

# Elliptic Curves

October 19, 2020

## Contents

<b>1</b>	<b>Fermat's Method of Infinite Descent</b>	<b>2</b>
1.1	A Variant for Polynomials . . . . .	3
<b>2</b>	<b>Some Remarks on Algebraic Curves</b>	<b>3</b>
2.1	Order of Vanishing . . . . .	5
2.2	Riemann Roch Spaces . . . . .	5
2.3	The Degree of a Morphism . . . . .	7
<b>3</b>	<b>Weierstrass Equations</b>	<b>7</b>
<b>4</b>	<b>Group Law</b>	<b>10</b>
4.1	Explicit Formulae for the Group Law . . . . .	11
4.2	Elliptic Curves over $\mathbb{C}$ . . . . .	13

# 1 Fermat's Method of Infinite Descent

Suppose we have a right-angled triangle  $\Delta$  with side lengths  $a, b, c$ , so that by Pythagoras we have  $a^2 + b^2 = c^2$ , and  $\text{area}(\Delta) = \frac{1}{2}ab$ .

**Definition 1.1.**  $\Delta$  is **rational** if  $a, b, c \in \mathbb{Q}$ , and **primitive** if  $a, b, c \in \mathbb{Z}$  coprime.

**Lemma 1.2.** Every primitive triangle is of the form  $a = u^2 - v^2, b = 2uv, c = u^2 + v^2$  for coprime integers  $u > v > 0$ .

*Proof.* If  $a, b$  were both odd, then  $a^2 + b^2 \equiv 2 \pmod{4}$ , and we have no solutions for  $c$ . If  $a, b$  both even, then they are not coprime. So we may assume  $a$  is odd,  $b$  is even,  $c$  is odd.

Then  $(\frac{b}{2})^2 = \frac{c+a}{2} \frac{c-a}{2}$ , and the right hand side is a product of coprime positive integers. So by unique prime factorisation in the integers,  $\frac{c+a}{2} = u^2, \frac{c-a}{2} = v^2$  for some coprime integers  $u, v$ . Rearranging, we have the lemma.  $\square$

**Definition 1.3.**  $D \in \mathbb{Q}_{>0}$  is a **congruent number** if it is the area of a rational triangle.

Note that, by scaling the triangle, it suffices to consider  $D \in \mathbb{Z}_{>0}$  squarefree.

For example,  $D = 5, 6$  are congruent numbers.  $6 = \frac{1}{2} \cdot 3 \cdot 4$ , and  $3^2 + 4^2 = 5^2$ , and 5 is left as an exercise.

**Lemma 1.4.**  $D \in \mathbb{Q}_{>0}$  is congruent if and only if  $Dy^2 = x^3 - x$  for some  $x, y \in \mathbb{Q}, y \neq 0$ .

*Proof.* Lemma 1.2 shows that  $D$  is congruent if and only if  $Dw^2 = uv(u^2 - v^2)$  for some  $u, v, w \in \mathbb{Q}, w \neq 0$ .

Setting  $x = \frac{u}{v}, y = \frac{w}{v^2}$  finishes the proof.  $\square$

Fermat showed that 1 is not a congruent number.

**Theorem 1.5.** There is no solution to

$$w^2 = uv(u+v)(u-v) \quad (*)$$

in integers  $u, v, w$  with  $w \neq 0$ .

*Proof.* Without loss of generality,  $u, v$  are coprime with  $u > 0, w > 0$ . If  $v < 0$  then replace  $(u, v, w)$  by  $(-v, u, w)$ . If  $u, v$  are both odd, then replace  $(u, v, w)$  by  $(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2})$ . So we may assume that all of  $u, v, u+v, u-v$  are coprime positive integers whose product is a square, and hence are all squares, say  $a^2, b^2, c^2, d^2$  respectively, where  $a, b, c, d \in \mathbb{Z}_{>0}$ .

Since  $u \not\equiv v \pmod{2}$ , both  $c, d$  are odd. Consider the right angled triangle with side lengths,  $\frac{c+d}{2}, \frac{c-d}{2}, a$ . This is a primitive triangle, and it has area  $\frac{c^2-d^2}{8} = \frac{v}{4} = (\frac{b}{2})^2$ .

