Chapter 2: Points of Finite Order

Jannik Kochert, Duri Janett

October 6, 2020

1 Introduction

In this talk, we deal with points on elliptic curves that have finite order. The goal is to state the Nagell-Lutz theorem, apply it to some examples, and sketch its proof. The order of a point on an elliptic curve is the order of that point as an element of the group defined on the curve.

Definition. An element P of a group is said to have *order* m if

$$mP = \underbrace{P + P + ... + P}_{m \text{ summands}} = \mathcal{O},$$

and $m'P \neq \mathcal{O}$ for all integers $1 \leq m' < m$. If such m exists, P is said to have *finite order*, otherwise it has *infinite order*.

2 Points of Order 2 and 3

First, we want to consider only the points of small order. Note that the only point of order 1 is $\mathcal{O}$. For points of order 2 and 3, we prove the theorem below. It gives equivalent conditions to find such points, and describes the subgroup containing all points of order dividing 2 or 3, respectively.

Theorem (Points of Order 2 and 3)**.** *Let C be a non-singular cubic curve*

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

It holds:

1. *A point $P = (x, y) \neq \mathcal{O}$ on C has order 2 if and only if $y = 0$.*
2. *The curve C has exactly four points of order 1 or 2. These four points form a group that is isomorphic to $C_2 \times C_2$.*
3. *A point $P = (x, y) \neq \mathcal{O}$ on C has order 3 if and only if x is a root of the polynomial $\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2$.*
4. *The curve C has exactly nine points of order 1 or 3. These nine points form a group that is isomorphic to $C_3 \times C_3$.*

Proof. For the proof of 1, we consider a point $P = (x, y) \neq \mathcal{O}$ on C. The condition $2P = \mathcal{O}$, i.e. P is of order 2, is equivalent to $P = -P$. We also know that $-P = -(x, y) = (x, -y)$. Hence, if P has order 2, then $y = -y$. This is fulfilled if and only if $y = 0$. Conversely, if $y = 0$, then $P = -P$ and P has order 2.

From 1, we know that the points of order 2 are of the form $P = (\alpha, 0)$, where α is some root of the polynomial $f(x)$. Because C is non-singular, $f(x)$ has no double roots. As $f(x)$ has degree 3, and $\mathbb{C}$ is algebraically closed, $f(x)$ has three distinct roots in $\mathbb{C}$. Thus, there are three points of order 2. Let P_1, P_2, P_3 be these three points. Since adding two of these points always yields the third, $\{\mathcal{O}, P_1, P_2, P_3\}$ is an abelian group of order 4. There are two such abelian groups: C_4 and $C_2 \times C_2$. Since all elements in our group have order 1 or 2, the group has to be isomorphic to $C_2 \times C_2$.

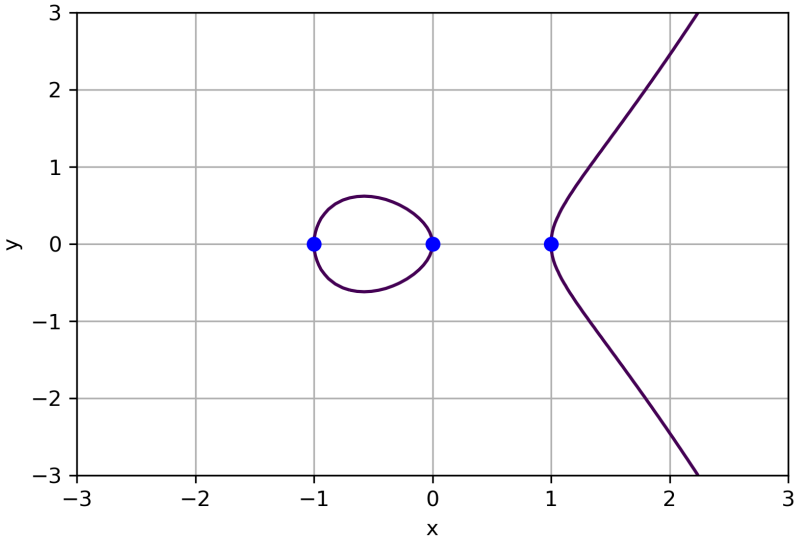

Figure 1: Plot of $C : y^2 = x^3 - x$ with points of order 2.

