mathbb{Q}$ there is a unique absolute value $|\cdot|_p$, where p is a prime number or $p = \infty$, such that every set that is open with respect to the induced metric topology of one is also open with respect to the other.*

Proof. See [Gou97] □

Just as in the case of the usual metric, the rational numbers are not complete with respect to any other metric defined by $|\cdot|_p$. In other words, we can find many Cauchy sequences which do not converge to an element of $\mathbb{Q}$.

Lemma 4. A sequence $\{\alpha_n\}$ in a field is a Cauchy sequence with respect to a non-archimedean absolute value if and only if $\lim_{n\to\infty} |\alpha_{n+1} - \alpha_n| = 0$.

The completion of $\mathbb{Q}$ with respect to the usual metric is he real numbers $\mathbb{R}$. We mimic such a completion with respect to the other absolute values as well.

Theorem 5. *For each prime p, there is a field $\mathbb{Q}_p$ such that $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is dense and $\mathbb{Q}_p$ is complete with respect to the absolute value $|\cdot|_p$. Furthermore, the field $\mathbb{Q}_p$ satisfying the above conditions is unique up to an isomorphism preserving the absolute value, and thus we call $\mathbb{Q}_p$ the field of p-adic numbers.*

Proof. See [Gou97] □

Now we are ready to state the Hasse-Minkowski Theorem in its full glory.

Theorem 6 (Hasse-Minkowski)**.** *Let $f(x_1, \ldots, x_n) \in \mathbb{Q}[x_1, \ldots, x_n]$ be a homogeneous polynomial of degree two (a quadratic form). The equation $f(x_1, \ldots, x_n) = 0$ has nontrivial solutions (i.e., a solution other than $x_1 = \cdots = x_n = 0$) in $\mathbb{Q}$ if and only if the equation has nontrivial solutions in $\mathbb{Q}_p$ for all $p \leq \infty$.*

Proof. See [Ser73]. □

3.2. **Hensel's Lemma.** It turns out that determining solvability of a homogeneous polynomial equation in $\mathbb{Q}_p$ is very straightforward. First, we decompose a polynomial using Taylor's formula:

Lemma 7 (Taylor's Theorem for Polynomials). If $f(x) \in \mathbb{F}[x]$, where $\mathbb{F}$ is a field of characteristic 0, then

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{2!}f''(x) + \frac{h^3}{3!}f'''(x) + \cdots + \frac{h^d}{d!}f^{(d)}(x)$$

for all $x, h \in \mathbb{F}$ and $d = \deg f$.

Since scaling of a solution vector to a homogeneous polynomial equation gives another solution, it suffices to look for solutions in the following ring:

Definition 3. Define $\mathbb{Z}_p = \{x \in \mathbb{Q}_p \mid \mathrm{ord}_p(x) \geq 0\}$ to be the ring of p-adic integers.

The following famous theorem provides a method to find solutions in $\mathbb{Z}_p$:

Proposition 8 (Weak Hensel's Lemma). Let $f(x) \in \mathbb{Z}_p[x]$. If there exists an element $\alpha_1 \in \mathbb{Z}_p$ such that $f(\alpha_1) \equiv 0 \mod p\mathbb{Z}_p$ and $f'(\alpha_1) \not\equiv 0 \mod p\mathbb{Z}_p$, where f' denotes the formal derivative of f, then there exists $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_1 \mod p\mathbb{Z}_p$.

Proof. We will inductively construct a sequence whose limit is our desired solution. Let α_1 be the first element of our sequence. Suppose the n-th element $\alpha_n \in \mathbb{Z}_p$ of our sequence satisfies $f(\alpha_n) \equiv 0 \mod p^n\mathbb{Z}_p$, $f'(\alpha_n) \not\equiv 0 \mod p\mathbb{Z}_p$, and $\alpha_n \equiv \alpha_1$, then we will construct the next element α_{n+1}.

We have $f'(\alpha_n) \neq 0 \mod p\mathbb{Z}_p \implies (f'(\alpha_n))^{-1} \in \mathbb{Z}_p, \mathrm{ord}_p\left((f'(\alpha_n))^{-1}\right) = 0$. Let

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)},$$

and we have

$$\begin{aligned} f(\alpha_{n+1}) &= f(\alpha_n) - \frac{f(\alpha_n)}{f'(\alpha_n)}f'(\alpha_n) + (f(\alpha_n))^2 g(x), \\ &= (f(\alpha_n))^2 g(x), \end{aligned}$$

by Lemma 7 above, where $g(x) \in \mathbb{Z}_p[x]$. The hypothesis $f(\alpha_n) \equiv 0 \mod p^n\mathbb{Z}_p$ then gives us $f(\alpha_{n+1}) \equiv 0 \mod p^{n+1}\mathbb{Z}_p$.

Also, $\mathrm{ord}_p(f(\alpha_n)) \geq 1 \implies \alpha_{n+1} \equiv \alpha_1 \mod p\mathbb{Z}_p \implies f'(\alpha_{n+1}) \equiv f'(\alpha_1) \not\equiv 0 \mod p\mathbb{Z}_p$. Iterating this process with the construction $\alpha_{n+1} = \alpha_n - f(\alpha_n)\big(f'(\alpha_n)\big)^{-1}$ yields a sequence $\{\alpha_k\}$ where $f(\alpha_k) \equiv 0 \mod p^k\mathbb{Z}_p$ and $\alpha_k \equiv \alpha_1 \mod pZ_p$ for all k. Since $|\alpha_{n+1} - \alpha_n|_p = p^{-n}$, the sequence is Cauchy by Lemma 4 and hence defines the root $\alpha = \lim_{k\to\infty} \alpha_k$ of f with the desired properties. □

However, there are many cases where we cannot apply the Weak Hensel's Lemma. The most famous case is the polynomial $p(x) = x^2 - 17$, which we will see later to have a root in $\mathbb{Q}_2$. Even though $x \equiv 1 \mod 2\mathbb{Z}_2$

is the only root of $p(x)$, we cannot apply Weak Hensel's Lemma because $p'(1) \equiv 0 \mod 2\mathbb{Z}_2$. The following proposition takes care of the blemish.

Proposition 9 (Strong Hensel's Lemma). Let $f(x) \in \mathbb{Z}_p[x]$. If there exists an element $\alpha_1 \in \mathbb{Z}_p$ such that $n = ord_p\Big(f(\alpha_1)\Big) > 2\,\mathrm{ord}_p\left(f'(\alpha_1)\right) = 2k$, where f' denotes the formal derivative of f, then there exists $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_1 \mod p^{n-k}\mathbb{Z}_p$.