Let  $w_1 = \frac{b}{2}$ . Then lemma 1.2 gives  $w_1^2 = u_1 v_1 (u_1^2 - v_1^2)$  for some  $u_1, v_1 \in \mathbb{Z}$ , giving a new solution to  $(*)$ . But  $4w_1^2 = b^2 = v|w|^2$ , and so  $w_1 \leq \frac{1}{2}w$ .

So by Fermat's method of infinite descent, if there were a solution we would have a strictly decreasing infinite sequence of positive integers  $\frac{1}{2}$ . Hence there is no solution to  $(*)$ .  $\square$

## 1.1 A Variant for Polynomials

Here,  $K$  is a field with  $\text{char } K \neq 2$ . The algebraic closure of  $K$  will be  $\overline{K}$ .

**Lemma 1.6.** *Let  $u, v \in K[t]$  be coprime. If  $\alpha u + \beta v$  is a square for four distinct  $(\alpha : \beta) \in \mathbb{P}^1$ , then  $u, v \in K$ .*

*Proof.* Without loss of generality we may assume  $K = \overline{K}$ , as that doesn't change the degree of polynomials, and every square is still a square.

Changing coordinates on  $\mathbb{P}^1$ , we may assume the ratios  $\alpha : \beta$  are  $(1 : 0), (0 : 1), (1 : -1), (1 : -\lambda)$  for some  $\lambda \in K \setminus \{0, 1\}$ , with  $\mu = \sqrt{\lambda}$ .

Then  $u = a^2, v = b^2, u - v = (a + b)(a - b), u - \lambda v = (a + \mu b)(a - \mu b)$  are all squares. They are also coprime, and so by unique factorisation in  $K[t]$ ,  $(a + b), (a - b), (a + \mu b), (a - \mu b)$  are all squares.

But  $\max\{\deg a, \deg b\} \leq \frac{1}{2} \max\{\deg u, \deg v\}$ . So by Fermat's method of infinite descent, we get that the original  $u, v \in K$ .  $\square$

Now we have some important definitions:

**Definition 1.7.**

1. An **elliptic curve**  $E$  over a field  $K$  is the projective closure of the affine curve  $y^2 = f(x)$  where  $f \in K[x]$  is a monic cubic polynomial with distinct roots.
2. For  $L/K$  any field extension,  $E(L) = \{(x, y) \in L^2 : y^2 = f(x)\} \cup \{0\}$ .  $0$  is called the **point at infinity**.

We call the point at infinity  $0$  because we will see that  $E(L)$  is naturally an abelian group under an operation we will denote by  $+$ , and  $0$  will be the identity for that group. In this course we will study  $E(L)$  for  $L$  a finite field, a local field, and a number field.

Lemma 1.4 and theorem 1.5 together imply that, if  $E$  is given by  $y^2 = x^3 - x$ , then  $E(\mathbb{Q}) = \{0, (0, 0), (\pm 1, 0)\}$ , which we will see is the group  $C_2 \times C_2$ .

**Corollary 1.8.** *Let  $E/K$  be an elliptic curve. Then  $E(K(t)) = E(K)$ .*

*Proof.* Without loss of generality,  $K = \overline{K}$ . By a change of coordinates we may assume  $E : y^2 = x(x - 1)(x - \lambda)$  for some  $\lambda \in K \setminus \{0, 1\}$ . Suppose  $(x, y) \in E(K(t))$ . Write  $x = \frac{u}{v}$  with  $u, v \in K[t]$  coprime. Then  $w^2 = uv(u - v)(u - \lambda v)$  for some  $w \in K[t]$ .

