Rational Points on Elliptic Curves

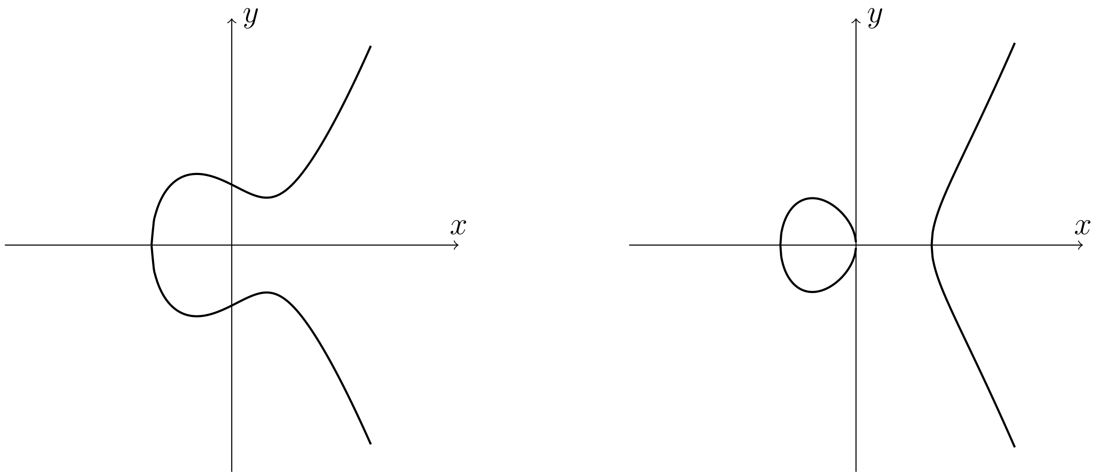
Heidi Lei

1 Introduction

Elliptic curves are non-singular cubic curves commonly in the form

$$y^2 = x^3 + ax^2 + b^x + c.$$

Figure 1.1 gives two examples of what an elliptic curve might look like when plotted in $\mathbb{R}^2$. It is in one connected piece if the cubic in x has one real root, and in two connected pieces if it has three real roots.



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

(b) $y^2 = x^3 - x$

Figure 1.1: Examples of elliptic curves.

Elliptic curves are particularly useful in number theory since elliptic curves over the rationals are related to modular forms, and they are involved in the proof of Fermat's last theorem through a form of the modularity theorem. Elliptic curves also have important cryptographic uses since an operation can be defined on the points of an elliptic curve, and there is an analog of the discrete log problem on the points under this operation. Compared to public-key encription algorithms based on the structure of the multiplicative group $\mathbb{Z}/p\mathbb{Z}^\times$, the keys using elliptic curve cryptography are much smaller in size.

In this paper, we prove some basic results concerning the structure of rational points on an elliptic curve mainly following the exposition of [2]. We first analyze rational points on conic curves to gain some intuition, then we build up the necessary tools for the main results of this paper, the Nagell-Lutz theorem, which lets us compute the torsion group of rational points, and Mordell's theorem, which states that the group of rational points is finitely generated.

2 Rational Points on Conics

Before we dive into elliptic curves, we will first look at rational points on conics, i.e., curves of degree 2 with the general formula

$$ay^2 + bxy + cx^2 + dx + ey + f = 0,$$

which gives us some insights on how rational points behave on a curve. If all the coefficients of the curve $a, \dots, f$ are rational, then we refer to the curve C as a rational conic. We are interested in the rational points on a rational conic.

We have a complete characterization of rational points on conics in the sense that we can check in finite steps whether there exists a rational point, and if so, we can represent all rational points on thee conic with a closed-form parametrization.

2.1 Conics with a Known Rational Point

The principal idea we develop in this section is that if we have one rational point on the conic, then in fact we have infinitely many of them. The rational points on the conic can tbe parametrized by projecting the conic onto the a rational line.

We assume that the conic C contains a rational point $\mathcal{O}$. Let l be a rational line. Then we can establish a correspondence between rational points on the conic C and rational points on the line l. We project C onto l through the point $\mathcal{O}$ as shown in Figure 2.1, i.e., let P be a point on C, then its projection P' onto l is given by the intersection of l with the line passing through $\mathcal{O}$ and P. There are a couple special points that we need to take care of. The point $\mathcal{O}$ itself is projected onto l using the line that is tangent to C at $\mathcal{O}$. The point at which the line passing through it and $\mathcal{O}$ is parallel to l is mapped onto their intersection at the point at infinity. (We often operate in the projective space for the benefit that two lines always intersect and curves have a "correct" number of intersections according to their degrees.) Conversely, if we have a point Q on the line l, then its corresponding point Q' on C is given by the intersection of C with the line passing through $\mathcal{O}$ and Q, which exists since a line intersects a cubic at two points generally.

Now that we have a bijective mapping between points on the conic and the line, we simply need to demonstrate that this map is also a correspondence of rational points. If P is a rational point on C, then the line passing through $\mathcal{O}$ and P is a rational line. It is easy to see that the intersection of two rational lines is indeed rational, so P' is a rational point on l. Conversely, if Q is a rational point on l, then the line passing through $\mathcal{O}$ and Q is a rational line. Since the coordinate of the intersection of a rational line and a rational conic is given by a quadratic with rational coefficients and its roots come in conjugate pairs. Since one of the intersection $\mathcal{O}$ is rational, then the other intersection Q' must also be rational.

