Chapter 2. Points of finite order

M. Imris, N. Navea de Grahl

October 10, 2023

The main goal of this talk is to prove the Nagell-Lutz theorem, which consists of two parts. The first part says that if a rational point (x, y) has finite order, then it's coordinates are integers. The second part states that either $y = 0$, in which case the point (x, y) has order two, or y divides the discriminant D. We used the book "Rational Points of on Elliptic Curves" by Joseph H. Silverman and John T. Tate.

1 Points of Order Two and Three

Definition 1.1 (Order)**.** For an element P of a group we say that P has order $n \in \mathbb{N}$ if

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ summands}} = \mathcal{O},$$

but $mP \neq \mathcal{O}$ for all intergers $1 \leq m < n$. If such a n exists, then we say that P has finite order, otherwise we say that P has infinite order.

Theorem 1.1 (Points of Order Two and Three)**.** *Let C be a non-singular cubic curve*

$$C : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

a) A point $P = (x, y) \neq \mathcal{O}$ on C has order two if and only if $y = 0$.

b) The curve C has exactly four points of order dividing two. The points form a group that is the product of two cyclic groups of order two.

c) A point $P = (x, y) \neq \mathcal{O}$ on C has order three if and only if x is a root of the polynomial

$$\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

d) The curve C has exactly nine points of order dividing three. These nine point form a group that is a product of two cyclic groups of order three.

Proof. $P = (x, y)$ has order equal to 2 is equivalent to the condition $P = -P$. Since $-(x, y) = (x, -y)$ we conclude that $y = -y$ and therefore $y = 0$. Conversely, if y = 0 we have $P = (x, 0) = (x, -0) = -P$ and $2P = \mathcal{O}$ follows immediately. This concludes part (a).

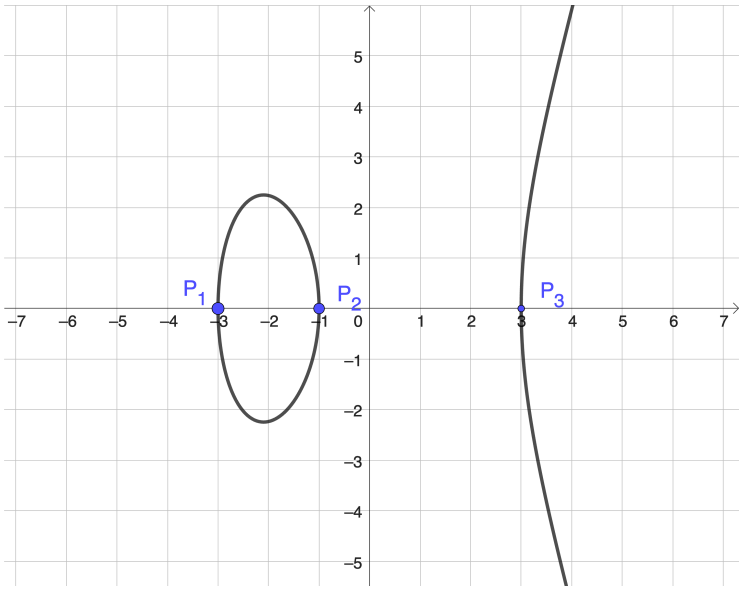

Figure 1: The points of order 2 on the curve $C : y^2 = x^3 + x^2 - 9x - 9$

By part (a), we know that the elements of order 2 are exactly the points $(x, 0)$, such that x is a root of f. By assumption, C is non singular, which means that over $\mathbb{C}$ f has 3 distinct roots a_1, a_2, a_3. Therefore the points

$$P_1 = (a_1, 0), P_2 = (a_2, 0), P_3 = (a_3, 0)$$

are exactly the points of order 2 of C. Combining this, and the fact that $\mathcal{O}$ has order 1, we get that the points with order a divisor of two are exactly

$$\{\mathcal{O}, P_1, P_2, P_3\}.$$

It's easy to see that the addition of any two elements of this set has order less than or equal to 2, and therefore it forms a subgroup of order 4. Since there is no element of order 4, we see that the group is just $C_2 \times C_2$.

image of curve with 3 real roots and the corresponding points of order 2

To prove (c) we first check that a point P that's not $\mathcal{O}$ has order 3 if and only if $x(2P) = x(P)$:

If we have $2P = -P$, it follows that $x(2P) = x(-P) = x(P)$. Conversely, if $x(2P) = x(P)$ holds, we have that $2P = -P$ or $2P = P$. If the latter is true, we get $P = \mathcal{O}$ which we excluded, and therefore we obtain that P has order 3.