Unique factorisation in  $K[t]$  gives  $u, v, u - v, u - \lambda v$  are all squares, and so by lemma 1.6,  $u, v \in K$ , and so  $x, y \in K$ .  $\square$

## 2 Some Remarks on Algebraic Curves

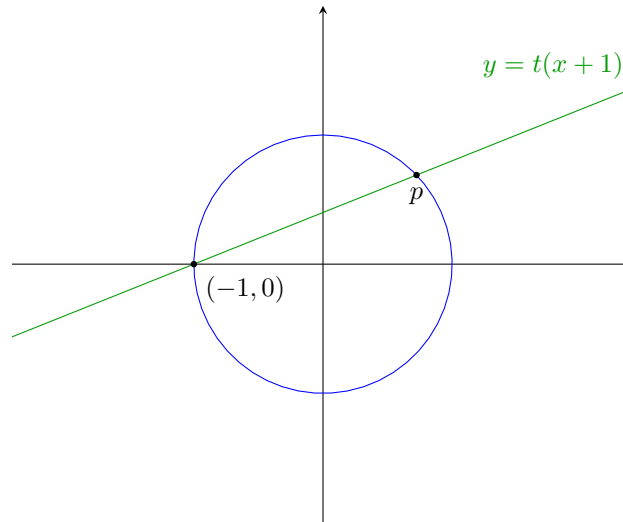
We will be working over an algebraically closed field  $K$ .

**Definition 2.1.** *An (irreducible) plane algebraic curve  $C = \{f(x, y) = 0\} \subset \mathbb{A}^2$  is **rational** if it has a rational parametrization, i.e. there are  $\phi, \psi \in K(t)$  such that:*

1.  $\mathbb{A}^1 \rightarrow \mathbb{A}^2; t \mapsto (\phi(t), \psi(t))$  is injective on  $\mathbb{A}^1 \setminus \{\text{finite set}\}$ .
2.  $f(\phi(t), \psi(t)) = 0$ .

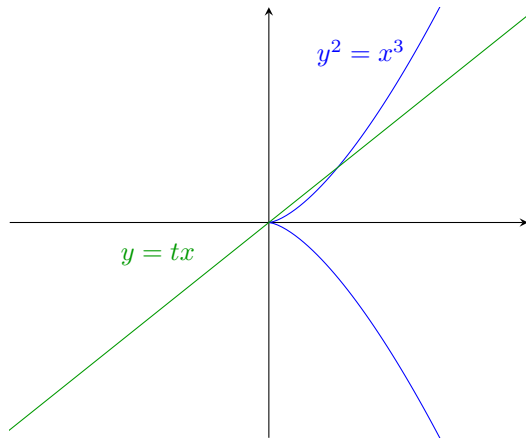
### Examples 2.2.

- Any nonsingular plane conic is rational. For example, take a circle  $x^2 + y^2 = 1$ . Pick a point on it,  $(-1, 0)$ . Now draw a line through it with slope  $t$ , and solve for the points of intersection between the curve and the line.

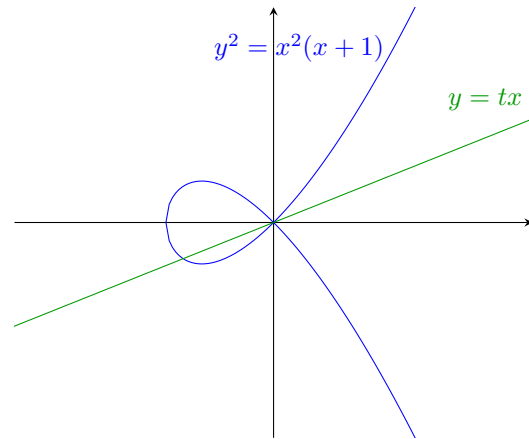


Solving for the coordinates of  $p$ , we get the quadratic  $x^2 + t^2(x + 1)^2 = 1$ , i.e.  $x = -1$  or  $\frac{1-t^2}{1+t^2}$ . So we have the rational parametrization  $(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$

- Any singular plane cubic is rational.



(a) Rational Parametrization  $(x, y) = (t^2, t^3)$



(b) Left as an example on the first sheet

- Corollary 1.8 shows that elliptic curves are *not* rational.

**Definition 2.3.** The **genus**  $g(C) \in \mathbb{Z}_{\geq 0}$  is an invariant of a smooth projective curve.

- If  $K = \mathbb{C}$ , then  $g(C) = \text{genus of the Riemann surface } C$ .

- A smooth plane curve  $C \subset \mathbb{P}^2$  of degree  $d$  has genus  $g(C) = \frac{(d-1)(d-2)}{2}$ .