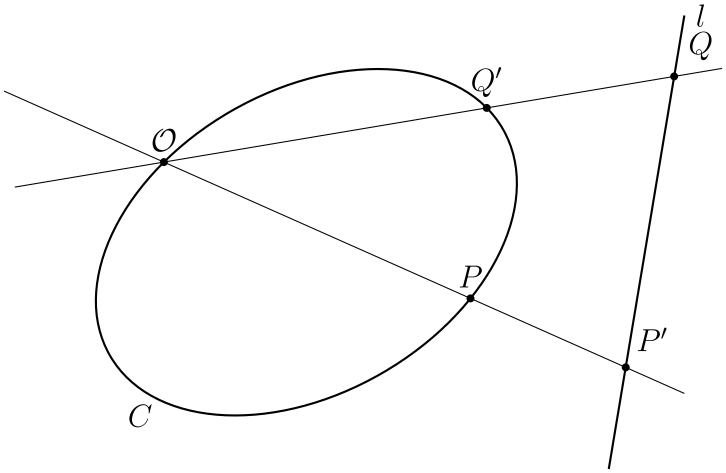


Figure 2.1: Projecting a conic onto a line through a point $\mathcal{O}$

Since the rational points on the line can be easily parametrized with one of the coordinates, we have obtained a parametrization of rational points on a conic. We demonstrate this procedure on a circle.

Example. Consider a circle given by the equation

$$x^2 + y^2 = 1.$$

We project the points on the circle from the point $(-1, 0)$ to the y-axis parametrized by $\{(0, t)\}$ as shown in Figure 2.2.

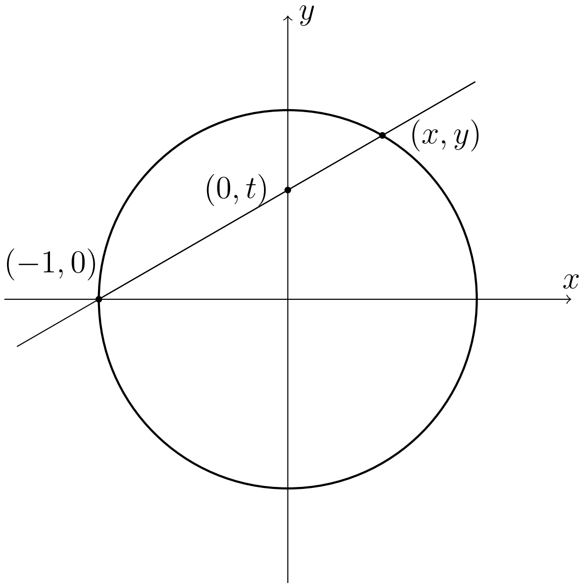


Figure 2.2: Rational points on the circle $x^2 + y^2 = 1$.

The line passing through (-1.0) and $(0, t)$ is given by $y = t(x + 1)$. Since the point (x, y) lies both on the line and on the circle, we have the relationship

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

Since one of the intersections of the line and the circle is $(-1, 0)$, we factor out $(x+1)$ from both sides,

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

Solving for x and using $y = t(x+1)$ to solve for y gives

$$x = \frac{1-t^2}{1+t^2}, \quad y = \frac{2t}{1+t^2},$$

and we have arrived at a rational parametrization of the circle.

2.2 Existence of Rational Points on Conics

In the previous section, we showed how we can parametrize the infinite family of rational points on a conic curve given the existence of one rational point. Now, we investigate the conditions the conic needs to satisfy to contain a rational point.

The general idea is given by Hasse's local-global principle, which states that certain families of equations have solutions in the rational numbers if and only if solutions exist in the real numbers and the p-adic numbers for each prime p.

In our specific case, we can first reduce the conic to a general form

$$ax^2 + by^2 + cz^2 = 0, \quad abc \neq 0, \quad a, b, c \text{ pairwise relatively prime and squarefree}$$

by homogenization and a change of variables through diagonalization. (See [1] for a complete process.) Then, the existence of a rational solution can be determined by Legendre's theorem, and we give a proof of it using elementary number theory.

Theorem 2.1 (Legendre)**.** *The homogeneous quadratic equation $ax^2 + by^2 + cz^2 = 0$ with nonzero, squarefree, and pairwise relatively prime coefficients $a, b, c \in \mathbb{Z}$ has a nontrivial integer solution if and only if*

(1) a, b, c do not share the same signs.

(2) $-ab \mod c, -bc \mod a, -ac \mod b$ are squares.

Remark. Condition (1) corresponds to solutions in the real numbers in Hasse principle, while condition (2) corresponds to solutions in the p-adic numbers.

Proof. $\Rightarrow$ (Necessity):

(1) If a, b, c have the same signs, then the only solution to the equation is the trivial solution $x = y = z = 0$.

(2) We show that $-ab$ is a square mod c, and the other conditions can be shown similarly by symmetry. It suffices to show that $-ab$ is a square mod p for some $p \mid c$, as the rest follows by the Chinese remainder theorem.

Let (x, y, z) be a nontrivial integer solution to $ax^2+by^2+cz^2 = 0$. Since the equation is homogeneous, we can take $\gcd(x, y, z) = 1$. Furthermore, x, y, z are pairwise relatively prime: Let d be a common divisor of x and y, then $d^2 \mid ax^2 + by^2$, which implies that

$d^2 \mid cz^2$. Since c is squarefree, we have $d \mid z$. Since $\gcd(x, y, z) = 1$, we must have $d = 1$, so $\gcd(x, y) = 1$, and we have shown that x, y, z are pairwise relatively prime.

Reducing the equation modulo p, where $p \mid c$, we have $ax^2 + by^2 \equiv 0 \mod p$. Since $\gcd(x, y) = 1$, p does not divide both x and y. Wlog we have $p \nmid x$. Then, rearranging the equation and multiplying by $-b$, we have

$$a \equiv -\frac{by^2}{x^2} \mod p \quad \Rightarrow \quad -ab \equiv \frac{b^2y^2}{x^2} \mod p.$$

$-ab$ is a square mod p as claimed.