Now to explicitly find the points that satisfy this condition, we apply the duplication formula for $P = (x, y)$ and set it equal to x. This yields

$$\frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = x,$$

or equivalently

$$3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2 = 0$$

Note that this is precisely the polynomial named in part (c) of the statement of the Theorem which concludes the proof of (c).

Now we want to to show that the polynomial ψ_3 has 4 distinct roots by showing that ψ_3 and ψ_3' have no common roots. One can check with a quick calculation that we can write ψ_3 as

$$\psi_3 = 2f(x)f''(x) - f'(x)^2.$$

Taking the derivative of ψ_3 we get

$$\psi_3' = 2f(x)f'''(x) = 12f(x)$$

and therefore, a common root of of ψ_3 and ψ_3' would imply a common root of f and f' which is a contradiction, since f is assumed to be non singular.

So ψ_3 has 4 distinct roots x_1, x_2, x_3, x_4 in $\mathbb{C}$. For $0 < i < 5$, define $y_i := \sqrt{f(x_i)}$. Now we can easily see that the set

$$\{(x_1, \pm y_1), (x_1, \pm y_2), (x_1, \pm y_3), (x_1, \pm y_4)\}$$

has exactly 8 elements: Since the x_i are pairwise different, we just have to check $y_i \neq 0$. But this is a consequence of part (a), since $y_i = 0$ would imply that the order of (x_i, y_i) is 2 and not 3, which is a contradiction. So we have 8 distinct elements of order 3. Together with $\mathcal{O}$ that makes 9 elements of order a divisor of three. These 9 elements (by the same reasoning as before) form a subgroup of order 9 that is not cyclic, and therefore must be $C_3 \times C_3$. This concludes the proof of the theorem.

2 The Discriminant

We first want to show that we may assume that our cubic curve is given by a polynomial with integer coefficients.

Consider a cubic curve in it's normal form

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{Q}$. Let $a = \frac{a_1}{a_2}, b = \frac{b_1}{b_2}$ and $c = \frac{c_1}{c_2}$ where $a_i, b_i, c_i \in \mathbb{Z}$ for $i = 1$ and $i = 2$. By letting $X = d^2x$ and $Y = d^3y$ this equation becomes

$$Y^2 = X^3 + d^2\frac{a_1}{a_2}X^2 + d^4\frac{b_1}{b_2}X + d^6\frac{c_1}{c_2}$$

and by choosing $d = a_2b_2c_2$ we can now eliminate all denominators in a, b and c. Therefore we will from now on assume that our cubic curve is given by an equation with integer coefficients.

We will now introduce the concept of the discriminant of a polynomial and prove a lemma from which the second claim of the Nagell-Lutz theorem follows.

Definition 2.1 (Discriminant)**.** Given a cubic curve

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{Z}$, we define the discriminant of $f(x)$ to be the value

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

If we factor f over the complex numbers we get

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3),$$

where α_1, α_2 and α_3 are the roots of f, and by direct computation we get

$$D = (\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2.$$

Therefore it is clear that $D \neq 0$ if and only if the polynomial f has distinct roots, which is why the Nagell-Lutz theorem stipulates that the cubic curve is non-singular.

Lemma 2.1. *Let $P = (x, y)$ be a point on our cubic curve such that both P and $2P$ have integer coordinates. Then either $y = 0$ or $y \mid D$.*

For the proof of this lemma we need an additional result.

