Seminar on Elliptic Curves: Points of Finite Order

Jannik Kochert, Duri Janett

ETH Zurich

October 6, 2020

Overview

1. Points of order 2 and 3
2. Nagell-Lutz theorem: statement and examples
3. Nagell-Lutz theorem: sketch of the proof

Points of order 2 and 3

Definition

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

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

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*.

Points of order 2 and 3

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 $y = 0$.*

Points of order 2 and 3

Proof.

We have

$$2P = \mathcal{O} \iff P = -P.$$

Since

$$-P = -(x, y) = (x, -y),$$

the conclusion follows.

□

Points of order 2 and 3

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 $C_2 \times C_2$.*

Points of order 2 and 3

Proof.

From 1, we know that the points of order 2 are of the form

$$P_1 = (\alpha_1, 0), P_2 = (\alpha_2, 0), P_3 = (\alpha_3, 0),$$

where α_1, α_2, α_3 are the roots of the polynomial $f(x)$.
Because C is non-singular, $f(x)$ has three distinct roots in $\mathbb{C}$ and thus three points of order 2.
$\{\mathcal{O}, P_1, P_2, P_3\}$ form an abelian group of order 4, which has to be isomorphic to $C_2 \times C_2$, since all elements are of order 1 or 2. □

Points of order 2 and 3

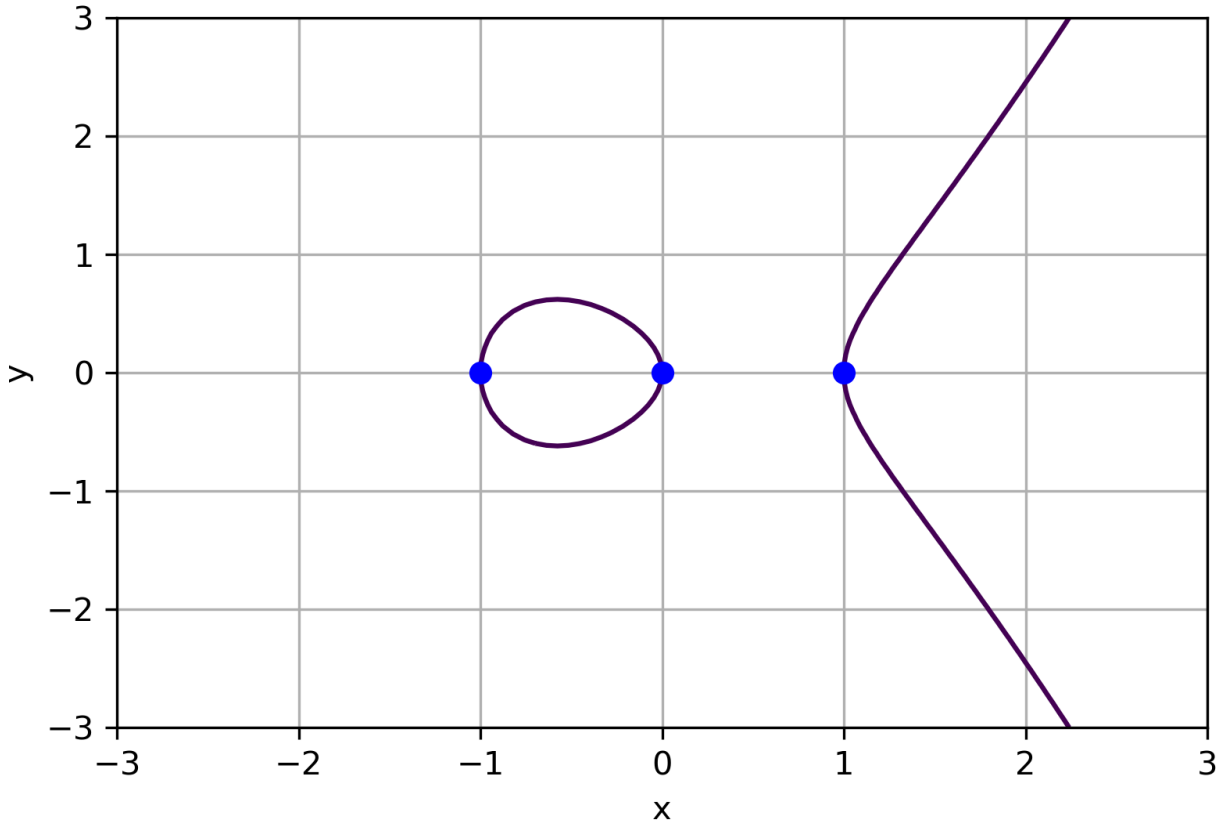


Figure: Plot of $C : y^2 = x^3 - x$

Points of order 2 and 3

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

Points of order 2 and 3

Proof.