Proof. We have $\mathrm{ord}_p\left(f(\alpha_1)\big(f'(\alpha_1)\big)^{-1}\right) = n - k > 0 \implies f(\alpha_1)\big(f'(\alpha_1)\big)^{-1} \in \mathbb{Z}_p$. Thus, let

$$\alpha_2 = \alpha_1 - f(\alpha_1)\big(f'(\alpha_1)\big)^{-1}.$$

By similar calculations above we have $f(\alpha_2) = \left(\dfrac{f(\alpha_1)}{f'(\alpha_1)}\right)^2 g(x)$, where $g(x) \in \mathbb{Z}_p[x]$. Therefore, $\mathrm{ord}_p(f(\alpha_2)) \geq 2\,\mathrm{ord}_p(f(\alpha_1)) - 2\,\mathrm{ord}_p\left(\big(f'(\alpha_1)\big)^{-1}\right) = 2n - 2k = n + (n-2k) > n \implies f(\alpha_2) \equiv 0 \mod p^{n+1}\mathbb{Z}_p$.

Moreover, the inequality $\mathrm{ord}_p\left(f(\alpha_1)\big(f'(\alpha_1)\big)^{-1}\right) = n - k > k$ gives us two vital pieces of information. First, we have $\alpha_2 \equiv \alpha_1 \mod p^{k+1}\mathbb{Z}_p \implies 0 \not\equiv f'(\alpha_1) \equiv f'(\alpha_2) \mod p^{k+1}\mathbb{Z}_p$ because $\mathrm{ord}_p\left(f'(\alpha_1)\right) = k$. Dropping down one order of p gives us $\alpha_2 \equiv \alpha_1 \mod p^k\mathbb{Z}_p \implies 0 \equiv f'(\alpha_1) \equiv f'(\alpha_2) \mod p^k\mathbb{Z}_p$. Hence $\mathrm{ord}_p\left(f'(\alpha_2)\right) = k \implies \mathrm{ord}_p\left(f(\alpha_2)\right) = n + 1 > 2k = 2\,\mathrm{ord}_p\left(f'(\alpha_2)\right)$. Iterating this process with the construction $\alpha_{n+1} = \alpha_n - f(\alpha_n)\big(f'(\alpha_n)\big)^{-1}$ yields the root $\alpha = \lim\limits_{i\to\infty} \alpha_i$ of f with the desired properties. □

Thus, a general method for finding a solution in $\mathbb{Q}_p$ for polynomials of any number of variables is to first find a solution $\mod p$. We then lift with respect to the partial derivative of one variable.

3.3. **Quadratic Reciprocity.**

Definition 4 (Legendre Symbol). For a given odd prime p, define the legendre symbol $\left(\dfrac{a}{p}\right) = 1$ if there exists an element $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 \equiv a \mod p$ and define $\left(\dfrac{a}{p}\right) = 0$ if $p \mid a$. Otherwise, define $\left(\dfrac{a}{p}\right) = -1$.

Proposition 10. For a given odd prime p, the following results hold:

(1) (Euler's Criterion) $\left(\dfrac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.
(2) $\left(\dfrac{ab}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.
(3) $\left(\dfrac{-1}{p}\right) = 1$ if and only if $p \equiv 1 \mod 4$.
(4) $\left(\dfrac{2}{p}\right) = 1$ if and only if $p \equiv \pm 1 \mod 8$.
(5) -1 is a fourth power mod p if and only if $p \equiv 1 \mod 8$.

Proof. All results are trivially true when $p \mid a$. As for the non-trivial cases:

(1) Since $a^{p-1} \equiv 1 \mod p$, we can rewrite the equivalence as $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \mod p$, which then implies $a^{\frac{p-1}{2}} - 1 \equiv 0 \mod p$ or $a^{\frac{p-1}{2}} + 1 \equiv 0 \mod p$. The $\frac{p-1}{2}$ quadratic residues $\mod p$ satisfy the former equivalence $a^{\frac{p-1}{2}} - 1 \equiv 0 \mod p$ and thus an argument upon the degree of the polynomial equivalence $(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \mod p$ shows that the non-residues must satisfy the latter equivalence $a^{\frac{p-1}{2}} + 1 \equiv 0 \mod p$. Our result then follows.

(2) By the result proven above,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \mod p,$$

from which our result follows.

(3) The backwards implication follows again from the result in (1). As for the forwards implication, if $\left(\frac{-1}{p}\right) = 1$, then there is some x such that $x^2 \equiv -1 \mod p$, which implies that the multiplicative order of x is 4. Since $x^{p-1} \equiv 1 \mod p$, it follows that $4 \mid p-1$ and thus $p \equiv 1 \mod 4$.

(4) See [Apo76].

(5) For the forward implication, if -1 is a fourth power mod p, then there is some x such that $x^4 \equiv -1 \mod p \implies x^8 \equiv 1 \mod p$. Since $x^{p-1} \equiv 1 \mod p$, it follows that $8 \mid (p-1) \implies p \equiv 1 \mod 8$. As for the backwards direction, by hypothesis there is some $k \in \mathbb{N}$ such that $p = 8k+1$. Since we also have $p \equiv 1 \mod 4$, it follows by the result in (3) that there is some a such that $a^2 \equiv -1 \mod p$. By the result in (1),

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv a^{\frac{8k}{2}} \equiv a^{4k} \equiv (-1)^{2k} \equiv 1^k \equiv 1 \mod p,$$

and thus a is a perfect square mod p, from which our result follows.

□

Theorem 11 (Quadratic Recipocity)**.** $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$

Proof. See [NZM91]. □

4. Bounds on the rank of $E^p : py^2 = x^3 - x$

Here we will consider the family of quadratic twists of the congruent number elliptic curve $E : y^2 = x^3 - x$. A quadratic twist of this curve is a curve whose points satisfy the equation

$$E^n : ny^2 = x^3 - x$$

Under the mapping

$$y \mapsto \frac{y}{n^2}, \quad x \mapsto \frac{x}{n},$$

we construct an isomorphic curve to our original quadratic twist.

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

Similarly, we find that the secondary curve outlined in Section 3 is of the form $\overline{E^n} : y^2 = x^3 + 4n^2 x$. For this section, we will consider the case when n is a positive prime number.

The nontrivial quartics associated with $\alpha(E^p)$ in our search are

$$\begin{aligned} a^2 &= b^4 - p^2 c^4, \\ a^2 &= -b^4 + p^2 c^4, \\ a^2 &= pb^4 - pc^4, \\ a^2 &= -pb^4 + pc^4. \end{aligned}$$

It is a theorem that all four quartics have non-trivial solutions in $\mathbb{Q}$ because each quartic corresponds to a rational point on the elliptic curve.