Lemma 2.2. *Let $f(x) = x^3 + ax^2 + bx + c$ be a monic polynomial in the ring $\mathbb{Z}[x]$, then it's discriminant is in the ideal of $\mathbb{Z}[x]$ generated by $f(x)$ and $f'(x)$.*

Proof. We define

$$r(x) := (18b - 6a^2)x - (4a^3 - 15ab + 27c)$$

and

$$s(x) := (2a^2 - 6b)x^2 + (2a^3 - 7ab + 9c)x + (a^2b + 3ac - 4b^2).$$

By direct computation we see that

$$D = r(x)f(x) + s(x)f'(x).$$

□

Remark 2.1. Lemma 2.2 also holds in a much more general context. Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$, then it's discriminant D is in the ideal generated by $f(x)$ and $f'(x)$.

Now we will prove lemma 2.1.

Proof. Let y be a non zero integer, we want to show that y divides the discriminant D. Since $P \neq \mathcal{O}$ and $y \neq 0$ it follows from theorem 1.1 that P isn't of order 2, therefore $2P \neq \mathcal{O}$ and we can write $2P = (X, Y)$. From the duplication formula we get

$$X = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c}$$

and it follows that

$$2x + X = \lambda^2 - a, \quad \text{where} \quad \lambda = \frac{f'(x)}{2y},$$

which is equivalent to

$$\frac{f'(x)^2}{y^2} = 8x + 4X + 4a.$$

Since $x, X, a, f'(x)$ and y are all integers it follows that y divides $f'(x)$. In particular we have $y \mid f(x)$ since $y^2 = f(x)$. Using lemma 2.2 we get

$$D = r(x)f(x) + s(x)f'(x)$$

for $r(x), s(x) \in \mathbb{Z}[x]$. Thus y divides D.

□

3 Points of Finite Order Have Integer Coordinates

In this section we want to prove that rational points (x, y) of finite order on a non singular curve with integer coefficients have integer coefficients, which will basically conclude the proof of the Nagell-Lutz theorem. The approach to do that is rather indirect: we're going to show that no prime divides the denominator of x or y in a series of steps. So let p be a prime.

It will be helpful to introduce some notation. We note that every non-zero rational number can be written uniquely in the form $\frac{m}{n}p^\nu$ where m, n are integers that are coprime to p and the fraction is in lowest terms.

Definition 3.1. We define the *order* of such a rational number as the unique exponent ν of p in that representation

$$\operatorname{ord}\Big(\frac{m}{n}p^\nu\Big) := \nu.$$

So we see that the denominator of a rational number is divisible by p if and only if the order of that rational number is negative. This order depends on the chosen prime:

$$\operatorname{ord}_2\Big(\frac{2}{7}\Big) = 1,\ \operatorname{ord}_2\Big(\frac{2}{7}\Big) = -1,\ \operatorname{ord}_3\Big(\frac{2}{7}\Big) = 0$$

If we know look at at point (x, y) on our curve and assume that p divides the denominator of x we obtain that $x = \frac{m}{n}p^\mu,\ y = \frac{u}{w}p^\sigma$ with $\mu > 0$ and p doesn't divide m, n, u, w. By plugging in our point in our curve and comparing the orders of both sides, we get

$$3\mu = 2\sigma,$$

and it quickly follows that that

$$\mu = 2\nu,\ \sigma = 3\nu$$

for some $\nu > 0$. In particular p also divides the denominator of y. Similarly, if we assume p divides the denominator of y, by the same calculation we get that $\mu = 2\nu,\ \sigma = 3\nu$ for again some $\nu > 0$. So if p divides the denominator of x or y, it divides both of them and the exact power is $p^{2\nu}$ and $p^{3\nu}$.

Definition 3.2. We define

$$C(p^\nu) = \{(x, y) \in C(\mathbb{C}) : \text{ord}(x) \leq -2\nu,\ \text{ord}(y) \leq -3\nu\},$$

in other words the rational points (x, y) on C such that $p^{2\nu}$ divides x and $p^{3\nu}$ divides y. By convention we include $\mathcal{O}$ in every $C(p^\nu)$. We clearly have

$$C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset C(p^3) \supset ...$$

Definition 3.3. We define

$$R := R_p := \{q \in \mathbb{Q} : \text{ord}(q) \geq 0\}.$$

Using the convention $\text{ord}(0) = \infty$, we see that R is the ring that contains 0 and the non-zero rational numbers with no p in the denominator. In fact, it can even be shown that R has unique factorization and is local with the maximal ideal (p). The units in R are the elements of $\mathbb{Q}$ with order 0.