The following claim is needed for the proof of 3.

Claim. A point $P \neq \mathcal{O}$ is of order 3 if and only if it satisfies $x(2P) = x(P)$.

Proof. If $3P = \mathcal{O}$, i.e. P is of order 3, then $2P = -P$. From $x(P) = x(-P)$, it follows $x(2P) = x(P) = x(-P)$.
On the other hand, if $x(2P) = x(P)$, then $2P = P$ or $2P = -P$, because there are at most two points on C with the same x-coordinate. But if $2P = P$, then $P = \mathcal{O}$. So $2P = -P$, and P has order 3. ■

With the claim and the duplication formula, we get that $P = (x, y)$ has order 3 if and only if

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

First, we multiply with the denominator. Then, we subtract all terms on the left-hand side. It follows that x satisfies the condition above if and only if x is a root of

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

We have

$$\psi_3(x) = 2f(x)f''(x) - f'(x)^2. \tag{1}$$

This can be checked by an explicit calculation. Our goal is to show that $\psi_3(x)$ has four distinct roots. To achieve this, we need to verify that $\psi_3(x)$ and $\psi_3'(x)$ have no common roots. When a polynomial and its derivative have no common roots, we know from the Algebra course that the polynomial is separable. Thus, it does not have multiple roots. Since $\psi_3(x)$ has degree 4, $\psi_3(x)$ then has four distinct (complex) roots.
We calculate $\psi_3'(x)$ by deriving (1):

$$\psi_3'(x) = 2f(x)f'''(x) = 12f(x). \tag{2}$$

If $\tilde{x}$ is a root of $\psi_3'(x)$, then by (2) $f(\tilde{x}) = 0$. Plugging this result back into (1), we get $\psi_3(\tilde{x}) = -f'(\tilde{x})^2$. So if $\tilde{x}$ is a common root of $\psi_3(x)$ and $\psi_3'(x)$, then $\tilde{x}$ is a common root of $f(x)$ and $f'(x)$. This contradicts the assumption that C is non-singular. Hence, $\psi_3(x)$ and $\psi_3'(x)$ have no common roots.
Let x_1, x_2, x_3 and x_4 be the roots of $\psi_3(x)$. Put $y_i \coloneqq \sqrt{f(x_i)}$ one of the square roots for $1 \leq i \leq 4$. Now,

$$\{(x_1, y_1), (x_1, -y_1), (x_2, y_2), (x_2, -y_2), (x_3, y_3), (x_3, -y_3), (x_4, y_4), (x_4, -y_4)\}$$

is the set of elements of order 3 by 3. All of these points are distinct: We already know that $x_i \neq x_j$ for $i \neq j$. If $y_i = -y_i$, then $y_i = 0$. But then (x_i, y_i) has order 2, which is a contradiction. Together with $\mathcal{O}$, we have nine points of order 1 or 3. These points form an abelian group of order 9. There are two such abelian groups: C_9 and $C_3 \times C_3$. Since no element of our group has order 9, our group is isomorphic to $C_3 \times C_3$. ■

Figure 1 and Figure 2 depict examples of elliptic curves with points of order 2 and 3, respectively.