**Proposition 2.4.** Let  $C$  be a smooth projective curve over  $K$ , an algebraically closed field. Then:

1.  $C$  is rational  $\iff g(C) = 0$ .
2.  $C$  is an elliptic curve  $\iff g(C) = 1$ .

*Proof.* A proof of 1 is omitted from this course. For 2, we check (on the first example sheet) that elliptic curves are smooth plane curves. Then they have degree 3, so genus  $\frac{2 \cdot 1}{2} = 1$ . For the other direction, see later on in the course.  $\square$

## 2.1 Order of Vanishing

$C$  will be an algebraic curve, and  $K(C)$  its function field, with  $P \in C$  a smooth point. Write  $\text{ord}_P(f)$  to mean the order of vanishing of  $f \in K(C)$  at  $P$  (negative if  $f$  has a pole).

Fact:  $\text{ord}_P : K(C)^\times \rightarrow \mathbb{Z}$  is a discrete valuation, i.e.  $\text{ord}_P(f_1 f_2) = \text{ord}_P(f_1) + \text{ord}_P(f_2)$  and  $\text{ord}_P(f_1 + f_2) \geq \min\{\text{ord}_P(f_1), \text{ord}_P(f_2)\}$ .

We say  $t \in K(C)^\times$  is a **uniformizer** at the point  $P$  if  $\text{ord}_P(t) = 1$ .

**Example 2.5.** Let  $C = \{g(x, y) = 0\} \subseteq \mathbb{A}^2$ , where  $g \in K[x, y]$  is irreducible. Then  $K(C) = \text{Frac} \frac{K[x, y]}{(g)}$ , with  $g = g_0 + g_1(x, y) + g_2(x, y) + \dots$ ,  $g_i$  homogeneous of degree  $i$ .

Suppose  $P = (0, 0) \in C$  is a smooth point, i.e.  $g_0 = 0, g_1(x, y) = \alpha x + \beta y$  with  $\alpha, \beta$  not both zero.

Let  $\gamma, \delta \in K$ . It is a fact that  $\gamma x + \delta y \in K(C)$  is a uniformizer at  $P$  if and only if  $\frac{\gamma}{\delta} \neq \frac{\alpha}{\beta}$ , i.e.  $\alpha\delta - \beta\gamma \neq 0$ .

**Example 2.6.**  $\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2$ ,  $\lambda \neq 0, 1$ . We take the projective closure, i.e. homogenize the equation as  $\{Y^2 Z = X(X-Z)(X-\lambda Z)\} \subset \mathbb{P}^2$  by setting  $x = X/Z, y = Y/Z$ .

Have we got new points by taking projective closure? We only get these when  $Z = 0$ , i.e.  $0 = X^3 \implies X = 0, Y \neq 0$ . Since we're in projective space, this is just one point:  $P = (0 : 1 : 0)$ . We compute  $\text{ord}_P(x)$  and  $\text{ord}_P(y)$ . Put  $t = X/Y, w = Z/Y$  (since we can't return to the original affine piece, as it doesn't contain  $Z = 0$ ). Then we get  $w = t(t-w)(t-\lambda w)$ . Now  $P$  is the point  $(t, w) = (0, 0)$ . This is a smooth point, as there are linear terms at that point (namely  $w$ ). So  $\text{ord}_P(t) = \text{ord}_P(t-2) = \text{ord}_P(t-\lambda w) = 1$ , and  $\text{ord}_P(w) = 1 + 1 + 1 = 3$ .

Then:

$$\begin{aligned}\text{ord}_P(x) &= \text{ord}_P(X/Z) = \text{ord}_P(t/w) = 1 - 3 = -2 \\ \text{ord}_P(y) &= \text{ord}_P(Y/Z) = \text{ord}_P(1/w) = -3\end{aligned}$$

## 2.2 Riemann-Roch Spaces

Let  $C$  be a smooth projective curve. Then a **divisor** is a formal sum of points on  $C$ , say  $D = \sum_{P \in C} n_P P$  where  $n_P \in \mathbb{Z}$ , and only finitely many  $n_P$  are nonzero, and let  $\deg D = \sum_{P \in C} n_P$ . These divisors form a group under addition, denoted  $\text{Div}(C)$ .