The nontrivial quartics associated with $\alpha(\overline{E^p})$ in our search are

$$(1) \qquad a^2 = b^4 + 4p^2 c^4,$$

$$(2) \qquad a^2 = 2b^4 + 2p^2 c^4,$$

$$(3) \qquad a^2 = pb^4 + 4pc^4,$$

$$(4) \qquad a^2 = 2pb^4 + 2pc^4.$$

$$(5) \qquad a^2 = -b^4 - 4p^2 c^4,$$

$$(6) \qquad a^2 = -2b^4 - 2p^2 c^4,$$

$$(7) \qquad a^2 = -pb^4 - 4pc^4,$$

$$(8) \qquad a^2 = -2pb^4 - 2pc^4.$$

However, it is obvious that the latter four quartics do not have a non-trivial solution in the rational numbers because they do not have a non-trivial solution in the real numbers. Thus, we will only focus on the former four quartics. It is a theorem that we only need check for non-trivial solutions of the quartics in $\mathbb{R}, \mathbb{Q}_p$ and $\mathbb{Q}_2$.

By multiplying each quartic equation by $\max(|a^2|_p, |b^4|_p, |c^4|_p)$, where $|x|_p = p^{-\operatorname{ord}_p(x)}$, we can certainly force each of a, b, c to be in $\mathbb{Z}_p$ (i.e., $\operatorname{ord}_p(a), \operatorname{ord}_p(b), \operatorname{ord}_p(c) \geq 0$) and at least one of a, b, c to be in $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ (i.e., $\min\Big(\operatorname{ord}_p(a), \operatorname{ord}_p(b), \operatorname{ord}_p(c)\Big) = 0$). The analysis of the solvability of the quartics begins with figuring out the possible values for $\operatorname{ord}_p(a)$. Let us study these quartics in $\mathbb{Q}_p$ first.

4.1. **Existence of Non-Trivial Solutions in $\mathbb{Q}_p$.**

(1) $a^2 = b^4 + 4p^2c^4$. This quartic corresponds to the point $(2p, 0)$ on E^p, which means the quartic is solvable in $\mathbb{Q}$ hence solvable in $\mathbb{Q}_p$ for all p.

(2) $a^2 = 2b^4 + 2p^2c^4$. We know $\operatorname{ord}_p(a) \geq 0$. If $\operatorname{ord}_p(a) \geq 1$, then $\operatorname{ord}_p(b) \geq 1$. However, if $\operatorname{ord}_p(a) \geq 2$, then

$$\begin{aligned} \operatorname{ord}_p(2p^2c^4) &= \operatorname{ord}_p(a^2 - 2b^4) \geq \min\Big(\operatorname{ord}_p(a^2), \operatorname{ord}_p(2b^4)\Big) \geq 4 \implies \\ 4\operatorname{ord}_p(c^4) &\geq 2 \implies \operatorname{ord}_p(c) \geq 1, \end{aligned}$$

which contradicts the condition $\min\Big(\operatorname{ord}_p(a), \operatorname{ord}_p(b), \operatorname{ord}_p(c)\Big) = 0$. Thus we can only have $\operatorname{ord}_p(a) = 0, 1$. Now we consider more cases:

- $\operatorname{ord}_p(a) = 0 \implies 0 \not\equiv a^2 \equiv 2b^4 \mod p \implies b^4 \not\equiv 0 \mod p \implies \left(\frac{a}{b^2}\right)^2 \equiv 2 \mod p$, which is solvable only when $p \equiv \pm 1 \mod 8$. These conditions are sufficient because one set of solutions is $a \equiv \sqrt{2} \mod p$ and $b \equiv 1 \mod p$. Thus, the quartic has a nontrivial solution in $\mathbb{Q}_p$ if and only if $p \equiv \pm 1 \mod 8$.
- $\operatorname{ord}_p(a) = 1 \implies a = pw, \operatorname{ord}_p(w) = 1, \operatorname{ord}_p(b) = 1 \implies w^2 = 2\frac{b^4}{p^2} + 2c^4 \implies 0 \not\equiv w^2 \equiv 2c^4 \mod p \implies c^4 \not\equiv 0 \mod p \implies \left(\frac{w}{c^2}\right)^2 \equiv 2 \mod p$, which is solvable only when $p \equiv \pm 1 \mod 8$. These conditions are sufficient because one set of solutions is $w \equiv \sqrt{2} \mod p$ and $c \equiv 1 \mod p$. Thus, the quartic has a nontrivial solution in $\mathbb{Q}_p$ if and only if $p \equiv \pm 1 \mod 8$.

(3) $a^2 = pb^4 + 4pc^4$. It is clear that $\operatorname{ord}_p(a) > 0$ and thus $a = pw, \operatorname{ord}_p(w) \geq 0$. We now reduce our equation to $pw^2 = b^4 + 4c^4$. Now,

$$\operatorname{ord}_p(b) > 0 \implies 0 \equiv 4c^4 \mod p \implies \operatorname{ord}_p(c) > 0,$$

which contradicts the condition $\min\Big(\operatorname{ord}_p(a), \operatorname{ord}_p(b), \operatorname{ord}_p(c)\Big) = 0$. Thus, $\operatorname{ord}_p(b) = 0$, and $\operatorname{ord}_p(c) = 0$ by a similar argument. We can now reduce our equation mod p to get $0 \equiv b^4 + 4c^4 \mod p \implies \left(\frac{b}{c}\right)^4 \equiv -4 = -1(2^2) \mod p \implies \left(\frac{b}{c}\right)^2 \equiv 2\sqrt{-1} \mod p$. Note that we must have $\left(\frac{-1}{p}\right) = 1$ and thus $p \equiv 1 \mod 4$. We now have two cases:

- $\left(\frac{\sqrt{-1}}{p}\right) = \left(\frac{2}{p}\right) = 1$. The former condition gives us $p \equiv 1 \mod 8$ while the latter condition gives us $p \equiv \pm 1 \mod 8$. Thus, the necessary and sufficient conditions for this case to be solvable in $\mathbb{Q}_p$ is $p \equiv 1 \mod 8$ because we can take $c = 1, b = (-1)^{1/4}\sqrt{2}$.
- $\left(\frac{\sqrt{-1}}{p}\right) = \left(\frac{2}{p}\right) = -1$. The latter condition gives us $p \equiv \pm 3 \mod 8$, which combines with the condition $p \equiv 1 \mod 4$ gives us that $p \equiv 5 \mod 8$. Thus, the necessary and sufficient conditions for this case to be solvable in $\mathbb{Q}_p$ is $p \equiv 5 \mod 8$ because we can take $c = 1, b = \sqrt{2\sqrt{-1}}$.

Therefore, we have that the quartic has a nontrivial solution in $\mathbb{Q}_p$ if and only if $p \equiv 1 \mod 4$.