3 The Nagell-Lutz theorem

3.1 The Discriminant

Before we can state the Nagell-Lutz theorem, we need to define the discriminant of a cubic polynomial. But first, we want to show that we can assume that our curve is given by an equation with integer coefficients.
Let C be a curve given in its normal form

$$y^2 = f(x) = x^3 + ax^2 + bx + c, \tag{3}$$

where $a = \frac{a_1}{a_2}, b = \frac{b_1}{b_2}, c = \frac{c_1}{c_2} \in \mathbb{Q}$. Let $X = d^2x$ and $Y = d^3y$. After this substitution, the equation (3) becomes

$$Y^2 = X^3 + d^2aX^2 + d^4bX + d^6c.$$

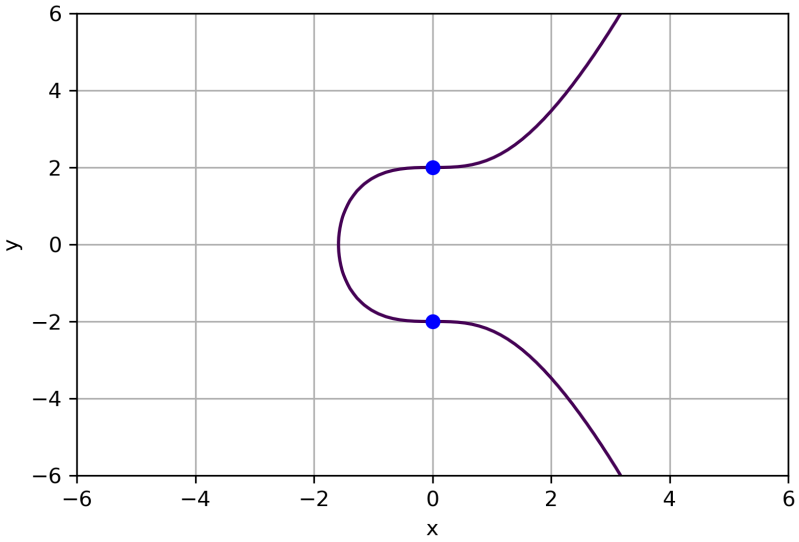

Figure 2: Plot of $C : y^2 = x^3 + 4$ with points of order 3.

Set $d = a_2 \cdot b_2 \cdot c_2$ to clear any denominators. Now, C is given by an equation with integer coefficients.

Definition. The *discriminant of* $f(x)$ is the quantity

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

The discriminant can be defined in greater generality. For the purposes of this talk, however, giving the definition by an explicit formula is sufficient, as we only deal with cubic polynomials. Notice that if we factorise $f(x)$ over $\mathbb{C}$, i.e. $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$, then the discriminant becomes

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

It follows that $D \neq 0$ if and only if C is non-singular. This explains why the Nagell-Lutz theorem will assume that C is non-singular: If $D = 0$, the conclusion that $y|D$ would always be true.

3.2 Statement of the theorem and some remarks

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

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

be a non-singular cubic curve with integer coefficients a,b,c, and let D be the discriminant of the cubic polynomial

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

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers, and either $y = 0$, in which case P has order 2, or else $y|D$.

Warning: The Nagell-Lutz theorem is not an if and only if! So it is possible to have points $P = (x, y)$ with integer coordinates and $y|D$ where P does not have finite order.
This means that we can compile a list of such points where $y \neq 0$ (points with $y = 0$ always have order 2). All points of finite order are included in the list, but to check whether a point actually has finite order we have to manually calculate $P, 2P, 3P, ...$ until we find some n with $nP = \mathcal{O}$.
In fact, it is actually easier to prove that a point has infinite order: We calculate $P, 2P, 3P, ...$ (or $P, 2P, 4P, ...$ using only the duplication formula) until we reach some point with non-integer coordinates.