$D$  is said to be **effective**, written  $D \geq 0$  if  $n_P \geq 0$  for all  $P \in C$ .

If  $f \in K(C)^\times$ , we write  $\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f)P$ .

The Riemann Roch space of  $D \in \operatorname{Div}(C)$  is:

$$\mathcal{L}(D) = \{f \in K(C) : \operatorname{div}(f) + D \geq 0\} \cup \{0\}$$

i.e. the  $K$ -vector space of rational functions on  $C$  with “poles no worse than specified by  $D$ .”

**Theorem 2.7** (Riemann Roch for genus 1).

$$\dim \mathcal{L}(D) = \begin{cases} 0 & \deg D < 0 \\ 0 \text{ or } 1 & \deg D = 0 \\ \deg D & \deg D > 0 \end{cases}$$

**Example 2.6 (revisited).** Our curve is  $\{y^2 = x(x-1)(x-\lambda)\} \subset \mathbb{A}^2$ , together with  $P = (0 : 1 : 0)$ , the point at infinity. Recall  $\operatorname{ord}_P(x) = -2, \operatorname{ord}_P(y) = -3$ .

We thus deduce that  $\mathcal{L}(2P) = \langle 1, x \rangle, \mathcal{L}(3P) = \langle 1, x, y \rangle$ .

**Proposition 2.8.** *Let  $K$  be an algebraically closed field not of characteristic 2. Let  $C \subset \mathbb{P}^2$  be a smooth plane cubic, and that  $P \in C$  is a point of inflection. Then we may change coordinates such that:*

$$\begin{aligned} C : Y^2Z &= X(X-Z)(X-\lambda Z), \quad \lambda \neq 0, 1 \\ P &= (0 : 1 : 0) \end{aligned}$$

*Proof.* We make a change of coordinates such that  $P = (0 : 1 : 0)$  and the tangent line to  $C$  at  $P$ ,  $T_P(C) = \{Z = 0\}$ . Now let  $C = \{F(X, Y, Z) = 0\}$ .

Since  $P \in C$  is a point of inflection,  $F(t, 1, 0)$  has a triple root at  $t = 0$ . But  $F$  is degree 3, so we have  $F(t, 1, 0) = kt^3$  for  $k$  some constant. I.e., there are no terms in  $F$  of the form  $X^2Y, XY^2, Y^3$ .

So  $F \in \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \rangle$ . The coefficient of  $Y^2Z$  is nonzero, as otherwise  $P$  would be singular. The coefficient of  $X^3$  is also nonzero, as  $C$  is irreducible and otherwise  $\{Z = 0\} \subset C$ .

We are free to rescale  $X, Y, Z, F$ , and so WLOG  $C$  is defined by

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

. We call this Weierstrass form.

Since our field doesn't have characteristic 2, we may complete the square by substituting  $Y = Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$ , we may assume  $a_1 = a_3 = 0$ .

Now  $C : Y^2Z = Z^3f(X/Z)$ , where  $f$  is a monic cubic polynomial. Since  $C$  is smooth,  $f$  has distinct roots, which are WLOG  $0, 1, \lambda$ . So

$$C : Y^2Z = X(X-Z)(X-\lambda Z)$$

which we call the Legendre form. □

It may be shown that the points of inflection on  $C = \{F = 0\} \subset \mathbb{P}^2$  are given by  $F = \det \left( \frac{\partial^2 f}{\partial X_i \partial X_j} \right) = 0$

## 2.3 The Degree of a Morphism

Let  $\phi : C_1 \rightarrow C_2$  be a nonconstant morphism of smooth projective curves. Let  $\phi^* : K(C_2) \rightarrow K(C_1)$ ,  $f \mapsto f \circ \phi$ .

**Definition.**

1.  $\deg \phi = [K(C_1) : \phi^* K(C_2)]$
2.  $\phi$  is separable if  $K(C_1)/\phi^* K(C_2)$  is a separable field extension (which by Galois theory is automatic if  $\text{char } K = 0$ )

Suppose  $P \in C_1, Q \in C_2, \phi : P \rightarrow Q$ . Let  $t \in K(C_2)$  be a uniformizer at  $Q$ . We then define  $e_\phi(P) = \text{ord}_P(\phi^* t)$ , which is always  $\geq 1$ , and independent of  $t$ .  $e_\phi(P)$  is called the **ramification index** of  $\phi$  at  $P$ .