$\Leftarrow$ (Sufficiency):

Since a, b, c do not share the same sign, assume that $a > 0$ and $b, c < 0$. If $|abc| = 1$, then the conic $x^2 - y^2 - z^2$ has the nontrivial solution $(1, 1, 0)$, so assume that $|abc| > 1$. Since $-bc \equiv k^2 \mod a$, the polynomial $ax^2 + by^2 + cz^2$ splits into linear factors over $\mathbb{Z}/a\mathbb{Z}$:

$$\begin{aligned} ax^2 + by^2 + cz^2 &\equiv by^2 + cz^2 \\ &\equiv b\left(y^2 + \frac{c}{b}z^2\right) \\ &\equiv b\left(y^2 - \frac{k^2}{b^2}z^2\right) \\ &\equiv b\left(y - \frac{k}{b}z\right)\left(y + \frac{k}{b}z\right) \mod a. \end{aligned}$$

By symmetry, $ax^2 + by^2 + cz^2$ also splits into linear factors over $\mathbb{Z}/|b|\mathbb{Z}$ and $\mathbb{Z}/|c|\mathbb{Z}$, so by CRT, it also factors over $\mathbb{Z}/abc\mathbb{Z}$:

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(rx + sy + tz) \mod abc.$$

Consider the set of triples of nonnegative integers

$$S = \{(x, y, z) : x, y, z \geq 0, x < \sqrt{|bc|}, y < \sqrt{|ca|}, z < \sqrt{|ab|}\}.$$

Since bc, ca, ab are not perfect squares, we have $|S| > abc$. Then, by pigeonhole principle, there exists two distinct triples (x_1, y_1, z_1) and (x_2, y_2, z_2) such that

$$\alpha x_1 + \beta y_1 + \gamma z_1 \equiv \alpha x_2 + \beta y_2 + \gamma z_2 \mod abc.$$

Setting $x = x_1 - x_2$, $y = y_1 - y_2$, $z = z_1 - z_2$, we have $\alpha x + \beta y + \gamma z \equiv 0 \mod abc$, which implies that

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(rx + sy + tz) \equiv 0 \mod abc.$$

Moreover, since $x < \sqrt{|bc|}, y < \sqrt{|ca|}, z < \sqrt{|ab|}$, and $a > 0, b, c < 0$ we have

$$\begin{aligned} ax^2 + by^2 + cz^2 &\leq ax^2 < abc, \\ ax^2 + by^2 + cz^2 &\geq by^2 + cz^2 > -2abc. \end{aligned}$$

Thus, $ax^2 + by^2 + cz^2$ is either 0 or abc. In the former case, (x, y, z) is a nontrivial solution since (x_1, y_1, z_1) and (x_2, y_2, z_2) are distinct and we are done. In the latter case, we make the following change of variables:

$$x' = xz - by, \quad y' = yz + ax, \quad z' = z^2 + ab$$

and it follows that $ax'^2 + by'^2 + cz'^2 = 0$. If (x', y', z') is trivial, then the conic is $x^2 - y^2 + cz^2$, and $(1, 1, 0)$ is a nontrivial solution.

□

3 From Conics to Cubics

Now with some intuition gained from analyzing the case for conics, we turn to discussing rational points on cubic curves. Similarly, we reduce the cubic to a form that is easier to deal with, namely the Weierstrass normal form:

$$y^2 = x^3 + ax^2 + bx + c.$$

With a smart choice of axes in the projective space, one can show that any cubic is birationally equivalent to a cubic in the Weierstrass normal form. (See Section 1.3 of [2] for a sketch of the transformation.) There is a bijection between rational points on the general cubic and those on the reduced cubic as a result of the birational equivalence. Note that a cubic in Weierstrass normal form is symmetric across the x-axis, i.e., if (x, y) is on the curve, then is $(x, -y)$.

An elliptic curve is a nonsingular cubic in the Weierstrass normal form. As shown in Figure 1.1, an elliptic curve could either be one or two connected pieces in $\mathbb{R}^2$ depending on whether they have 1 or 3 real roots.

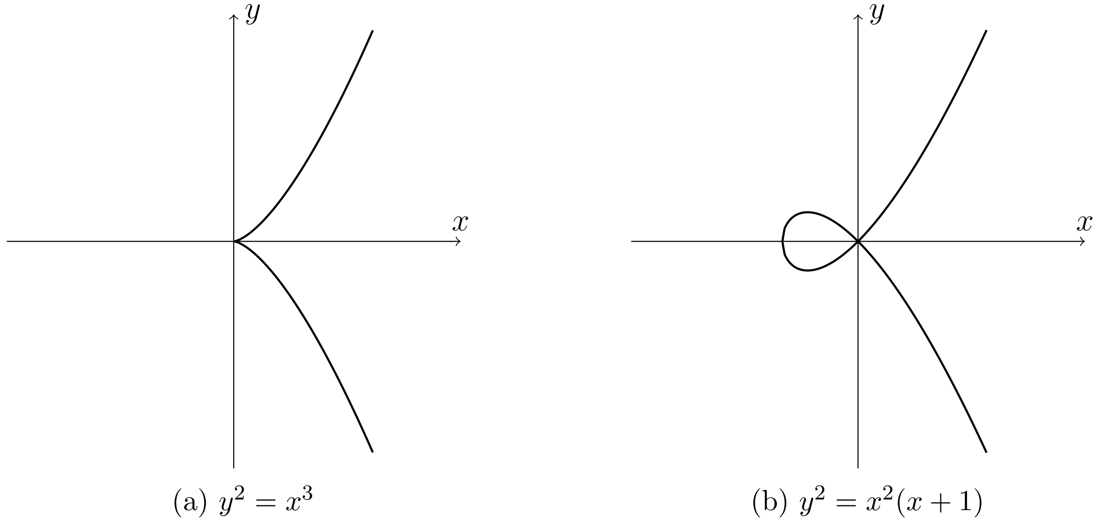
A cubic in the Weierstrass form is singular when $y^2 = f(x) = x^3 + ax^2 + bx + c$ has a repeated root (See Figure 3.1). If $f(x)$ has three repeated roots, e.g., $f(x) = x^3$, then the curve has a cusp, or a "sharp" point. If the curve has two repeated roots, e.g., $f(x) = x^2(x+1)$ then it has a pair of tangents (real or complex) at the point of singularity.