(4) $a^2 = 2pb^4 + 2pc^4$. It is clear that $\text{ord}_p(a) > 0$ and thus $a = pw, \text{ord}_p(w) \geq 0$. We now reduce our equation to $pw^2 = 2b^4 + 2c^4$. Now,

$$\text{ord}_p(b) > 0 \implies 0 \equiv 2c^4 \mod p \implies \text{ord}_p(c) > 0,$$

which contradicts the condition $\min\Big(\text{ord}_p(a), \text{ord}_p(b), \text{ord}_p(c)\Big) = 0$. Thus, $\text{ord}_p(b) = 0$, and $\text{ord}_p(c) = 0$ by a similar argument. Thus, $\text{ord}_p(b) = 0$, and $\text{ord}_p(c) = 0$ by a similar argument. We can now reduce our equation mod p to get $0 \equiv 2b^4 + 2c^4 \mod p \implies \left(\frac{b}{c}\right)^4 \equiv -1 \mod p$. Thus, the necessary and sufficient conditions for this case to have a nontrivial solution in $\mathbb{Q}_p$ is $p \equiv 1 \mod 8$ because we can take $b = (-1)^{1/4}, c = 1$.

4.2. **Existence of Non-Trivial Solutions in $\mathbb{Q}_2$.** Now that we have necessary and sufficient conditions for each of the quartics to be solvable in $\mathbb{Q}_p$, we impose those conditions upon our search for further conditions for these quartics to be solvable in $\mathbb{Q}_2$. Let's begin:

(1) $a^2 = b^4 + 4p^2c^4$. This quartic corresponds to the point $(2p, 0)$ on E^p, which means the quartic is solvable in $\mathbb{Q}$ hence solvable in $\mathbb{Q}_p$ for all p.

(2) $a^2 = 2b^4 + 2p^2c^4$. It is clear that $\text{ord}_2(a) \geq 0$. Now,

$$\begin{aligned} \text{ord}_2(a) \geq 2 \quad &\implies \quad 2b^4 + 2p^2c^4 \equiv 0 \mod 16 \implies b^4 + p^2c^4 \equiv 0 \mod 8, \\ &\implies \quad b^4 + c^4 \equiv 0 \mod 8 \implies b \equiv c \equiv 0 \mod 2, \end{aligned}$$

which contradicts the condition $\min(\text{ord}_2(b), \text{ord}_2(c)) = 0$. Thus, we must have $\text{ord}_2(a) = 1 \implies a = 2w, \text{ord}_2(w) = 0 \implies 2w^2 = b^4 + p^2c^4$. Also, note that $\text{ord}(b) > 0 \implies \text{ord}(c) > 0 \implies \text{ord}(w) > 0$, which is a contradiction. Thus $\text{ord}(b) = 0$ and $\text{ord}(c) = 0$ by a similar argument. We already have from our analysis in $\mathbb{Q}_p$ the necessary conditions $p \equiv \pm 1 \mod 8$. For sufficiency, note that the triplet $(w, b, c) = (1, 1, 1)$ solves the equation when $p \equiv 1, 15, 17, 31 \mod 32$ and $(w, b, c) = (3, 1, 1)$ solves the equation when $p \equiv 7, 9, 23, 25 \mod 32$. Now we apply the Strong Hensel's Lemma. For

the former case, consider $F(b) = b^4 + p^2 - 2 \implies F'(b) = 4b^3$. We have $5 = \text{ord}_2(F(1)) > 2\,\text{ord}_2(F'(1)) = 4$, and thus we have a solution in $\mathbb{Q}_2$. The same argument works in the latter case as well. Thus, the quartic has a non-trivial solution if and only if$p \equiv \pm 1 \mod 8$.

(3) $a^2 = pb^4 + 4pc^4$. We inherit the necessary condition $p \equiv 1 \mod 4$ from our analysis of this quartic in $\mathbb{Q}_p$. To show sufficiency, we must look for solutions modulo 32 in order to apply the Strong Hensel's Lemma. The array of solutions

$p \mod 32$	(a, b, c)
1	$(1, 1, 2)$ or $(1, 1, 0)$
5	$(5, 1, 1)$
9	$(3, 1, 2)$ or $(3, 1, 0)$
13	$(1, 1, 1)$
17	$(7, 1, 2)$ or $(7, 1, 0)$
21	$(3, 1, 1)$
25	$(5, 1, 2)$ or $(5, 1, 0)$
29	$(7, 1, 1)$

shows that the quartic is always solvable given our necessary condition. Thus, we have that the quartic is solvable in $\mathbb{Q}_2$ if and only if $p \equiv 1 \mod 4$.

(4) $a^2 = 2pb^4 + 2pc^4$. We inherit the necessary condition $p \equiv 1 \mod 8$ from our analysis of this quartic in $\mathbb{Q}_p$. To show sufficiency, note that $(a, b, c) = (2, 1, 1)$ solves the quartic modulo 32 and hence Strong Hensel's Lemma shows that the quartic is solvable in $\mathbb{Q}_2$.

Now we can tabulate our results

$p \mod 8$	Solvable Quartics in $\mathbb{Q}_p$	Solvable Quartics in $\mathbb{Q}_2$	Rank Bound
1	1,2,3,4	1,2,3,4	2
3	1	1	0
5	1,3	1,3	1
7	1,2	1,2	1

5. Bounds on the rank of $E^p : py^2 = x^3 - 7x - 6$

First we will use to the mapping $x \mapsto x+3$ to study an isomorphic elliptic curve $E_1^p : y^2 = x^3 + 9px^2 + 20p^2x$. To find bounds on the rank of our curve $E : y^2 = x^3 + \alpha x^2 + \beta x$, we will utilize a corollary to the Mordell-Weil Theorem

$$2^r = \frac{\#\phi(E) \cdot \#\bar{\phi}(\bar{E})}{4},$$

where r is the rank of our ellitipc curve and $\#\phi(E)$ denote the number of quartics of the form

$$a^2 = \alpha_1 b^4 + \beta a^2 b^2 + \alpha_2 c^4,$$

which have non-trivial primitive solutions $a, b, c \in \mathbb{Q}$ and $\alpha_1 \alpha_2 = \alpha$. Therefore, $\bar{E}_1^p : y^2 = x^3 - 18px^2 + p^2 x$ gives us four quartics to reckon for,

$$\begin{aligned} a^2 &= b^4 - 18pb^2c^2 + p^2c^4, \\ a^2 &= pb^4 - 18pb^2c^2 + pc^4, \\ a^2 &= -b^4 - 18pb^2c^2 - p^2c^4, \\ a^2 &= -pb^4 - 18pb^2c^2 - pc^4, \end{aligned}$$

The latter two quartics have no non-trivial in $\mathbb{R}$ and hence cannot have any non-trivial solutions in $\mathbb{Q}$ while the the first quartic always have a non-trivial solution in $\mathbb{Q}$ because it corresponds to $\phi(\mathcal{O}) \equiv \phi(0,0) \mod \mathbb{Q}^{*2}$, both of which are in $\phi(E)$. Therefore, the size of $\phi(E) = 1$ (resp. 2) depending on the solvability (resp. insolvability) of the second quartic, which we will analyze as quartic (4) below.