**Theorem 2.9.** Let  $\phi : C_1 \rightarrow C_2$  be a nonconstant morphism of smooth projective curves. Then

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$$

for any point  $Q \in C_2$ . Moreover, if  $\phi$  is separable then  $e_\phi(P) = 1$  with at most finitely many exceptions.

In particular:

1.  $\phi$  is surjective
2. If  $\phi$  is separable,  $\#\phi^{-1}(Q) \leq \deg \phi$ , with equality for all but finitely many choices of  $Q$ .

**Remark 2.10.** Let  $C$  be an algebraic curve. A rational map is given by  $\phi : C \dashrightarrow \mathbb{P}^n, P \mapsto (f_0(P) : \dots : f_n(P))$ , where  $f_0, \dots, f_n \in K(C)$  are not all zero. If  $C$  is smooth then  $\phi$  is a morphism.

## 3 Weierstrass Equations

In this section,  $K$  is a perfect field (so that all finite extensions of  $K$  are separable), with algebraic closure  $\bar{K}$ .

**Definition.** An elliptic curve  $E$  over  $K$  is a smooth projective curve of genus 1 defined over  $K$  with a specified  $K$ -rational point  $O_E$ .

Example: Take  $\{X^3 + pY^3 + p^2Z^3 = 0\} \subset \mathbb{P}^2$  for  $p$  prime. This is not an elliptic curve over  $\mathbb{Q}$  since there is no  $\mathbb{Q}$ -points.

**Theorem 3.1.** Every elliptic curve  $E$  is isomorphic over  $K$  to a curve in Weierstrass form via an isomorphism taking  $O_E$  to  $(0 : 1 : 0)$ .

Proposition 2.8 treated the special case where  $E$  is a smooth plane cubic and  $O_E$  is a point of inflection.

If  $D \in \text{Div}(E)$  is defined over  $K$  (i.e. fixed by the natural action of  $\text{Gal}(\bar{K}/K)$ ), then  $\mathcal{L}(D)$  has a basis in  $K(E)$ , not just in  $\bar{K}(E)$ .

*Proof.* Note that

$$\mathcal{L}(2O_E) \subset \mathcal{L}(3O_E)$$

Pick bases of these spaces, say  $\{1, x\}$  and  $\{1, x, y\}$ .

Note that  $\text{ord}_{O_E}(x) = -2, \text{ord}_{O_E}(y) = -3$ . The 7 elements  $\{1, x, y, x^2, xy, x^3, y^2\}$  are rational functions with no pole except at  $O_E$ , where they have poles of degree at most 6, so they all lie in  $\mathcal{L}(6O_E)$ . Riemann-Roch tells us this space has dimension 6, so there is a dependence relation between these elements.

Leaving out  $x^3$  or  $y^2$  gives a basis for  $\mathcal{L}(6O_E)$  since each term has a different order pole at  $O_E$ , so they are independent.

Therefore this dependence relation *must* involve both  $x^3$  and  $y^2$ . Rescaling  $x, y$  we get

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

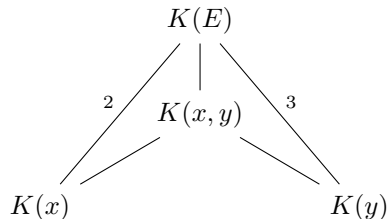
Let  $E'$  be the curve defined by this equation (or rather its projective closure).