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

$$3P = \mathcal{O} \iff 2P = -P.$$

Because $x(P) = x(-P)$, the first direction of the claim follows.
For the other direction, note that if $x(2P) = x(P)$, then $2P = P$ or $2P = -P$.

Points of order 2 and 3

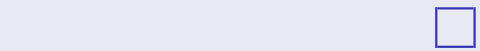
Proof. (Cont.)

It follows with the duplication formula

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

which is equivalent to x being a root of

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



Points of order 2 and 3

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 $C_3 \times C_3$.*

Points of order 2 and 3

Proof.

We have

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

We want to show that $\psi_3(x)$ has four distinct roots. So we check that $\psi_3(x)$, $\psi_3'(x)$ have no common roots.

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

so if $\tilde{x}$ is a common root of $\psi_3(x)$, $\psi_3'(x)$, then $\tilde{x}$ is a common root of $f(x)$, $f'(x)$, which contradicts the assumption that C is non-singular.

Points of order 2 and 3

Proof. (Cont.)

Let x_1, x_2, x_3 and x_4 be the roots of $\psi_3(x)$. Put $y_i = \sqrt{f(x_i)}$ one of the square roots.

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

is the set of the elements of order three.
All of the points are distinct.
Together with $\mathcal{O}$ (the only point of order 1), we have nine points of order 1 or 3. These points form an abelian group of order 9, which has to be isomorphic to $C_3 \times C_3$, since all elements are of order 1 or 3. $\square$