As for $\bar{\phi}(\bar{E})$, we must take a different approach. Since it is very difficult to determine solvabilty in $\mathbb{Q}$ in general, we will instead give necessary and sufficient conditions for each quartic to be solvable in $\mathbb{Q}_p$ for all $p \leq \infty$. To make our endeavor more tractable, we make use of the group structure on the quartics. Let $d_1, d_2, d_3 \in \mathbb{Q}$ such that $d_1 d_2 \equiv d_3 \mod \mathbb{Q}^{*2}$, and let each p_{d_i} correspond to the quartic $a^2 = d_i b^4 + \beta a^2 b^2 + \frac{\alpha}{d_i} c^4$. Since $d_i \in \phi(E) \iff p_{d_i}$ has a nontrivial primitive solution in $\mathbb{Q}$, we then get $d_1, d_2 \in \phi(E) \implies d_3 \in \phi(E) \implies p_{d_3}$ has a nontrivial primitive solution in $\mathbb{Q}$. Recall that

$$\begin{aligned} \phi(\mathcal{O}) &\equiv 1 \mod \mathbb{Q}^{*2}, \\ \phi(0,0) &\equiv \beta \mod \mathbb{Q}^{*2}, \\ \phi(x,y) &\equiv x \mod \mathbb{Q}^{*2}. \end{aligned}$$

Thus, we have the mappings

$$\begin{aligned} \phi(\mathcal{O}) &\equiv 1 \mod \mathbb{Q}^{*2}, \\ \phi(0,0) &\equiv \beta \equiv 5 \mod \mathbb{Q}^{*2}, \\ \phi(-4,0) &\equiv -4 \equiv -1 \mod \mathbb{Q}^{*2}, \\ \phi(-5,0) &\equiv -5 \mod \mathbb{Q}^{*2}, \end{aligned}$$

which means that the quartics

$$\begin{aligned} a^2 &= b^4 + 9pb^2c^2 + 20p^2c^4, \\ a^2 &= 5b^4 + 9pb^2c^2 + 4p^2c^4, \\ a^2 &= -b^4 + 9pb^2c^2 + 20p^2c^4, \\ a^2 &= -5b^4 + 9pb^2c^2 + 4p^2c^4, \end{aligned}$$

have non-trivial global solutions in $\mathbb{Q}$. By the group structure on $\phi(E)$, the following chains of quartics have equivalent solvability conditions in $\mathbb{Q}$ (and hence $\mathbb{Q}_p$ for all $p \leq \infty$)

$$\begin{aligned} a^2 = 2b^4 + 9pb^2c^2 + 10p^2c^4 \quad &\iff \quad a^2 = 10b^4 + 9pb^2c^2 + 2p^2c^4, \\ &\iff \quad a^2 = -2b^4 + 9pb^2c^2 + 10p^2c^4, \\ &\iff \quad a^2 = -10b^4 + 9pb^2c^2 + 2p^2c^4, \end{aligned}$$

and

$$\begin{aligned} a^2 = pb^4 + 9pb^2c^2 + 20pc^4 \quad &\iff \quad a^2 = 5pb^4 + 9pb^2c^2 + 4pc^4, \\ &\iff \quad a^2 = -pb^4 + 9pb^2c^2 + 20pc^4, \\ &\iff \quad a^2 = -5pb^4 + 9pb^2c^2 + 4pc^4, \end{aligned}$$

and

$$\begin{aligned} a^2 = 2pb^4 + 9pb^2c^2 + 10pc^4 \quad &\iff \quad a^2 = 10pb^4 + 9pb^2c^2 + 2pc^4, \\ &\iff \quad a^2 = -2b^4 + 9pb^2c^2 + 10p^2c^4, \\ &\iff \quad a^2 = -10pb^4 + 9pb^2c^2 + 2pc^4. \end{aligned}$$

Therefore, we will only determine solvability conditions for the quartics

$$a^2 = 2b^4 + 9pb^2c^2 + 10p^2c^4, \tag{9}$$

$$a^2 = pb^4 + 9pb^2c^2 + 20pc^4, \tag{10}$$

$$a^2 = 2pb^4 + 9pb^2c^2 + 10pc^4. \tag{11}$$

5.1. **Existence of Non-Trivial solutions in $\mathbb{Q}_p$.** Note: By multiplying by appropriate powers of p, we can assume that all of a, b, c are in $\mathbb{Z}_p$ with at least one of a, b, c not in $p\mathbb{Z}_p$

(1) $a^2 = 2b^4 + 9pb^2c^2 + 10p^2c^4$. We will work on the possible values of $\text{ord}_p(a)$. If $\text{ord}_p(a) \geq 2$, then we have $p \mid a^2 - 9pb^2c^2 - 10p^2c^4 = b \implies \text{ord}_p(b) \geq 1$ and thus $p^3 \mid a^2 - 2b^4 - 9pb^2c^2 = 10p^2c^4 \implies \text{ord}_p(c) \geq 1$, which contradicts the condition $\min\Big(\text{ord}_p(a), \text{ord}_p(b), \text{ord}_p(c)\Big) = 0$. Therefore, we must have $\text{ord}_p(a) \leq 1$ and we consider cases.

- Case 1: $\text{ord}_p(a) = 0$. Reduction modulo p gives $a^2 \equiv 2b^4 \mod p$. Observe that $\text{ord}_p(a) = 0 \implies b \not\equiv 0 \mod p$. By choosing $b \equiv 1 \mod p$, we see that this equation has a non-trivial solution modulo p if and only if $\left(\frac{2}{p}\right) = 1$ (If we have a non-trivial solution where $b \not\equiv 1 \mod p$, then we can divide through by b^4 to obtain a solution in the desired form). In this case, the quartic has a non-trivial solution in $\mathbb{Q}_p$ if and only if $p \equiv \pm 1 \mod 8$.
- Case 2: $\text{ord}_p(a) = 1$. Note that we still have $p \mid a^2 - 9pb^2c^2 - 10p^2c^4 = b \implies \text{ord}_p(b) \geq 1$ and thus let $a = wp, \text{ord}_p(w) = 0$ and $b = yp, \text{ord}_p(y) \geq 0$. The equation now becomes

$$w^2p^2 = 2y^4p^4 + 9p(y^2p^2)c^2 + 10p^2c^4 \implies w^2 = 2p^2y^4 + 9py^2c^2 + 10c^4.$$

  Reduction modulo p yields $w^2 \equiv 10c^4 \mod p$. Observe that $\text{ord}_p(w) = 0 \implies c \not\equiv 0 \mod p$. Similar reasoning as above shows that this equation has a non-trivial solution modulo p if and only if $\left(\frac{10}{p}\right) = 1 \iff p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \mod 40$.