Proposition. *Let P be a point of finite order. Then nP has integer coordinates for all $n \in \mathbb{Z}$.*

Proof. Let m be the order of P, so $mP = \mathcal{O}$. Assume for contradiction that there exists some $n \in \mathbb{Z}$ such that nP has non-integer coordinates. It holds that $a(mP) = \mathcal{O}\ \forall a \in \mathbb{Z}$.
Hence $\mathcal{O} = n(mP) = (nm)P = m(nP)$. This means that nP is a point of finite order. But according to Nagell-Lutz, nP must have integer coordinates. Contradiction! ■

Remark: There is a stronger version of Nagell-Lutz which states that if $P = (x, y)$ is a rational point of finite order with $y \neq 0$, then $y^2|D$ (instead of only $y|D$). This is very useful for computations, as we will see in the upcoming examples.
It can happen that, if we search for points of order 4 and above, we get infinitely many such curves:

Example. Let C be the cubic curve given by

$$y^2 = x^3 - (2t - 1)x^2 + t^2x$$

for some $t \in \mathbb{Q}$.
Then for all $t \in \mathbb{Q} \setminus \{0, \frac{1}{4}\}$, (t, t) is a point of order 4.

Proof. Let $t \in \mathbb{Q} \setminus \{0, \frac{1}{4}\}$. If we plug (t, t) into the curve equation we get:

$$t^2 = t^3 - (2t - 1)t^2 + t^3 = t^3 - 2t^3 + t^2 + t^3 = t^2$$

Hence the point (t, t) is actually lying on our curve.
Now, by using the point duplication formula, we get:

$$x' = \frac{t^4 - 2t^4 + t^4}{4t^3 - 8t^3 + 4t^2 + 4t^3} = \frac{0}{4t^2} = 0$$

Plugging our x'-coordinate into our curve we instantly get $y'^2 = 0$, hence $y' = 0$.
So we get $2(t, t) = (0, 0)$. Hence we conclude that $4(t, t) = \mathcal{O}$.
Now consider the case $t = 0$. For this case our curve equation turns into

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

Using the point duplication formula again we get:

$$x' = \frac{0}{4} = 0$$

From this we get again that $y' = 0$. Hence $2(0,0) = (0,0)$. But this means that $nP = 0$ for all $n \in \mathbb{N}$, hence $(0,0)$ has infinite order. With $t = \frac{1}{4}$, we get a similar problem. ■

3.3 Examples

Definition. $C(\mathbb{Q})_{tor} := \{P \in C(\mathbb{Q}) \mid P \text{ is of finite order}\}$ is called the *torsion subgroup* of $C(\mathbb{Q})$.

Proposition. *$C(\mathbb{Q})_{tor}$ is a subgroup of $C(\mathbb{Q})$.*

Proof. $\mathcal{O}$ has order 1, hence $\mathcal{O} \in C(\mathbb{Q})_{tor}$. Now consider $P, P' \in C(\mathbb{Q})_{tor}$. Then there exist $n, m \in \mathbb{N}$ such that $nP = mP' = \mathcal{O}$. Let $l := m \cdot n$. Then

$$l(P + P') = lP + lP' = m(nP) + n(mP) = \mathcal{O} + \mathcal{O} = \mathcal{O}$$

Hence $P + P' \in C(\mathbb{Q})_{tor}$. Lastly consider $P \in C(\mathbb{Q})_{tor}$. Then there exists some $n \in \mathbb{N}$ such that $nP = \mathcal{O}$. But then also $n(-P) = -nP = -\mathcal{O} = \mathcal{O}$, so $-P \in C(\mathbb{Q})_{tor}$. Hence $C(\mathbb{Q})_{tor}$ is a subgroup. ■

Example. Consider the cubic curve given by

$$C: \ y^2 = x^3 - 2$$

Find the points of finite order and determine $C(\mathbb{Q})_{tor}$.