Proposition 3.1. *Let p be a prime number, R the ring of rational numbers with denominator prime to p and $C(p^\nu)$ the set of rational point (x, y) on our curve for which x has denominator divisible by $p^{2\nu}$, together with the point $\mathcal{O}$.*

a) $C(p)$ consists of all rational points (x, y) for which the denominator of either x or y is divisible by p.

b) For every $\nu \geq 1$, the set $C(p^\nu)$ is a subgroup of the group of rational points $C(\mathbb{Q})$.

c) The map

$$\frac{C(p^\nu)}{C(p^{3\nu})} \longrightarrow \frac{p^\nu R}{p^{3\nu} R}, \quad P = (x, y) \longmapsto t(P)\frac{x}{y},$$

is a one-to-one homomorphism which by convention sends $\mathcal{O}$ to 0.

Proof. (Sketch) In the previous discussion we proved part (a).
For (b) we change the coordinates by

$$t = \frac{x}{y},\ s = \frac{1}{y}.$$

Intuitively, this means that in our $s - t$ plane our origin is now $\mathcal{O}$, and all our points with $y = 0$ lie now at infinity. Apart from those points, all other points get mapped bijectively between the two planes.
We can also see with a computation that a line in the x, y plane correspond to lines in the t, s plane, and therefore we can add points in the t, s plane in the same sense as in the x, y plane. Additionally, we see that for a point on the curve we have

$$(t, s) \in C(p^\nu) \text{ if and only if } t \in p^\nu R \text{ and } s \in p^{3\nu} R.$$

So to show that $C(p^\nu)$ is a group we check that it is closed under addition: One can show that if we have $P_1 = (t_1, s_1),\ P_2 = (t_2, s_2) \in C(p^\nu)$ or equivalently $t_1, t_2 \in p^\nu R$, then the t coordinate of $P_1 + P_2$ is also in $p^\nu R$. A similar property also holds for the s coordinates.

Additionally, if for $P = (t, s)$ p^ν divides t and $p^{3\nu}$ divides s, the same holds for $-t$ and $-s$ respectively, and therefore $-P = (-t, -s) \in C(p^\nu)$.
Thus $C(p^\nu)$ is closed under addition and taking inverses, and we conclude the proof of (b).
The key to prove part (c) is to use a formula derived in the proof of (b) that we omitted, namely that

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3\nu}R}$$

. Thus, we get a surjective homomorphism

$$\phi : C(p^\nu) \twoheadrightarrow \frac{p^\nu R}{p^{3\nu}R},\ (x, y) \mapsto \frac{x}{y} \bmod (p^{3\nu}R).$$

Note that the kernel of ϕ is given by those points whose t coordinate is in $p^{3\nu}R$, i.e. the points that are in $C(p^{3\nu})$. This proves the proposition.

Corollary 3.1. *(a) For every prime p, the only point of finite order in the group $C(p)$ is the identity point $\mathcal{O}$.*

(b) Let $P = (x, y) \in C(\mathbb{Q})$ be a rational point of finite order. Then x and y are integers.