Thus, this equation has a non-trivial solution modulo p if and only if

$$p \equiv \pm 1, \pm 3, \pm 7, \pm 9, \pm 13, \pm 17 \mod 40.$$

(2) $a^2 = pb^4 + 9pb^2c^2 + 20pc^4$. We clearly have $\text{ord}_p(a) \geq 1$; thus, let $a = wp$. Dividing both sides by p gives us $w^2p = b^4 + 9b^2c^2 + 20c^4 = (b^2 + 4c^2)(b^2 + 5c^2)$. Reduction mod p gives us $(b^2 + 4c^2)(b^2 + 5c^2) \equiv 0 \mod p$. Note that either b or $c \equiv 0 \mod p$ forces the other to be divisible by p, which contradicts the condition that not all a, b, c are in $p\mathbb{Z}_p$. Therefore, the quartic has nontrivial solutions mod p if and only if:

- $b^2 \equiv -4c^2 \mod p \implies \left(\frac{-1}{p}\right) = 1$, or
- $b^2 \equiv -5c^2 \mod p \implies \left(\frac{-1}{p}\right) = \left(\frac{5}{p}\right)$.

Note that $\left(\frac{5}{p}\right) = -1$ (or $p \equiv \pm 2 \mod 5$) or $\left(\frac{-1}{p}\right)$ (or $p \equiv 1 \mod 4$) implies that the quartic is solvable. Otherwise, we have $\left(\frac{5}{p}\right) = 1$, and $\left(\frac{-1}{p}\right) = 1 \implies p \equiv 1, 9 \mod 20$.

Thus, this equation has a non-trivial solution modulo p if and only if

$$p \equiv 1, 3, 7, 9, 13, 17, 21, 23, 27, 29, 33, 37 \mod 40.$$

(3) $a^2 = 2pb^4 + 9pb^2c^2 + 10pc^4$. We clearly have $\text{ord}_p(a) \geq 1$; thus, let $a = wp$. Dividing both sides by p gives us $w^2p = 2b^4 + 9b^2c^2 + 10c^4 = (2b^2 + 5c^2)(b^2 + 2c^2)$. Reduction mod p gives us $(2b^2 + 5c^2)(b^2 + 2c^2) \equiv 0 \mod p$. By the same argument above, $b, c \not\equiv 0 \mod p$. Henceforth, the quartic has nontrivial solutions mod p if and only if:

- $-2b^2 \equiv 5c^2 \mod p \implies \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = \left(\frac{5}{p}\right)$ or
- $b^2 \equiv -2c^2 \mod p \implies \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$.

Note that $\left(\frac{5}{p}\right) = -1$ (or $p \equiv \pm 2 \mod 5$) or $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right)$ (or $p \equiv 1, 3 \mod 8$) implies that the quartic is solvable. Otherwise, we have $\left(\frac{5}{p}\right) = 1$, and $\left(\frac{-1}{p}\right) = \left(\frac{2}{p}\right) \implies p \equiv 1 \mod 8$. Thus, this equation has a non-trivial solution in $\mathbb{Q}_p$ if and only if

$$p \equiv 1, 3, 7, 9, 11, 13, 17, 19, 23, 27, 33, 37 \mod 40.$$

(4) $a^2 = pb^4 - 18pb^2c^2 + pc^4$. We clearly have $\text{ord}_p(a) \geq 1$; thus, let $a = wp$. Dividing both sides by p gives us $w^2p = b^4 - 18b^2c^2 + c^4 = (b^2 - 4bc - c^2)(b^2 + 4bc - c^2)$. Reduction mod p gives us $(b^2 - 4bc - c^2)(b^2 + 4bc - c^2) \equiv 0 \mod p$. Note that either b or $c \equiv 0 \mod p$ forces the other to be divisible by p, which contradicts the condition that not all a, b, c are in $p\mathbb{Z}_p$. Simplifying each quadratic via the quadratic formula gives us that there is a non-trivial solution to this equation if and only if $\left(\frac{5}{p}\right) = 1 \iff p \equiv \pm 1 \mod 5$. Thus, this equation has a non-trivial solution in $\mathbb{Q}_p$ if and only if

$$p \equiv \pm 1, \pm 9, \pm 11, \pm 19 \mod 40.$$

5.2. **Existence of Non-Trivial Solutions in $\mathbb{Q}_5$.** Note: By multiplying by appropriate powers of 5, we can assume that all of a, b, c are in $\mathbb{Z}_5$ with at least one of a, b, c not in $5\mathbb{Z}_5$

(1) $a^2 = 2b^4 + 9pb^2c^2 + 10p^2c^4$. We have $5 \mid b \implies 5 \mid a \implies \mathrm{ord}_5(c) \geq \mathrm{ord}_5(a^2 - 2b^4 - 9pb^2c^2) - \mathrm{ord}_5(10p^2) = 1$, which contradicts the condition that at least one of a, b, c not in $5\mathbb{Z}_5$. Thus, $b \not\equiv 0 \mod 5$. Reduction mod 5 gives us $a^2 \equiv 2 + 9b^2c^2 \mod 5$. The array

$p \mod 5$	(a, b, c)
1	$(1, 1, 1)$
2	$(0, 1, 1)$
3	$(2, 1, 1)$
4	$(1, 2, 1)$

shows that the quartic has a nontrivial solution mod 5 (and hence in $\mathbb{Q}_5$ by Hensel's lemma) for all p.

(2) $a^2 = pb^4 + 9pb^2c^2 + 20p^2c^4$. The same reasoning as above shows that $c \not\equiv 0 \mod 5$. Reduction mod 5 gives us $a^2 \equiv p + 4pb^2c^2 \mod 5$. The array

$p \mod 5$	(a, b, c)
1	$(0, 1, 1)$
2	$(0, 1, 1)$
3	$(0, 1, 1)$
4	$(0, 1, 1)$

shows that the quartic has a nontrivial solution mod 5 (and hence in $\mathbb{Q}_5$ by Hensel's lemma) for all p.

(3) $a^2 = 2pb^4 + 9pb^2c^2 + 10pc^4$. The same reasoning as above shows that $c \not\equiv 0 \mod 5$. Reduction mod 5 gives us $a^2 \equiv 2p + 4pb^2c^2 \mod 5$. The array

$p \mod 5$	(a, b, c)
1	$(1, 1, 1)$
2	$(2, 0, 1)$
3	$(1, 0, 1)$
4	$(2, 1, 1)$

shows that the quartic has a nontrivial solution mod 5 (and hence in $\mathbb{Q}_5$ by Hensel's lemma) for all p.

(4) $a^2 = pb^4 - 18pb^2c^2 + pc^4$. The ordered triple $(a, b, c) \equiv (0, 1, 1) \mod 5$ shows that the quartic has a nontrivial solution mod 5 (and hence in $\mathbb{Q}_5$ by Hensel's lemma) for all p.

5.3. **Existence of Non-Trivial Solutions in $\mathbb{Q}_2$.** Note: By multiplying by appropriate powers of 2, we can assume that all of a, b, c are in $\mathbb{Z}_2$ with at least one of a, b, c not in $2\mathbb{Z}_2$.