Points of order 2 and 3

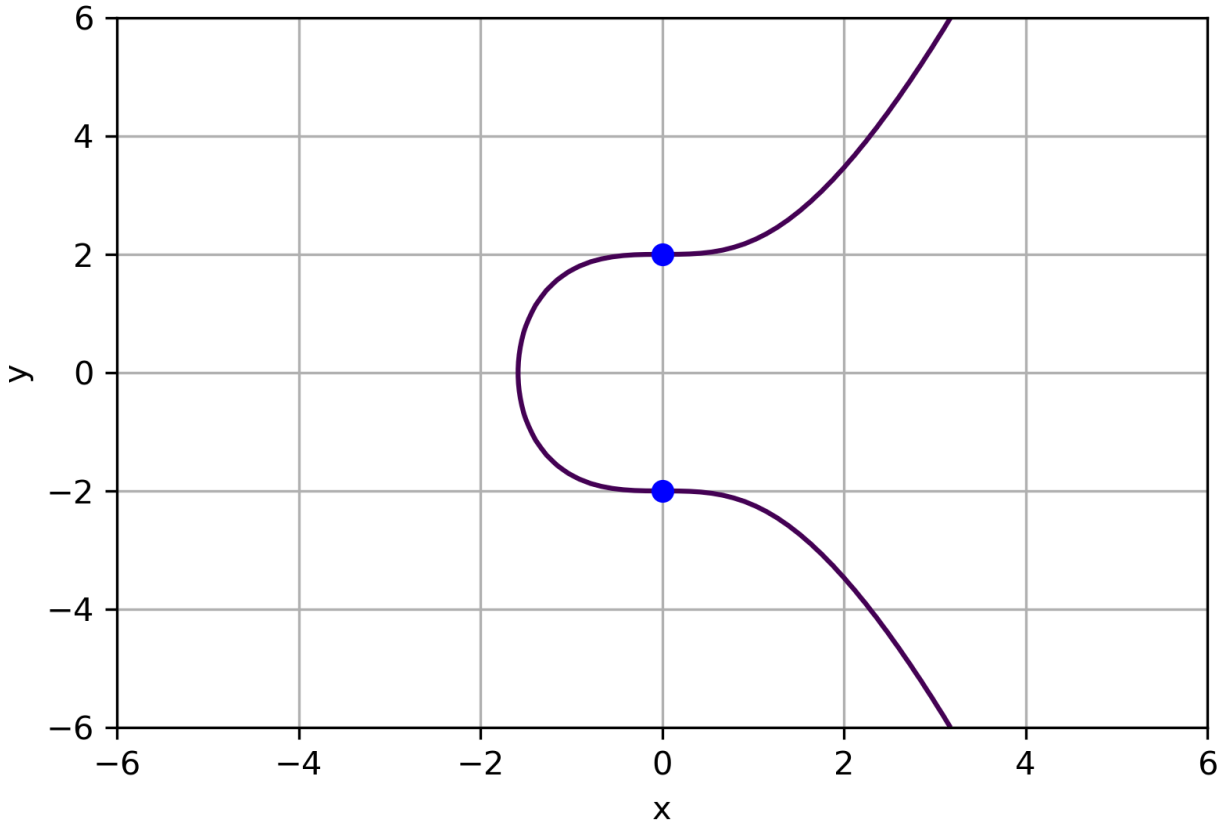


Figure: Plot of $C : y^2 = x^3 + 4$

The discriminant

Let C be a curve given in its normal form

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

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 becomes

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

Set $d = a_2 \cdot b_2 \cdot c_2$ to clear any denominators.
From now on we will assume that our cubic curve is given by an equation with integer coefficients.

The discriminant

Definition

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

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

If we factor f over $\mathbb{C}$,

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

we can write the discriminant as follows:

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

It follows that $D \neq 0$ if and only if C is non-singular.

The Nagell-Lutz Theorem

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 $y|D$.

The Nagell-Lutz Theorem: Remarks

- Warning: The Nagell-Lutz Theorem is not an iff! It is possible that there exist points with integer coordinates $P = (x, y)$ with $y|D$ but P is not of finite order!
- It is easier to prove that a point has infinite order.

The Nagell-Lutz Theorem: Remarks

- 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 $y | D$).
- If we search for points of order 4 and above, we can often get infinitely many curves with points of such order.

Example

Let C be the cubic curve given by

$$y^2 = x^3 - (2t - 1)x^2 + t^2 x \text{ for some } t \in \mathbb{Q}.$$

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

The Nagell-Lutz Theorem: Example 1

Definition

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

Example

Let C be the cubic curve given by

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

Determine all points of finite order and find $C(\mathbb{Q})_{tor}$.