Proof. First we will prove (a). Let $P = (x, y) \in C(\mathbb{Q})$ be a point of order $m \geq 2$ and let p be a prime number. We will show $P \notin C(p)$ by contradiction. Assume that $P \in C(p)$, because the denominator of x cannot be divisible by arbitrary large powers of p, we can find $\nu > 0$ such that $P \in C(p^\nu)$ and $P \notin C(p^{\nu+1})$. We have two cases to consider: $p \nmid m$ and $p \mid m$.
First suppose that $p \nmid m$, by repeatedly applying the congruence

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \pmod{p^{3\nu}R}$$

we get

$$t(mP) \equiv mt(P) \pmod{p^{3\nu}R}.$$

Since P is of order m, we get $t(mP) = t(\mathcal{O}) = 0$. Since m is prime to p, it is a unit in the ring R, thus

$$0 \equiv t(P) \pmod{p^{3\nu}R}.$$

This implies that $P \in C(p^{3\nu})$, which contradicts our assumption that $P \notin C(p^{\nu+1}) \supset C(p^{3\nu})$.
Now we suppose that $p \mid m$, and write $m = pq$. Now we consider the point $P' := (x', y') = qP$, which is clearly of order p. In addition we have $P' \in C(p^\nu)$ and $P' \notin C(p^{\nu+1})$, since $C(p^\sigma)$ is a subgroup of $C(\mathbb{Q})$ for $\sigma \geq 1$. By using the same congruence we get

$$0 = t(\mathcal{O}) = t(pP') \equiv pt(P') \pmod{p^{3\nu}R}.$$

Therefore

$$t(P') \equiv 0 \pmod{p^{3\nu-1}R},$$

and since $C(p^{\nu+1}) \supset C(p^{3\nu-1})$ we get a contradiction, in that $P' \notin C(p^{\nu+1})$.

Now we will prove (b). Let $P = (x, y)$ be a point of finite order, from (a) we know that $P \notin C(p)$ for all primes p. Therefore the denominators of x and y are not divisible by any primes, which implies that they are both equal to one. Thus x and y are integers. □

4 The Nagell-Lutz Theorem and Further Developments

We will now precisely state and prove the Nagell-Lutz theorem.

Theorem 4.1 (Nagell-Lutz Theorem)**.** *Let*

$$y^2 = f(x) = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c, let D be the discriminant of the cubic polynomial and $P = (x, y)$ a rational point of finite order. Then x and y are integers, and either $y = 0$, in which case P has order two, or y divides D.

Proof. It follows from corollary 3.1 that a point of finite order necessarily has integer coefficients. If P is a point of order two, it follows from theorem 1.1 that $y = 0$ and otherwise $2P \neq \mathcal{O}$. Since $2P$ is also a point of finite order, it's coordinates are also integers. Using lemma 2.1 it follows that y divides D, thus concluding the proof. □

At this point it is important to make clear that the Nagell-Lutz theorem says nothing about the order of a point (x, y) with integer coordinates such that $y \mid D$.

Remark 4.1. There is also a stronger form of the Nagell-Lutz Theorem which states that if $P = (x, y)$ is a rational point of finite order with $y \neq 0$, then y^2 divides the discriminant D.

With the help of the Nagell-Lutz theorem one can therefore find the rational points of finite order in a finite amount of steps. We take the discriminant D and consider it's finite amount of divisors. We then substitute these integers into the polynomial equation $y^2 = f(x)$. Since by assumption f is monic and has integer coefficients, any integer root will divide the constant term c. Once we find a potential integer point P of finite order, we can compute $2P, 3P, ...$ until we get a point nP for $n \in \mathbb{N}$ with non integer coordinates. It then follows from the Nagell-Lutz theorem that our candidate point P must have infinite order. To accelerate this computation we can restrict the calculation to the x-coordinates with the help of the duplication formula.

Example 4.1. Consider the curve

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

We will now use the Nagell-Lutz theorem to find all points of finite order. We first set $y = 0$ and get

$$0 = x(x^2 - x + 1).$$

Thus it follows from theorem 1.1 that the point $P_1 = (0, 0)$ has order 2. For the discriminant we get $D = -3$ and it's divisors are ± 1 and ± 3. If we set $y = \pm 1$

and solve for x we find that the only integer value for x is 1, thus $P_1 = (1, 1)$ and $-P_1 = (1, -1)$ are potential points of finite order. Using the duplication formulas we get the value $2P_1 = 2(-P_1) = (0, 0)$, and since $(0, 0)$ is of order 2 it follows that P_1 and $-P_1$ have order 4.
Setting $y = \pm 3$ and solving for x we find that there are no more possible points of finite order.