Singular cubics behave quite differently from nonsingular ones. Since a line that passes through the singular point only crosses the curve at one other point, rational points on a singular cubic can be projected on to a rational line in the same way as conics, so the analysis of rational points on singular cubics can be dealt with similarly. Therefore, we will restrict our attention to singular cubics, i.e., birationally equivalent to a nonsingular cubic in the Weierstrass normal form.

3.1 Group Structure of Points on Elliptic Curves

The ubiquity and usefulness of elliptic curves can be partially attributed to the fact that points on elliptic curves have a very conveninet additional structure — they form an abelian group under a natural geometric operation involving lines and intersections.

Since an elliptic curve is nonsingular, a line generally intersects the curve at three points (counting multiplicities). In order to make the idea of intersections precise, we work in the



(a) $y^2 = x^3$ (b) $y^2 = x^2(x+1)$

Figure 3.1: Examples of singular cubics.

projective space. In addition to the affine part, the elliptic curve also contains a point at infinity $\mathcal{O} = (0 : 1 : 0)$ in projective space, i.e., a point that lies on all the vertical lines parallel to the y-axis. A binary operation can be defined on points on the curve by taking the line that connects the two points and find the third intersection with the curve. More precisely, let P and Q be two points on the elliptic curve, then the point $P * Q$ is the intersection of the line PQ and C. If $P = Q$, then the third point is the intersection of the curve with the tangent line at P, which intersects C at P "twice".

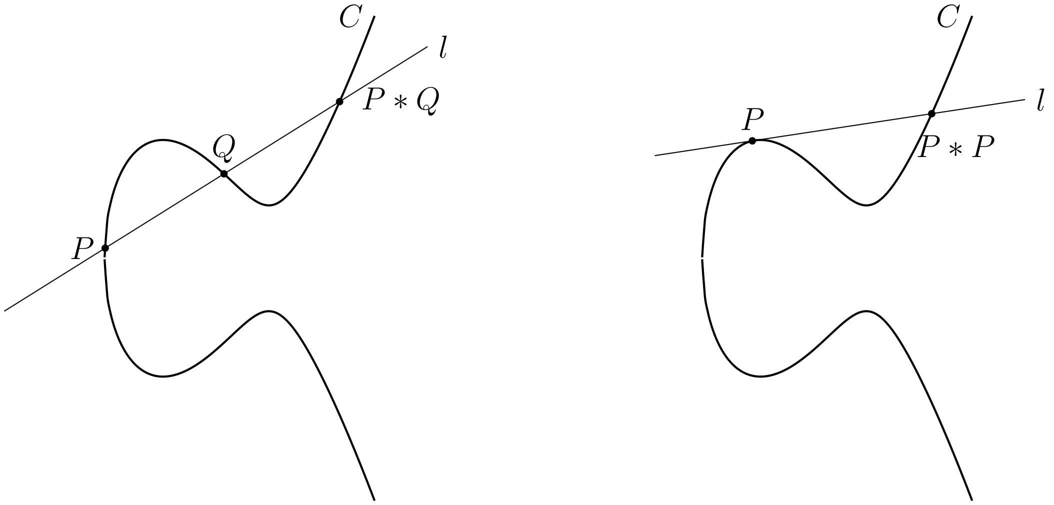


Figure 3.2: A binary operation on an elliptic curve.

We do not yet have an identity with the binary operation $*$, but we can turn the points on the curve into a group by buildig upon $*$. First, we need a point to be the identity. Any rational point can be chosen to be the identity, but for the ease of computation, we conventionally define the group operation such that the point at infinity $\mathcal{O}$ be the identity.

The group operation, which we denote by +, is defined as

$$P + Q = \mathcal{O} * (P * Q),$$

i.e., we take the third intersection of the line connecting P and Q, and then connect it with $\mathcal{O}$, where the third intersection between this new line and the curve is taken to be $P + Q$.