From the Nagell-Lutz theorem we know that the points of order 2 are exactly the zeroes of $x^3 - 2$. Hence our only candidate for a point of order two is $(\sqrt[3]{2}, 0)$. But $\sqrt[3]{2}$ is not an integer, hence this is not a point of finite order.
As explained in the last section, we can now compile a list of rational points $P = (x, y)$ where y divides the discriminant: Our curve has coefficients $a = 0, b = 0, c = -2$, which means that $D = -108 = -2^2 \cdot 3^3$.
This gives us the following list of possible candidates for y:

$$y \in \{1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108\}$$

But, using the stronger version of Nagell-Lutz, we can only pick those where y^2 divides D, resulting in a smaller list:

$$y \in \{1, 2, 3, 6\}$$

We calculate the x-coordinates of these four points:

$$1 = x^3 - 2 \iff x = \sqrt[3]{3} \notin \mathbb{Z}$$

$$4 = x^3 - 2 \iff x = \sqrt[3]{6} \notin \mathbb{Z}$$

$$9 = x^3 - 2 \iff x = \sqrt[3]{11} \notin \mathbb{Z}$$

$$36 = x^3 - 2 \iff x = \sqrt[3]{38} \notin \mathbb{Z}$$

Unfortunately, we now have to conclude that the curve C actually has no (non-trivial) points of finite order, hence we get $C(\mathbb{Q})_{tor} = \{\mathcal{O}\} \cong \{1\}$.

Example. Consider the cubic curve given by

$$C: \ y^2 = x^3 + 8$$

Find the points of finite order and determine $C(\mathbb{Q})_{tor}$.

We proceed analogously to above and first check whether there exist any points of order 2:

$$0 = x^3 + 8 \iff x = \sqrt[3]{-8} = -2 \in \mathbb{Z}$$

Here we have actually found a point of order 2.
We again compile a list of possible candidates for y, but now knowing that y^2 must divide D. Our curve has coefficients $a = 0, b = 0, c = 8$, which means that $D = -1728 = -3^3 \cdot 2^6$.
This gives us the following list of possible candidates for y:

$$y \in \{1, 2, 3, 4, 6, 8, 12, 24\}$$

We calculate the x-coordinates of these four points:

$$1 = x^3 + 8 \iff x = \sqrt[3]{-7} = -\sqrt[3]{7} \notin \mathbb{Z}$$

$$4 = x^3 + 8 \iff x = \sqrt[3]{-4} = -\sqrt[3]{4} \notin \mathbb{Z}$$

$$9 = x^3 + 8 \iff x = \sqrt[3]{1} = 1 \in \mathbb{Z}$$

$$16 = x^3 + 8 \iff x = \sqrt[3]{8} = 2 \in \mathbb{Z}$$

$$36 = x^3 + 8 \iff x = \sqrt[3]{28} \notin \mathbb{Z}$$

$$64 = x^3 + 8 \iff x = \sqrt[3]{56} \notin \mathbb{Z}$$

$$144 = x^3 + 8 \iff x = \sqrt[3]{136} \notin \mathbb{Z}$$

$$576 = x^3 + 8 \iff x = \sqrt[3]{568} \notin \mathbb{Z}$$

We have actually found two more candidates, namely $P_{1,2} := (1, \pm 3)$ and $P_{3,4} := (2, \pm 4)$. We now calculate $2P_{1,2}$ and $2P_{3,4}$:

$$x(2P_{1,2}) = \frac{1(-63)}{36} = -\frac{7}{4} \notin \mathbb{Z}$$

$$x(2P_{3,4}) = \frac{2(8-64)}{4(8+8)} = -\frac{7}{4} \notin \mathbb{Z}$$

Hence we have found multiples of $P_{1,2,3,4}$ which have non-integer coordinates, and by the previous section this means that they cannot be points of finite order!
We conclude that the only (non-trivial) point of finite order is $P := (-2, 0)$. Hence $C(\mathbb{Q})_{tor} = \{\mathcal{O}, P\} \cong \mathbb{Z}/2\mathbb{Z}$.