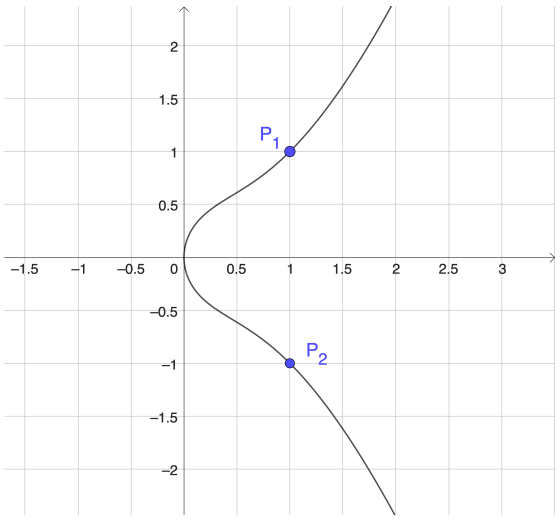

Figure 2: $C : y^2 = x^3 - x^2 + x$ with the two points of finite order $P_1 = (1, 1)$ and $P_2 = (1, -1)$

Example 4.2. Consider the curve

$$y^2 = x^3 + 8.$$

First we set $y = 0$ and get

$$0 = (x + 2)(x^2 - 2x + 4).$$

It follows from theorem 1.1 that $P_1 = (-2, 0)$ is a point of order two. By computing the discriminant, we get

$$D = -1'728 = -2^6 \cdot 3^3.$$

It follows now from the stronger version of the Nagell-Lutz theorem that the possible y-coordinates of points of finite order are $\pm 1, \pm 2, \pm 3, \pm 2^2, \pm 2 \cdot 3, \pm 2^3, \pm 2^2 \cdot 3$ and $\pm 2^3 \cdot 3$. After plugging these values into our cubic equation and solving for x, we find that the only other possible points of finite order are $P_2 = (1, 3)$, $P_3 = (2, 2^2)$ and their inverses. However by using the duplication formula we find that $x(2P_2) = x(2P_3) = -1, 75$ and therefore both P_2 and P_3 are points of infinite order.

Given the existence of points of finite order, one can ask the natural question, what orders can these points of finite order take? This question can be answered with Mazur's theorem.

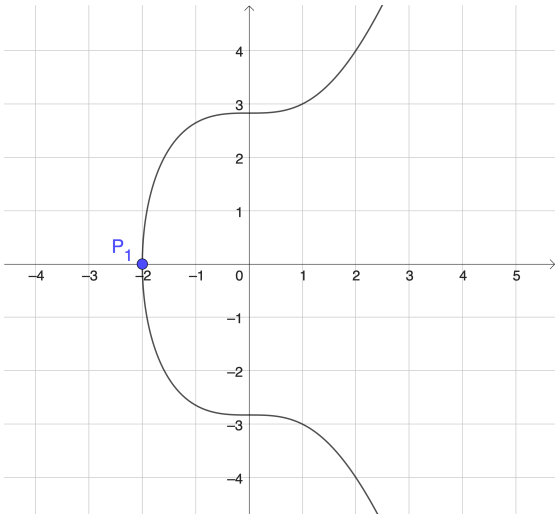

Figure 3: $C : y^2 = x^3 + 8$ with the point of finite order $P_1 = (-2, 0)$

Theorem 4.2 (Mazur's Theorem)**.** *Let C be a non-singular rational cubic curve, and suppose that $C(\mathbb{Q})$ contains a point of finite order m. Then either*

$$1 \leq m \leq 10 \quad \textit{or} \quad m = 12.$$

More precisely, the set of points of finite order in $C(\mathbb{Q})$ forms a subgroup that has one of the following forms:

1. *A cyclic group of order N with $1 \leq N \leq 10$ or $N = 12$.*
2. *The product of a cyclic group of order two and a cyclic group of order $2N$ with $1 \leq N \leq 4$.*

The proof of this theorem goes beyond the scope of this paper.

References

[1] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, Springer (1992).