(1) $a^2 = 2b^4 + 9pb^2c^2 + 10p^2c^4$. Note the chain of logic

$$\begin{array}{lllllll} 2 \mid a & \implies & 4 \mid a^2 = 2b^4 + 9pb^2c^2 + 10p^2c^4 & \implies & 2 \mid b \text{ or } 2 \mid c & \implies & 2 \text{ divides the other} \\ 2 \mid b & \implies & 2 \mid 2b^4 + 9pb^2c^2 + 10p^2c^4 = a^2 & \implies & 2 \mid a & \implies & 2 \mid c \\ 2 \mid c & \implies & 2 \mid 2b^4 + 9pb^2c^2 + 10p^2c^4 = a^2 & \implies & 2 \mid a & \implies & 2 \mid b \end{array},$$

which shows that we must have a, b, c all be odd, lest we contradict the condition

$$\min(\mathrm{ord}_2(a), \mathrm{ord}_2(b), \mathrm{ord}_2(c)) = 0.$$

Since they are all odd, we must have $1 \equiv a^2 \equiv 2b^4 + 9pb^2c^2 + 10p^2c^4 \equiv 4 + p \mod 8 \implies p \equiv 5 \mod 8$. The ordered triple $(a, b, c) \equiv (1, 1, 1) \mod 8$, along with the fact that $2 \nmid a$ means that we can always find a nontrivial solution to the quartic in $\mathbb{Q}_2$ by applying Strong Hensel's Lemma if and only if $p \equiv 5 \mod 8$.

(2) $a^2 = pb^4 + 9pb^2c^2 + 20pc^4$. We inherit conditions for solvability from our analysis in $\mathbb{Q}_p$ that $p \equiv 1 \mod 4$, the table

$$\begin{array}{cc} p \mod 8 & (a, b, c) \\ \hline 1 & (1, 1, 4) \\ 5 & (7, 1, 2) \end{array},$$

shows that because we can find a solution mod 8 with a odd, we can always find a nontrivial solution to the quartic in $\mathbb{Q}_2$ by applying Strong Hensel's Lemma if and only $p \equiv 1 \mod 4$.

(3) $a^2 = 2pb^4 + 9pb^2c^2 + 10pc^4$. Note the chain of logic

$$\begin{array}{lllllll} 2 \mid a & \implies & 4 \mid a^2 = 2pb^4 + 9pb^2c^2 + 10pc^4 & \implies & 2 \mid b \text{ or } 2 \mid c & \implies & 2 \text{ divides the other} \\ 2 \mid b & \implies & 2 \mid 2pb^4 + 9pb^2c^2 + 10pc^4 = a^2 & \implies & 2 \mid a & \implies & 2 \mid c \\ 2 \mid c & \implies & 2 \mid 2pb^4 + 9pb^2c^2 + 10pc^4 = a^2 & \implies & 2 \mid a & \implies & 2 \mid b \end{array},$$

which shows that we must have a, b, c all be odd, lest we contradict the condition

$$\min(\mathrm{ord}_2(a), \mathrm{ord}_2(b), \mathrm{ord}_2(c)) = 0.$$

Since they are all odd, we must have $1 \equiv a^2 \equiv 2pb^4 + 9pb^2c^2 + 10pc^4 \equiv 5p \mod 8 \implies p \equiv 5 \mod 8$. A nontrivial solution $(a, b, c) \equiv (1, 1, 1) \mod 8$, along with the fact that $2 \nmid a$ means that we

can always find a nontrivial solution to the quartic in $\mathbb{Q}_2$ by applying Strong Hensel's Lemma if and only if $p \equiv 5 \mod 8$.

(4) $a^2 = pb^4 - 18pb^2c^2 + pc^4$. The ordered triple $(a, b, c) \equiv (4, 1, 1) \mod 32$ shows that the quartic has nontrivial solution mod 32 (and hence in $\mathbb{Q}_2$ by Strong Hensel's lemma) for all p.

Therefore, for each quartic we will now tabulate the prime twists mod 40 is that quartic everywhere locally solvable:

Quartic	$p \mod 40$
1	13, 37
2	1, 9, 13, 17, 21, 29, 33, 37
3	13, 37
4	1, 9, 11, 19, 21, 29, 31, 39

We now retabulate the results to find rank bounds for our elliptic curves based upon the residue classes of p modulo 40.

$p \mod 40$	$\#\phi(E)$	$\#\bar{\phi}(\bar{E})$	Rank Bound
1	2	8	2
3	1	4	0
7	1	4	0
9	2	8	2
11	2	4	1
13	1	16	2
17	1	8	1
19	2	4	1
21	2	8	2
23	1	4	0
27	1	4	0
29	2	8	2
31	2	4	1
33	1	8	1
37	1	16	2
39	2	4	1

6. The L-series of an Elliptic Curve

Now we consider the family of elliptic curves:

$$E^n : y^2 = x^3 - nx,$$

where n ranges over the natural numbers. To each curve there is an associated complex function $L(E^n, s)$, the L function of the elliptic curve, defined as

$$L(E^n, s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}},$$

where Δ is the discriminant of the relevant cubic and $a_p = p + 1 - \#E^n(\mathbb{F}_p)$, where $\#E^n(\mathbb{F}_p)$ is the size of the group of points of the elliptic curve over the finite field $\mathbb{F}_p$. This function is of particular interest in that it is part of the Birch and Swinnerton-Dyer Conjecture that near $s = 1$ in the complex plane, stated weakly,

$$L(E^n, s) \approx (s - 1)^r,$$

where r is the rank of the elliptic curve E^n.

In order to begin our study of this function, we must make sure that it makes sense to speak about the L function near $s = 1$. Namely, we should show that $L(E^n, s)$ is analytic in a neighborhood of 1; in fact, we will end up showing that $L(E^n, s)$ is an entire function[1]. To do this, we will first understand the numbers a_p for every p via the object known as a Hecke character through the language of Gauss and Jacobi sums.

6.1. **Gauss and Jacobi Sums; Hecke Characters.**

Definition 5. Let $\psi : \mathbb{F}_q \to \mathbb{C}^*$ be a nontrivial additive character (i.e., $\psi(a + b) = \psi(a)\psi(b)$ for all $a, b \in \mathbb{F}_q$) and $\chi : \mathbb{F}_q^* \to \mathbb{C}^*$ be any multiplicative character (i.e., $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in \mathbb{F}_q$). Define the **Gauss Sum** $g(\chi)$, where the multiplicative character χ is treated as the input variable, by

$$g(\chi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x)$$

and the **Jacobi sum** $J(\chi_1, \chi_2)$ on two multiplicative characters by

$$J(\chi_1, \chi_2) = \sum_{x \in \mathbb{F}_q} \chi_1(x)\chi_2(1 - x).$$

[1]The claim that the L-function of *every* elliptic curve is entire is the content of the Hasse-Weil Conjecture

Proposition 12 (Properties of Gauss and Jacobi Sums). Let χ_{triv} be the trivial multiplicative character from $\mathbb{F}_q$ to $\mathbb{C}^*$ (i.e., $\chi_{triv}(x) = 1$ for all $x \in \mathbb{F}_q$) and let χ, χ_1, χ_2 be nontrivial characters from F_q to $\mathbb{C}^*$. The following results hold:

(1) $g(\chi_{triv}) = -1$;

(2) $J(\chi_{triv}, \chi_{triv}) = q - 2$;

(3) $J(\chi_{triv}, \chi) = -1$;

(4) $J(\chi, \bar{\chi}) = -\chi(-1)$;

(5) $J(\chi_1, \chi_2) = J(\chi_2, \chi_1)$;

(6) $g(\chi) \cdot g(\bar{\chi}) = \chi(-1)q$;

(7) $|g(\chi)| = \sqrt{q}$;

(8) $J(\chi_1, \chi_2) = g(\chi_1)g(\chi_2)/g(\chi_1\chi_2)$ if $\chi_1\chi_2 \neq \chi_{triv}$.