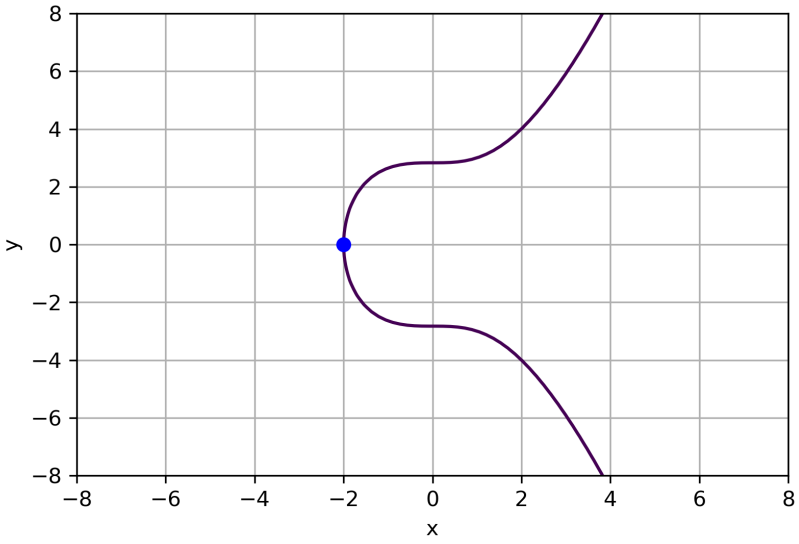

Figure 3: $C: \ y^2 = x^3 + 8$ with point P of order 2

4 Proof of the Nagell-Lutz theorem

4.1 Discriminant Lemma

With the following lemma, we show the second part of the conclusion of the Nagell-Lutz theorem.

Lemma. *Let $P = (x, y)$ be a point on C such that both P and $2P$ have integer coordinates. Then either $y = 0$ or $y|D$.*

Note that the additional assumption that $2P$ has integer coordinates follows immediately from the first part of the conclusion of the Nagell-Lutz theorem: If P is a rational point of finite order, then $2P$ is a rational point of finite order as well. Hence, $2P$ has integer coordinates.

Proof. For the proof of the lemma, we need the following claim.

Claim. There are polynomials $r(X), s(X) \in \mathbb{Z}[X]$, such that we have

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

Proof. Similarly to how we only gave the definition of the discriminant for the special case that interests us, we will show this claim with an explicit calculation.

$$D = \underbrace{((18b - 6a^2)X - (4a^3 - 15ab + 27c))}_{r(X)} f(X)$$
$$\underbrace{-((2a^2 - 6b)X^2 + (2a^3 - 7ab + 9c)X + (a^2b + 3ac - 4b^2))}_{s(X)} f'(X).$$

■

Assume $y \neq 0$ (otherwise, there is nothing to prove). Then, by the theorem on points of order 2 and 3, $2P \neq \mathcal{O}$. So we can put $2P = (X, Y)$. By the duplication formula, we have

$$2x + X = \lambda^2 - a,$$

where $\lambda \coloneqq \frac{f'(x)}{2y}$. As x, X, and a are integers, it follows $\lambda^2 \in \mathbb{Z}$ and thus $\lambda \in \mathbb{Z}$. As $2y$ and $f'(x)$ are integers, we have $2y|f'(x)$ (see the definition of λ), which implies $y|f'(x)$. Additionally, $y^2 = f(x)$, so in particular $y|f(x)$. By the claim, $D = r(x)f(x) + s(x)f'(x)$. Thus, it follows that $y|D$. ■

4.2 Order, $C(p^\nu)$ and R

Definition. Let $x \in \mathbb{Q}$ and let p be prime. If $x \neq 0$, there are unique $m, n, \nu \in \mathbb{Z}$, $n \geq 1$, such that $x = \frac{m}{n}p^\nu$, where $\frac{m}{n}$ is in lowest terms and p does not divide m and n.
The *order of x (with respect to p)* is defined to be the exponent ν,

$$\mathrm{ord}_p(x) \coloneqq \mathrm{ord}_p(\frac{m}{n}p^\nu) \coloneqq \nu,$$

By convention, $\mathrm{ord}_p(0) = \infty$.