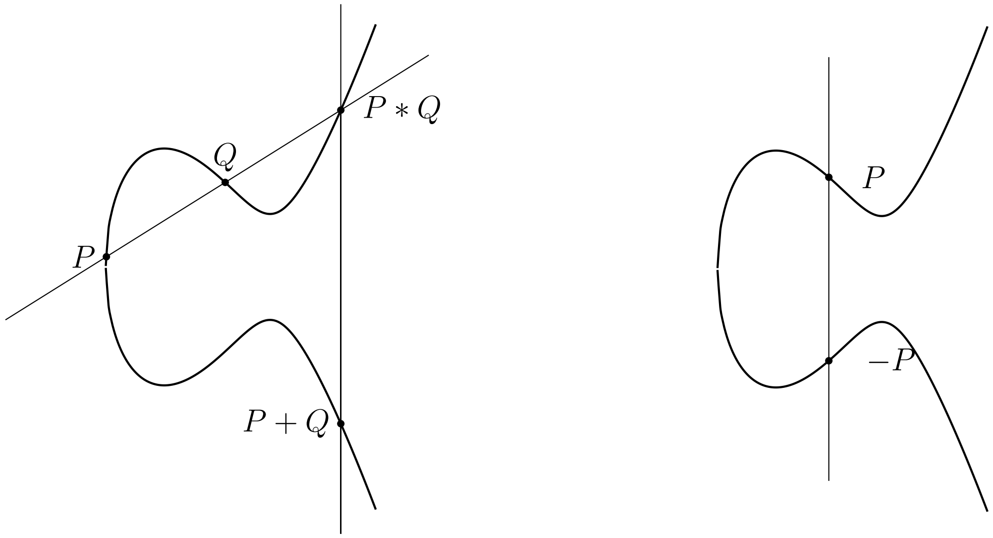


Figure 3.3: The group operation on an elliptic curve

We need to verify that the points on the curve and + do form an abelian group. First, it is easy to check that + is commutative, since $*$ is commutative: $P * Q$ and $Q * P$ give us the same line and thus the same third intersection point. Then, we check that $\mathcal{O}$ is indeed the identity, i.e., $P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = P$ for any point P on the curve. Note that the line passing connecting $\mathcal{O}$ and P passes through $P * \mathcal{O}$ by definition, then the third intersection point given $\mathcal{O}$ and $P * \mathcal{O}$ is clearly P. Next, we check that each point P does have an inverse $-P$, which we show to be its reflection across the x-axis, i.e., if the point $P = (x, y)$, then its inverse $-P = (x, -y)$. Since the line passing through P and $-P$ is vertical, its third intersection point with the curve is the point at infinity $\mathcal{O}$, so we have $P + (-P) = \mathcal{O} * (P * (-P)) = \mathcal{O} * \mathcal{O}$. The line tangent at $\mathcal{O}$ is the line at infinity, and its third intersection point is again at $\mathcal{O}$, and we have shown that $P + (-P) = \mathcal{O}$.

The last thing we need to check is that + is associative. We could do so by computing the coordinates through explicit formulas, which is doable but not quite a pleasant task. Instead, we appeal to Caley-Bacharach theoreme, an important result on cubics that can be proved from Bezout's theorem.

Theorem 3.1 (Cayley-Bacharach)**.** *Let C_1 and C_2 be two cubic curves that intersect at exactly nine points. Then any cubic curve C that passes through eight of the points also passes through the ninth.*

We are interested in showing that $(P + Q) + R = P + (Q + R)$, which is equivalent to $P * (Q + R) = (P + Q) * R$. We draw the points $\mathcal{O}, P, Q, R, P * Q, P + Q, Q * R, Q + R$ and intersection of line $P(Q + R)$ and $R(P + Q)$. Note that the set of three dashed lines and three solid lines all pass through the above nine points, and the elliptic curve passes through the first eight points except the intersection. Therefore, since a union of three lines is a cubic, by Cayley-Bacharach theorem, the elliptic curve C also passes through the ninth point, which implies that $P(Q+R)$ and $R(P+Q)$ intersects C at the same point. And we have shown $P * (Q+R) = (P+Q) * R$.

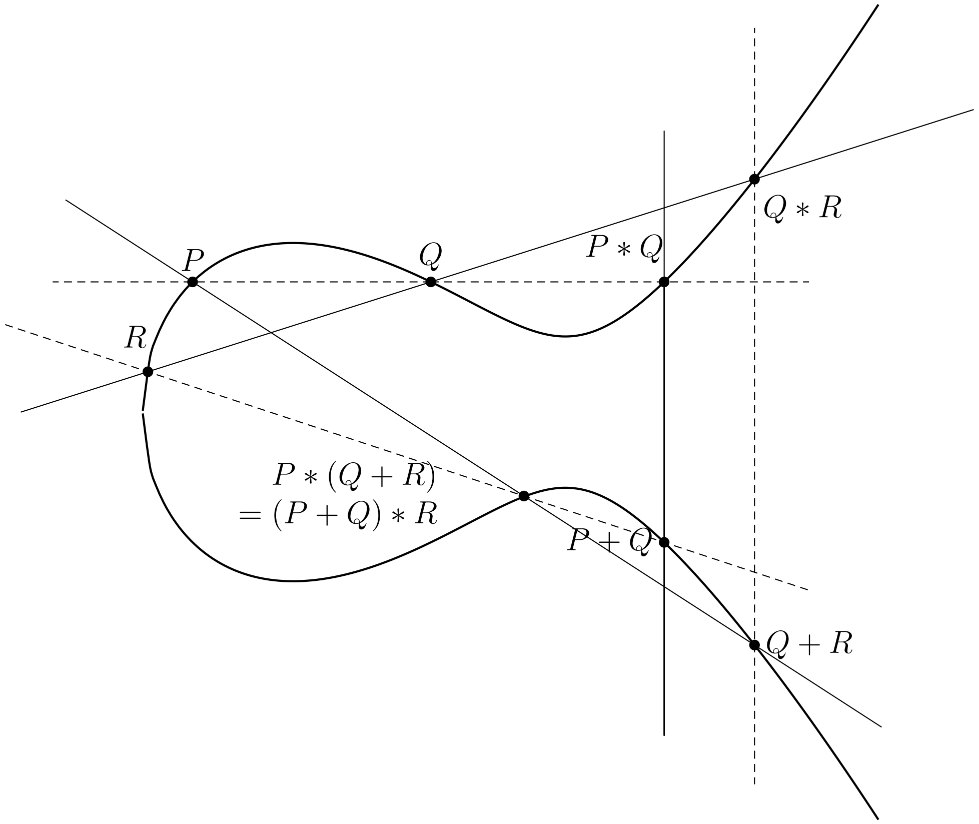


Figure 3.4: Associativity of the group operation.

Note that the rational points on an elliptic curve are closed under + and thus form a group. If P and Q have rational coefficients, then the line passing through them is a rational line. The x-coordinates of the intersections of C and l are given by a cubic with rational coefficients. Since the two roots corresponding to P and Q are rational, the third root must also be rational by Vieta's formula, so $P * Q$ has rational coefficients, and so does $P+Q$. Therefore, if we have rational points on an elliptic curve, we could potentially use the addition operation to generate more rational points on the curve.

3.2 Explicit Formulas for the Group Operation

In this section, we will derive some explicit formulas for adding two points on the curve. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two distinct points, and we try to compute $P * Q = (x_3, y_3)$ and $P + Q = (x_3, -y_3)$.