Proof. This is the first part of Chapter 8 in [IRo90]. □

Definition 6. Let $K \subset \mathbb{C}$ be a field that is a totally complex quadratic extension of a totally real subfield K_0. Furthermore, let $K/\mathbb{Q}$ be Galois and let j be the restriction of complex conjugation to K. Let $\mathscr{O} \subset K$ be the ring of integers and let $M \leq \mathscr{O}$ be an ideal. An **algebraic Hecke character modulo** M is a function χ from the ideals of $\mathscr{O}$ to $\mathbb{C}$ such that for all $A, B \leq \mathscr{O}$ ideals, $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$

(1) $\chi(\mathscr{O}) = 1$.

(2) $\chi(A) \neq 0$ if and only if A is relatively prime to M.

(3) $\chi(AB) = \chi(A)\chi(B)$.

(4) There is an element $\theta = \sum_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} n(\sigma)\sigma \in \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ such that if $\alpha \in \mathscr{O}, \alpha \equiv 1 \mod M$, then $\chi(\langle\alpha\rangle) = \alpha^\theta$.

(5) There is an integer $m > 0$ such that $n(\sigma) + n(j\sigma) = m$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$.

The number m in (5) is called the weight of χ.

Theorem 13. *Let χ be an algebraic Hecke character and let*

$$L(s, \chi) = \prod_P (1 - \chi(P)N(P)^{-s})^{-1} = \sum_A \chi(A)N(A)^{-s},$$

where the product is over all prime ideals of $\mathscr{O}$ and the sum is over all ideals of $\mathscr{O}$. If $\chi(A) \neq 0, 1$ for some A, then $L(s, \chi)$ can be analytically continued to an entire function on all of $\mathbb{C}$.

Proof. This is the content of Chapter 14 of [Lang]. □

6.2. $y^2 = x^3 - n^2x$, **Local Information.** The following result is a straightforward computation:

Proposition 14. Consider the two curves

$$E : y^2 = x^3 - n^2x \qquad \text{and} \qquad C : u^2 = v^4 + 4n^2.$$

There is a bijection from $E \setminus \{0, 0\}$ to C

$$S(x, y) = \left(2x - \frac{y^2}{x^2}, \frac{y}{x}\right)$$

to which the inverse is

$$T(u, v) = \left(\frac{u + v^2}{2}, \frac{v(u + v^2)}{2}\right).$$

As for something slightly non-trivial:

Proposition 15. Let p be a prime number such that $p \nmid 2n^2$. Let $E : y^2 = x^3 - n^2x$ be an elliptic curve over $\mathbb{F}_p$ and denote $N_p = 1 + \#\{(x, y) \in \mathbb{F}_p^2, y^2 = x^3 - n^2x\}$ (the extra 1 is for the point at infinity). If $p \equiv 3 \mod 4$, then $N_p = p + 1$. If $p \equiv 1 \mod 4$, then by letting $p = \pi\bar{\pi}$ such that $\pi \in \mathbb{Z}[i]$ and $\pi \equiv 1 \mod 2 + 2i$,

$$N_p = p + 1 - \overline{\left(\frac{n^2}{\pi}\right)_4}\,\pi - \left(\frac{n^2}{\pi}\right)_4 \bar{\pi}.$$

Proof. This is the content of Section 18.4 in [IRo90]. □

6.3. $y^2 = x^3 - n^2x$, L**-series and its Analytic Continuation.**

Theorem 16. *Consider the elliptic curve $E : y^2 = x^3 - n^2x$ for some given $n \in \mathbb{Z}$. Construct a map χ from the prime ideals of $\mathbb{Z}[i]$ to the complex numbers such that for all prime ideals $P \leq \mathbb{Z}[i]$,*

1. *If P divides $2n^2$, then define $\chi(P) = 0$.*
2. *If $N(P) = p$, then $p \equiv 1 \mod 4, P = (\pi)$ with $\pi \equiv 1 \mod 2 + 2i$ and define $\chi(P) = \overline{(n^2/\pi)_4}\pi$.*
3. *If $N(P) = p^2$, then $p \equiv 3 \mod 4, P = (\pi)$ and define $\chi(P) = -p$.*

The map χ is an algebraic Hecke character of weight 1 modulo $\langle 8n^2 \rangle$ and $L(E, s) = L(s, \chi)$. It then follows that $L(E, s)$ has an analytic continuation to an entire function on the complex plane.

Proof. This is the content of Section 18.6 in [IRo90]. □

References

[Apo76] Apostol, T. *Introduction to Analytic Number Theory*. New York: Springer Science+Business Media, Inc., 1976.

[Gou97] Gouvêa, F. *p-adic Numbers*. Berlin: Springer-Verlag, 1997.

[IRo90] Ireland, K; Rosen, M. *A Classical Introduction to Modern Number Theory*. New York: Springer Science+Business Media, Inc., 1990.

[Kob93] Koblitz, N. *Introduction to Elliptic Curves and Modular Forms*. New York: Springer-Verlag, 1993.

[Lang] Lang, S. *Algebraic Number Theory*. New York: Springer-Verlag, 1994.

[NZM91] Niven, I; Zuckerman, H; Montgomery; H. *An Introduction to the Theory of Numbers*. New York: Wiley, 1991.

[RS02] Rubin, K; Silverberg, A. "Ranks of elliptic curves." *Bull. Amer. Math. Soc.* **39** (2002) 455–474.

[Ser73] Serre, J.P. *A Course in Arithmetic*. New York: Springer-Verlag, 1973.

[Sil86] Silverman, J.H. *The Arithmetic of Elliptic Curves*. New York: Springer-Verlag, 1986.

[ST92] Silverman, J.H.; Tate, J. *Rational points on elliptic curves*. New York: Springer Science+Business Media, Inc., 1992.

[Wil00] Wiles, A. "The Birch and Swinnerton-Dyer Conjecture."
`http://www.claymath.org/millennium/`