To highlight the importance of the chosen prime p, we calculate for $\frac{2}{3}$:

$$\mathrm{ord}_2(\frac{2}{3}) = \mathrm{ord}_2(\frac{1}{3}2^1) = 1.$$
$$\mathrm{ord}_3(\frac{2}{3}) = \mathrm{ord}_3(\frac{2}{1}3^{-1}) = -1.$$
$$\mathrm{ord}_5(\frac{2}{3}) = \mathrm{ord}_5(\frac{2}{3}5^0) = 0.$$

For the next definition, we want to give some motivation. Let $P = (x, y) \in C(\mathbb{Q})$ be a rational point on the curve C. Assume that p divides the denominator of x. We write

$$x = \frac{m}{np^\mu}, \qquad y = \frac{u}{wp^\sigma}, \tag{4}$$

where $m, n, \nu, u, w, \sigma \in \mathbb{Z}$. Note that $\mu > 0$. Additionally, we assume that p does not divide m, n, u, and w. We get $2\sigma = 3\mu$ by plugging (4) into the Weierstrass equation of our curve and comparing the orders of both sides. In particular, p divides the denominator of y. The converse statement can be shown with a similar argument. Let us fix $\nu \in \mathbb{Z}$, $\nu > 0$, such that

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

Note that if p appears in the denominator of x or y, it appears in the denominators of both x and y. The exact powers are $p^{2\nu}$ and $p^{3\nu}$ for x and y, respectively.

Definition. We define

$$C(p^\nu) \coloneqq \{(x, y) \in C(\mathbb{Q}) : \mathrm{ord}_p(x) \leq -2\nu \text{ and } \mathrm{ord}_p(y) \leq -3\nu\} \cup \{\mathcal{O}\}.$$

It holds

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

Definition. We define for p prime

$$R := R_p := \{q = \frac{x}{y} \in \mathbb{Q} \mid p \text{ does not divide } y\}.$$

It can be checked that R is a ring. Moreover, R is actually a unique factorization ring which only has one maximal ideal, namely the ideal (p). We can also write R as

$$R = \{\alpha \in \mathbb{Q} \mid ord_p(\alpha) \geq 0\}$$

The units in R are the rational numbers of order 0, i.e. numbers where p divides neither numerator nor denominator.

4.3 Proposition

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

1. *$C(p)$ consists of all rational points (x, y) for which the denominator of either x or y is divisible by p.*
2. *For every $\nu \geq 1$, the set $C(p^\nu)$ is a subgroup of the group of rational points $C(\mathbb{Q})$.*
3. *The map*

$$\frac{C(p^\nu)}{C(p^{3\nu})} \to \frac{p^\nu R}{p^{3\nu} R}$$

$$P = (x, y) \mapsto t(P) = \frac{x}{y}$$

is a one-to-one homomorphism. (By convention, we send $\mathcal{O} \mapsto 0$.)

The proof of the first part was done in section 2.

Proof of Part 2: To prove the second part of the proposition we first introduce a change of coordinates: Let $t := \frac{x}{y}$, $s := \frac{1}{y}$. The intuitive way of understanding this change is the following: The point at infinity $\mathcal{O}$ is moved to the origin $(0, 0)$ while all points with $y = 0$ get moved to infinity. All other points get mapped bijectively between the (x, y) and the (t, s) coordinates.
A quick calculation shows us that lines in (x, y) are also lines in (t, s), hence we can add points in the (t, s) coordinate system in the same way as in the (x, y) coordinate system. Also, it holds that

$$(t, s) \in C(p^\nu) \iff t \in p^\nu R,\ s \in p^{3\nu} R$$

Now let p be prime and $\nu \geq 1$.