The Nagell-Lutz Theorem: Example 1

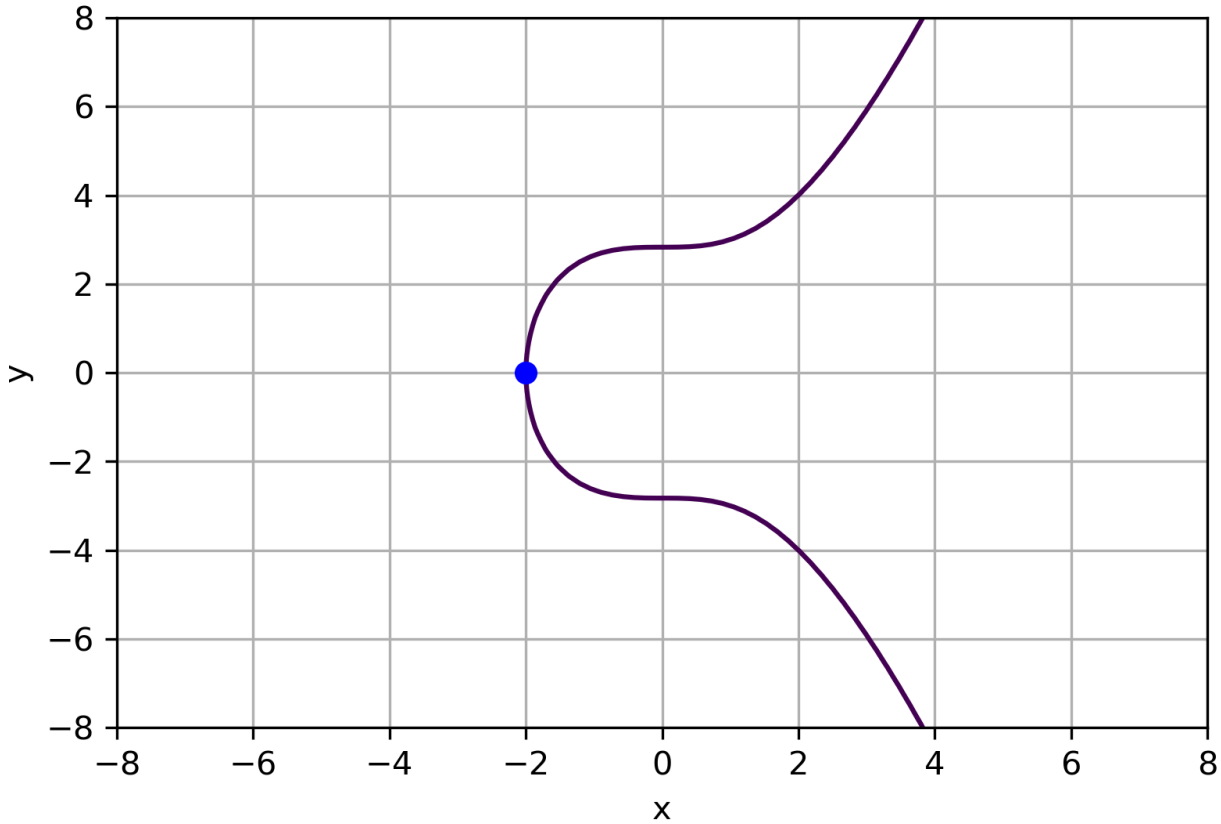


Figure: Plot of $C : y^2 = x^3 + 8$

The Nagell-Lutz Theorem: Example 2

Example

Let C be the cubic curve given by

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

Determine all points of finite order and find $C(\mathbb{Q})_{tor}$.

Proof of the Nagell-Lutz Theorem: Overview

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 $y|D$.*

Proof of the Nagell-Lutz Theorem: Discriminant Lemma

Lemma

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

Remark.

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 of the Nagell-Lutz Theorem: Discriminant Lemma

Proof.

Assume $y \neq 0$. Then $2P \neq \mathcal{O}$. Put $2P = (X, Y)$.
By the duplication formula, we have

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

where $\lambda = \frac{f'(x)}{2y}$. It follows $\lambda \in \mathbb{Z}$.
As $2y, f'(x) \in \mathbb{Z}$, we have $2y | f'(x)$ which implies $y | f'(x)$.
Additionally, $y^2 = f(x)$, so $y | f(x)$.
By the remark, $D = r(x)f(x) + s(x)f'(x)$, and $y | D$ follows. □

Proof of the Nagell-Lutz Theorem: Some definitions

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,

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

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

Proof of the Nagell-Lutz Theorem: Some definitions

Let $P = (x, y) \in C(\mathbb{Q})$. Assume p divides the denominator of x. Write

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

Then $2\sigma = 3\mu$, so in particular, p divides the denominator of y.
The converse statement is also true. Choose $\nu \in \mathbb{Z}$, $\nu > 0$, such that

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

Proof of the Nagell-Lutz Theorem: Some definitions

Definition

We define

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

We have

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

The ring R_p

Definition

We define for p prime

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

- R is a ring
- $R = \{\alpha \in \mathbb{Q} \mid ord_p(\alpha) \geq 0\}$
- The units in R are the rational numbers of order 0, i. e. where p neither divides numerator nor denominator

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 $\mathcal{O} \mapsto 0$.)

Proof of Proposition (1)

- **Part 1**: Just done
- Change of coordinates: $t := \frac{x}{y}, s := \frac{1}{y}$.
- New equation: $s = t^3 + at^2s + bts^2 + cs^3$
- Analogous addition in (t,s)
- $(t, s) \in C(p^\nu) \iff t \in p^\nu R,\ s \in p^{3\nu} R$

Proof of Proposition (2)

- **Part 2**: Show that $C(p^\nu)$ is a subgroup
- $\mathcal{O} \in C(p^\nu)$
- $P_1 \in C(p^\nu)$, $P_2 \in C(p^\nu) \implies P_1 + P_2 \in C(p^\nu)$
- $P_1 \in C(p^\nu) \implies -P_1 \in C(p^\nu)$

Proof of Proposition (3)

- **Part 3**: Show that this map is an isomorpism:

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

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

- $t(P_1 + P_2) \equiv t(P_1) + t(P_2) \ (mod \ p^{3\nu})$
- Quotient + Homomorphism theorem

Corollary

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 of Corollary

- **(a)**:
- $P \in C(\mathbb{Q})$ of order m, $P \neq \mathcal{O}$, p prime. We want to show: $P \notin C(p)$
- Find $\nu > 0$ s. t. $P \in C(p^\nu)$ and $P \notin C(p^{\nu+1})$.
- $t(mP) \equiv mt(P)\ (mod\ p^{3\nu})$
- $P \in C(p^{3\nu})$, contradiction.
- **(b)**: Use (a).

Mazur's theorem

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

- Silverman and Tate, *Rational points on elliptic curves (pp. 35-64)*, Springer 2015.
- R. Tandon, *Elliptic Curves, Modular Forms and Cryptography (pp. 49-61)*, Hindustan Book Agency (India) 2003.