There is a morphism

$$\begin{aligned}\phi : E &\rightarrow E' \\ P &\mapsto (x(P) : y(P) : 1) = \left( \frac{x}{y}(P) : 1 : \frac{1}{y}(P) \right) \\ O_E &\mapsto (0 : 1 : 0)\end{aligned}$$

$$\begin{aligned}[K(E) : K(x)] &= \deg(E \xrightarrow{x} \mathbb{P}^1) = \text{ord}_{O_E}\left(\frac{1}{x}\right) = 2 \\ [K(E) : K(y)] &= \deg(E \xrightarrow{y} \mathbb{P}^1) = \text{ord}_{O_E}\left(\frac{1}{y}\right) = 3\end{aligned}$$

This gives us a diagram of field extensions



So  $[K(E) : K(x, y)]$  divides both 2 and 3 by the tower law, and hence  $K(E) = K(x, y)$ , and hence  $\deg(E \xrightarrow{\phi} E') = 1$ , and  $\phi$  is birational. If  $E'$  is singular, then it is rational, and so  $E$  is also rational  $\nmid$ . So  $E'$  is not singular and hence smooth, and we may use remark **2.10** to  $\phi^{-1}$  to see that  $\phi^{-1}$  is a morphism, and hence  $\phi$  is an isomorphism.  $\square$

**Proposition 3.2.** *Let  $E, E'$  be elliptic curves over  $K$  in Weierstrass form. Then  $E \cong E'$  over  $K$  if and only if the Weierstrass equations are related by a change of variables of the form*

$$\begin{aligned}x &= u^2x' + r \\ y &= u^3yu' + u^2sx' + t\end{aligned}$$

for  $u, r, s, t \in K, u \neq 0$ .



*Proof.* Using the notation of the previous proof,

$$\begin{aligned}\langle 1, x \rangle &= \mathcal{L}(2O_E) = \langle 1, x' \rangle \\ \langle 1, x, y \rangle &= \mathcal{L}(3O_E) = \langle 1, x', y' \rangle \\ \implies &\begin{cases} x = \lambda x' + r & \lambda_1 r \in K, \lambda \neq 0 \\ y = \mu y' + \sigma x' + t & \mu, \sigma, t \in K, \mu \neq 0 \end{cases}\end{aligned}$$

Looking at the coefficients of  $x^3$  and  $y^2$ ,  $\lambda^3 = \mu^2 \implies (\lambda, \mu) = (u^2, u^3)$  for  $u \in K^\times$ .

Put  $s = \sigma/u^2$  □

The effect of this transformation on the coefficients  $a_i$  is on the formula sheet for this course. A Weierstrass equation defines an elliptic curve if and only if it defines a smooth curve, if and only if  $\Delta(a_1, \dots, a_6) \neq 0$  where  $\Delta$  is as follows:

$$\begin{aligned}b_2 &:= a_1^2 + 4a_2 \\ b_4 &:= 2a_4 + a_1a_3 \\ b_6 &:= a_3^2 + 4a_6 \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6\end{aligned}$$

If  $\text{char } K \neq 2, 3$ , then we can reduce to the case

$$\begin{aligned}E : y^2 &= x^3 + ax + b \\ \Delta &= -16(4a^3 + 27b^2)\end{aligned}$$

**Corollary 3.3.** Assume  $\text{char } K \neq 2, 3$ . If we have two elliptic curves

$$\begin{aligned}E : y^2 &= x^3 + ax + b \\ E' : y^2 &= x^3 + a'x + b'\end{aligned}$$

then they are isomorphic over  $K$  if and only if

$$\begin{aligned}a' &= u^4a \\ b' &= u^6b\end{aligned}$$

for some  $u \in K^\times$ .

*Proof.*  $E$  and  $E'$  are related as in **3.2** with  $r = s = t = 0$ . □

**Definition.** The ***j*-invariant** is  $j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}$ . Note that the denominator is nonzero since the discriminant is nonzero.

**Corollary 3.4.**  $E \cong E' \implies j(E) = j(E')$ , and the converse holds if  $K = \bar{K}$ .

*Proof.*

$$\begin{aligned}E \cong E' &\iff a' = u^4a; b' = u^6b \text{ for some } u \in K^\times \\ &\implies (a^3 : b^2) = ((a')^3 : (b')^2) \\ &\iff j(E) = j(E')\end{aligned}$$

and the reverse implication holds in the second line if  $K = \bar{K}$ . □

## 4 Group Law

Let  $E \subset \mathbb{P}^2$  be a smooth plane cubic, and  $O_E \in E(K)$ . Since  $E$  is of degree 3, it meets each line in 3 points counted with multiplicity. Hence, given two points  $P, Q$  on  $E$ , the line  $\overline{PQ}$  meets  $E$  at a third point  $S$ . Then the line  $\overline{O_E S}$  meets  $E$  at a third point  $R$ . We then define  $P \oplus Q = R$ .