First, the equation for the line connecting P and Q is given by

$$y = \alpha x + \beta, \text{ where } \alpha = \frac{y_2 - y_1}{x_2 - x_1}, \quad \beta = y_1 - \alpha x_1.$$

We find the intersection of this line and the elliptic curve by substituting in y:

$$y^2 = (\alpha x + \beta)^2 = x^3 + ax^2 + bx + c.$$

Expanding and collecting terms, we have

$$x^3 + (a - \alpha^2)x^2 + (b - 2\alpha\beta)x + (c - \beta^2).$$

Since the three intersections are P, Q, and $P * Q$, the three roots of the cubic are x_1, x_2, and x_3. So by Vieta's formula, we have

$$x_3 = \alpha^2 - a - x_1 - x_2, \quad y_3 = \alpha x_3 + \beta.$$

For the case when $P = Q$, i.e., computing $2P$, we need to find the tangent line at P. Using the same variables, the slope α of the tangent line is given by implicit differentiation

$$\alpha = \frac{dy}{dx}\bigg|_P = \frac{f'(x_1)}{2y_1}.$$

Then, using the same formula we derived above, we have

$$x_3 = \left[\frac{f'(x_1)}{2y_1}\right]^2 - a - 2x_1 = \frac{(3x_1^2 + 2ax_1 + b)^2}{4y_1^2} - a - 2x_1.$$

Simplifying and substituting in y_1^2, we arrive at the formula for the x-coordinate of $2(x, y)$, referred to as the *duplication formula*:

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

4 Torsion Points on Elliptic Curves

As in the last section we showed how the points on an elliptic curve form a group, we can now talk about the torsion points on an elliptic curve, i.e., points with finite order. We first characterize general points on the curve of small orders. Then we discuss specifically rational torsion points on the curve and show how they can be determined algorithmically in finite steps, as a consequence of our main result of the section, the Nagell-Lutz theorem.

4.1 Points of Order 2 and 3

Let $P = (x, y)$ be a point of order 2, i.e., $2P = \mathcal{O}$, which is equivalent to $P = -P$. Since $-P = (x, -y)$, we have $y = 0$, so the points of order 2 on the curve are precisely $(r, 0)$, where r is a root of the cubic $f(x) = x^3 + ax^2 + bx + c$. Since $f(x)$ is a nonsingular cubic, it has three distinct complex roots r_1, r_2, r_3, so there are three points with order 2. The points satisfying $2P = \mathcal{O}$ are

$$\{\mathcal{O}, (r_1, 0), (r_2, 0), (r_3, 0)\}$$

, and they form a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ since it is a group of four elements and all non-identity elements have order 2.

Now let us move on to points of order 3. We can characterize them by noting that they are exactly the points that satisfy $x(2P) = x(P)$ and is not the identity. By the duplication formula, we have

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

Simplifying and rearranging, we find that $P \neq \mathcal{O}$ is a point of order 3 if and only if $x(P)$ is a root of the quartic

$$\phi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + 4ac - b^2.$$

We want to show that $\phi_3(x)$ has four distinct roots, and we do so by relating $\phi_3(x)$ to $f(x)$, since $f(x)$ is nonsingular. Recall the following form of the duplication formula:

$$x(2P) = \frac{f'(x)^2}{4f(x)} - a - 2x.$$

Setting it to equal to x and rearranging, we have

$$\phi_3(x) = f'(x)^2 - 4f(x)(a + 3x) = f'(x)^2 - 2f(x)f''(x).$$

In order to see if $\phi_3(x)$ have repeated roots, we differentiate

$$\phi_3'(x) = 2f'(x)f''(x) - (2f'(x)f''(x) + 2f(x)f'''(x)) = -2f(x)f'''(x) = -12f(x).$$

Since $f(x)$ and $f'(x)$ do not have common roots, $\phi_3(x) = f'(x)^2 - 2f(x)f''(x)$ and $\phi_3'(x) = -12f(x)$ also do not have any common roots.

As we have shown that $\phi_3(x)$ has four distinct roots s_1, s_2, s_3, s_4, there are eight points of order 3, and including the identity there are nine points satisfying the equation $3P = \mathcal{O}$:

$$\mathcal{O}, (s_1, \pm t_1), (s_2, \pm t_2), (s_3, \pm t_3), (s_4, \pm t_4).$$

Since each non-identity point has order 3, it is easy to see that they form a group isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

4.2 Nagell-Lutz Theorem

After a discussion of points of small orders in the field of complex numbers, we return to the rational numbers and look at rational torsion points. If we take an elliptic curve in Weierstrass form with rational coefficients, we can always make a change of variables to clear the denominators of the coefficients, so we assume that the coefficients a, b, c of the curve are all integers.

The Nagell-Lutz theorem gives us a nice characterization of rational torsion points on the curve.

Theorem 4.1 (Nagell-Lutz). *Let*

$$y^2 = x^3 + ax^2 + bx + c$$

be an elliptic curve with integer coefficients a, b, c, and its discriminant be

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

Let $P = (x, y)$ be a rational torsion point on the curve, then its coordinates x and y are integers and either $y = 0$ (P has order two), or $y \mid D$.

Proof. We first prove the second part of the statement assuming the first part of the theorem which states that rational torsion points have integer coefficient. Let $P = (x, y)$ be a rational torsion point, then $2P$ must also be a rational torsion point, so P and $2P$ both have integer coefficients. We need to show that either $y = 0$ or $y \mid D$.

Assume that $y \neq 0$, then $2P \neq \mathcal{O}$ and the duplication formula applies:

$$x(2P) = \left[\frac{f'(x)}{2y}\right]^2 - a - 2x.$$

Since a, x and $x(2P)$ are integers, we must have $y \mid f'(x)$. Since $f(x) = y^2$, we also have $y \mid f(x)$. By the general theorey of discriminants, we can write D as a linear combination of $f(x)$ and $f'(x)$:

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

from which we conclude that $y \mid D$.

Next, we move onto proving the crux of the theorem: a rational torsion point on an elliptic curve has integer coordinates. We prove this rather indirectly by showing that the p-adic valuation of the coordinates is nonnegative for all prime p.