Claim. $C(p^\nu)$ is a group

Proof (Sketch). We only provide a sketch of the proof: By convention it holds that $\mathcal{O} \in C(p^\nu)$. Let $P_1 = (t_1, s_1), P_2 = (t_2, s_2) \in C(p^\nu)$. To show that $P_3 = (t_3, s_3) := P_1 + P_2$ is in $C(p^\nu)$, we show that if p divides t_1 and t_2, then p must also divide t_3, which takes some calculations. We then show that if $p^{3\nu}$ divides s_1 and s_2, then p must also divide s_3.
Now let $P = (t, s) \in C(p^\nu)$. If p divides t, then p also divides $-t$, and if $p^{3\nu}$ divides s, then it also divides $-s$, hence $-P = (-t, -s)$ is in $C(p^\nu)$. ■

With the second part proven, we now need to prove the third part.

Proof of Part 3: We want to prove that the map

$$\frac{C(p^\nu)}{C(p^{3\nu})} \to \frac{p^\nu R}{p^{3\nu} R}$$

$$P = (x, y) \mapsto t(P) = \frac{x}{y}$$

is an isomorphism. For that we consider a statement from the omitted part of the proof of part 2:

$$t(P_1 + P_2) \equiv t(P_1) + t(P_2) \ (mod\ p^{3\nu}) \tag{5}$$

From this we get a well-defined homomorphism $\phi : C(p^\nu) \to \frac{p^\nu R}{p^{3\nu} R}$ with $\phi : P \mapsto [t(P)]$ where $[t(P)]$ is the equivalence class under $\equiv$. The kernel of ϕ consists of all points with $t(P) \in p^{3\nu} R$, and the image of ϕ is the whole of $\frac{p^\nu R}{p^{3\nu} R}$. Hence, by the homomorphism theorem, we can conclude the statement. ■

4.4 Finishing the proof

After having proven the main proposition, we can finally move on to the Corollary that proves the final statement of the Nagell-Lutz theorem:

Corollary. *1. For every prime p, the only point of finite order in the group $C(p)$ is the identity point $\mathcal{O}$.*

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

Proof. First we prove 1.: Let $P \in C(\mathbb{Q})$ be a point of order m, $P \neq \mathcal{O}$, p a prime number. We want to show that $P \notin C(p)$. Assume for contradiction that $P \in C(p)$. Because $P = (x, y)$ is a finite point, there cannot exist arbitrarily large powers of p dividing the denominator of x. Hence we can find some $\nu > 0$ such that $P \in C(p^\nu)$ but $P \notin C(p^{\nu+1})$. Subsequently, because $C(p^{\nu+1}) \supset C(p^{\nu+2}) \supset ...$ we also get $P \notin C(p^{\nu+d})$ for any $d \in \mathbb{N}$.
We have to do a case distinction between the cases $p \nmid m$ and $p \mid m$, where we can actually reduce the second case to the first one. If we apply formula (5) repeatedly to the same point P, we get

$$t(mP) \equiv mt(P) \ (mod\ p^{3\nu})$$

So

$$0 = t(\mathcal{O}) = t(mP) \equiv mt(P) \ (mod\ p^{3\nu})$$

p does not divide m, so we conclude $t(P) \equiv 0 \ (mod\ p^{3\nu})$. But this shows that $P \in C(p^{3\nu})$. $3\nu > \nu$, hence we get a contradiction.
Now, to prove 2., assume $P = (x, y) \in C(\mathbb{Q})$ to be a rational point of finite order. Then, according to 1., $P \notin C(p)$ for any prime p. This means that the denominators of both x and y are not divisible by any prime number p, hence they must be equal to 1. This finally shows $x, y \in \mathbb{Z}$. ■

4.5 Mazur's Theorem

To show that the research on points of finite order on elliptic curves is far more extensive than what we have covered in this section, we state one important theorem concerning that topic:

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

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

More precisely, $C(\mathbb{Q})_{tor}$ forms a subgroup that has one of the following forms:

1. C_N *for* $1 \leq N \leq 10$ *or* $N = 12$
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ *with* $1 \leq N \leq 4$.

References

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

[2] R. Tandon, *Elliptic Curves, Modular Forms and Cryptography (pp. 49-61)*, Hindustan Book Agency (2003).