To this end, let $P = (x, y)$ be a rational torsion point and let $\mu = v_p(x)$ and $\sigma = v_p(y)$. Then we can write the coordinates as

$$x = mp^\mu, \quad y = np^\sigma.$$

Plugging them into the equation of the elliptic curve, we have

$$n^2p^{2\sigma} = m^3p^{3\mu} + am^2p^{2\mu} + bmp^\mu.$$

If σ and μ are negative, then by the properties of the p-adic valuation we have $2\sigma = 3\mu$. Therefore, there exists $v \in \mathbb{Z}+$ such that $\mu = -2v$ and $\sigma = -3v$, so we can filter the rational points based on the p-adic valuation of their coordinates.

Let $E(p^v)$ denote the set of rational points such that

$$E(p^v) = \{\mathcal{O} \cup (x, y) \in E(\mathbb{Q}) : v_p(x) \leq -2v, v_p(y) \leq -3v\}.$$

Then, we obtain a chain of inclusions

$$E(\mathbb{Q}) \subset E(p) \subset E(p^2) \subset \dots$$

(In p-adic topology, we have built a chain of neighborhoods around the identity $\mathcal{O}$.)

Our goal is to show that the only torsion point in $E(p)$ is $\mathcal{O}$. We first make a transformation to move the infinite point $\mathcal{O}$ to the origin. Let

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

then the curve $y^2 = x^3 + ax^2 + bx + c$ becomes

$$s = t^3 + at^2 s + bts^2 + cs^3.$$

This transformation is bijective except for points of order 2, i.e., when $y = 0$.

Let $(x, y) \in E(p^v)$ be a point in the xy-plane, then for its corresponding point (t, s) in the ts-plane, we have

$$\begin{aligned} v_p(t) &= v_p\left(\frac{x}{y}\right) = -2(v+k) - (-3(v+k)) = v + k \geq v, \\ v_p(s) &= v_p\left(\frac{1}{y}\right) = -(-3(v+k)) \geq 3v. \end{aligned}$$

Next, we compute explicit formula for the group law in ts-plane. Let $P = (t_1, s_1)$ and $Q = (t_2, s_2)$ be two distinct points, then the line passing through P and Q is given by

$$y = \alpha x + \beta, \quad \alpha = \frac{s_2 - s_1}{t_2 - t_1}.$$

Since P and Q are on the curve, we substitute in $s = t^3 + at^2 s + bts^2 + cs^3$. After a bit of algebra, we arrive at

$$\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + t_1^2 + a\left(t_2 + t_1\right) s_2 + bs_2^2}{1 - at_1^2 - bt_1\left(s_2 + s_1\right) - c\left(s_2^2 + s_1 s_2 + s_1^2\right)}.$$

Similarly, we compute α when $P = Q$. The slope of the tangent line is given by

$$\alpha = \left.\frac{ds}{dt}\right|_P = \frac{3t_1^2 + 2at_1 s_1 + bs_1^2}{1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2}.$$

Since this is the same as the case with distinct P and Q, we simply use the former.

Let us compute $v_p(\alpha)$ for later use and recall that $v_p(t_i) \geq v, v_p(s_i) \geq 3v$. Note that for the denominator we have $v_p(1 - at_1^2 - 2bt_1 s_1 - 3cs_1^2) = v_p(1) = 0$, so

$$v_p(\alpha) = v_p(t_2^2 + t_1 t_2 + t_1^2 + a\left(t_2 + t_1\right) s_2 + bs_2^2) \geq 2v.$$

Recall that $\beta = s_1 - \alpha t_1$, so we also have $v_p(\beta) \geq 3v$.

We find the third intersection $P * Q = (t_3, s_3)$ of the line $y = \alpha x + \beta$ with the transformed curve by a procedure similar to when we computed explicit formulas for an elliptic curve in Weierstrass form. We substitute in the equation of the line and use Vieta's formula to arrive at

$$t_1 + t_2 + t_3 = -\frac{\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta}{1 + a\alpha + b\alpha^2 + c\alpha^3}.$$

Since the identity in the ts-plane is $(0,0)$, $P+Q$ has coordinates $(-t_3, -s_3)$.

We then calcualte $v_p(t_1+t_2+t_3)$. Since the denominator contains 1, and recall that $v_p(\alpha) \geq 2v, v_p(\beta) \geq 3v$, we have

$$v_p(t_1+t_2+t_3) = v_p(\alpha\beta + 2b\alpha\beta + 3c\alpha^2\beta) \geq 5v.$$

Since $v_p(t_1), v_p(t_2) \geq v$, we have $v_p(t_3) \geq v$ as well, and we have shown that the points in $E(p^v)$ are closed under addition and hence form a subgroup of $E(\mathbb{Q})$. Moreover, we obtain the relation that

$$v_p(t(P)+t(Q)-t(P+Q) \geq 5v,$$

which could be turned into a homomorphism using the ring $p^v\mathbb{Z}_p/p^5v\mathbb{Z}_p$.

We are ready to complete the proof by showing that the only torsion point in $E(p)$ is $\mathcal{O}$. Suppose $P=(t,s)$ is a torsion point of order n, i.e., $nP=(0,0)$ and thus $t(nP)=0$. Let $v_p(t)=v$, which means that $P \in E(p^v)$ but $P \notin E(P^{v+1})$. Then, by applying the above relation repeatedly, we have

$$v_p(nt - t(nP)) = v_p(nt) \geq 5v.$$

Suppose $p \nmid n$, then $v_p(nt) = v_p(t) = v$, a contradiction.

Suppose $n = kp$, then we look at $P' = kP = (t', s')$ which has order p. Let $v' = v_p(P')$ So similarly we have $v_p(pt') \geq 5v$ but $v_p(pt') = v+1$, a contradiction.

□

Let us see how the Nagell-Lutz theoren can be used to compute torsion points through an simple example.

Example. Consider the elliptic curve $y^2 = x^3 + x$. The only rational point of order 2 is $(0,0)$. Let (x,y) be a rational torsion point. Since the discriminant $D=-4$, then y must be $\pm1, \pm2$, or ±4. None of these cases are possible, so the only torsion points are $\{\mathcal{O}, (0,0)\}$, which form a group isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Mazur's theorem gives us a characterization of all the possibilities of the structure of rational torsion points of an elliptic curve. It is a beautiful and challenging theorem, and the proof is beyond the scope of this paper.

Theorem 4.2 (Mazur). *Let $E(\mathbb{Q})$ be the group of rational points on a rational elliptic curve. Then the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to*

- *either $\mathbb{Z}/n\mathbb{Z}$ for $1 \leq n \leq 10$, or $n = 12$*
- *or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ for $1 \leq m \leq 4$.*

5 Group of Rational Points on Elliptic Curves

In this section, we will provide a sketch of proof of the celebrated Mordell's theorem, which states that the group of rational points on an elliptic curve is finitely generated.

We define a measure of "complexity" of a rational number where a rational number is complex if it has a large denominator or numerator. Let the height H of a rational number be

$$H\left(\frac{m}{n}\right) = \max\{|m|, |n|\},$$

and define the height of a point to be the height of its x-coordinate, i.e., $H(P) = H(x)$. We are interested in how $H(P+Q)$ compares to $H(P)$ and $H(Q)$. For the ease of notations, we use the additive counterpart of H denoted by h.

Definition 5.1. The *height* $h(P)$ of a point P is

$$h(P) = \log H(P).$$

A nice property of the height function is that the set of points with height less than a real number is finite.

Lemma 5.2. *The set*

$$P \in E(\mathbb{Q}) : h(P) \leq M$$

is finite for any $M \in \mathbb{R}$.

Proof. If $h(P) \leq M$, then $H(P) \leq e^M$, so there are finite choices for the numerator and denominator for x, so the set of x-coordinates is finite. Since each x-coordinate corresponds to two possible y-coordinates, the set of points is also finite. □

By the following lemmas, we see how the height function behave with respect to the adding and doubling points, which allows us to translate the geometric group operation to number theoretic information given by the height function.

Lemma 5.3. *For a fixed rational point* P_0 *and an arbitrary rational point* P *on an elliptic curve,*

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

for some constant κ_0 *specific to the curve and dependent on the choice of* P_0.

Lemma 5.4. *For a rational point* P *on an elliptic curve,*

$$h(2P) \geq 4h(P) + \kappa$$

for some constant κ *specific to the curve.*

We note that the above two lemmas simply characterize the behavior of the height function and do not rely on any fact about elliptic curves as we have explicit formulas for adding and doubling points. The proof of Lemma 5.3 simply involves direct algebraic computation with the formulas and applying triangle inequalities. The proof of Lemma 5.4 is a bit more involved as we need to show that doubling the point increases the height of the point by a lot, so there cannot be too much cancelling happening with the numerator and the denominator. We do so by writing $x(2P)$ as a function of $f(x)$ and $f'(x)$, and proving a more general bound on the height of quotients of polynomials evaluated at a rational number.

The crux of Mordell's theorem lies in the following key lemma.

Lemma 5.5. *The index $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ is finite.*

The proof is quite subtle and relies on a homomorphism ϕ that factors the duplication map $P \mapsto 2P$. ϕ maps C to a closely related curve $\overline{C}$, and applying ϕ twice gives us C again after an appropriate scaling.

Equipped with the above lemmas, we are ready to prove Mordell's theorem. The main idea of the proof is in a similar vein to infinite descent. We start with an arbitrary point and produces a smaller point with the size of points measured by the height function, and show that we arrive at a finite set, and thus the entire group is finitely generated as we can reverse the descent procedure.

Theorem 5.6 (Mordell)**.** *The group of rational points $E(\mathbb{Q})$ on an elliptic curve is a finitely generated abelian group.*

Proof. Let $[E(\mathbb{Q}) : 2E(\mathbb{Q})] = n$, and pointe $Q_1, \dots, \mathbb{Q}_n$ be the representatives for each coset of $2E(\mathbb{Q})$. Therefore, for a point $P_0 \in E(\mathbb{Q})$, we can repeatedly perform the operation

$$P_k = Q_{i_k} + 2P_{k+1}$$

to arrive at the expansion

$$P = Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m.$$

Consequently, it suffices to show that for large enough m, we can obtain a bound for the height of P_m independent of the initial point P, which implies that the Q_i's and the finite set of points less than a certain height generate $E(\mathbb{Q})$.

We use the bounds in Lemma 5.3 and Lemma 5.4 to show that the height of each P_{k+1} is proportionally smaller than P_k. Take $-Q_i$ to be the fixed point, then for any point P_k, we have

$$h(P_k - Q_{i_k}) = h(2P_{k+1}) \leq 2h(P) + \kappa_i.$$

Let $\kappa = \max \kappa_i$, we combine the bounds and find that for all Q_i, we have

$$h(2P_{k+1}) \leq 2h(P_k) + \kappa.$$

Recall that

$$h(2P_{k+1}) \geq 4h(P_{k+1}) + \kappa'.$$

From the upper and lower bounds on $h(2P_{k+1})$, we obtain

$$4h(P_{k+1}) + \kappa' \leq 2h(P_k) + \kappa,$$

which we rewrite as

$$h(P_k + 1) \leq \frac{3}{4}h(P_k) - \frac{1}{4}\left(h(P_k) - (\kappa + \kappa')\right).$$

Therefore, if $h(P_k) > \kappa + \kappa'$, we can always find P_{k+1} whose height is smaller by a factor of 3/4. So we are guaranteed with a positive integer m such that $P_m \leq \kappa + \kappa'$, which finishes our proof.

□

References

[1] Kumar, Abhinav. *18.701 Theory of Numbers.* Spring 2012. Massachusetts Institute of Technology: MIT OpenCouseWare, `https://ocw.mit.edu/`. License: Creative Commons BY-NC-SA.

[2] Silverman, Joseph H. and Tate, John T. *Rational points on elliptic curve.* Undergraduate Texts in Mathematics, Springer, New York 2015.