If  $P = Q$ , then we take the tangent line at  $P$ , likewise if  $S = O_E$ . We can view this diagrammatically as follows:

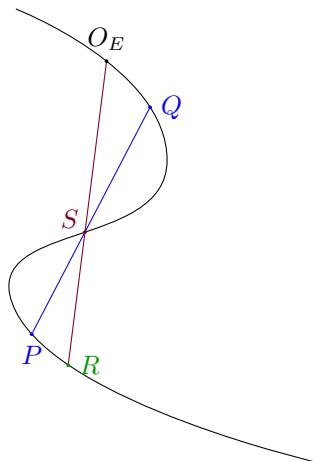


Figure 2: Illustration of the group operation on an elliptic curve

We call this the “chord and tangent process”.

**Theorem 4.1.**  $(E, \oplus)$  is an abelian group.

*Proof.*

- (i)  $P \oplus Q = Q \oplus P$  by construction.
- (ii)  $O_E$  is the identity.
- (iii) For inverses, let  $S$  be the third point of intersection of  $T_{O_E}$  and  $E$ , and  $Q$  be the third point of intersection of  $\overline{PS}$  and  $E$ . Then  $P \oplus Q = O_E$ .
- (iv) Associativity is much harder.

□

**Definition.**  $D_1, D_2 \in \text{Div}(E)$  are **linearly equivalent** (written  $D_1 \sim D_2$ ) if there is  $f \in \bar{K}(E)^\times$  such that  $\text{div}(f) = D_1 - D_2$ . Then we will let  $[D] = \{D' : D' \sim D\}$ .

**Definition.** The **Picard group of  $E$** ,  $\text{Pic}(E) = \text{Div}(E) / \sim$ . We write  $\text{Div}^0(E) := \ker \left( \text{Div}(E) \xrightarrow{\deg} \mathbb{Z} \right)$  for the group of degree 0 divisors on  $E$ , and then  $\text{Pic}^0(E) = \text{Div}^0(E) / \sim$ . Sometimes  $\text{Pic}^0$  is called the Jacobian.

**Proposition 4.2.** Let  $\psi : E \rightarrow \text{Pic}^0(E); P \mapsto [(P) - (O_E)]$ . Then:

1.  $\psi(P \oplus Q) = \psi(P) + \psi(Q)$
2.  $\psi$  is a bijection

*Proof.*

1. Referring back to Fig. 2, let  $\{\ell = 0\}$  be the line  $\overline{PQ}$ , and  $\{m = 0\}$  be the line  $\overline{O_E R}$ . Then:

$$\begin{aligned}
\operatorname{div}(\ell/m) &= (P) + (S) + (Q) - (R) - (S) - (O_E) \\
&= (P) + (Q) - (O_E) - (P \oplus Q) \\
\implies (P \oplus Q) + (O_E) &\sim (P) + (Q) \\
\implies (P \oplus Q) - (O_E) &\sim (P) - (O_E) + (Q) - (O_E) \\
\implies \psi(P \oplus Q) &= \psi(P) + \psi(Q)
\end{aligned}$$

2. For injectivity, suppose  $\psi(P) = \psi(Q)$ . Then there is  $f \in \bar{K}(E)^\times$  such that  $\operatorname{div}(f) = P - Q$ . Then  $\deg \left( E \xrightarrow{f} \mathbb{P}^1 \right) = \operatorname{ord}_P(f) = 1$ . But then  $f$  is a birational morphism, so an isomorphism, and  $E \cong \mathbb{P}^1$ .

For surjectivity, let  $[D] \in \operatorname{Pic}^0(E)$ . Then  $D + (O_E)$  has degree 1 (as  $D$  had degree 0). Then Riemann-Roch tells us  $\dim \mathcal{L}(D + (O_E)) = 1$ , and so there exists some  $f \in \bar{K}(E)^\times$  such that  $\operatorname{div}(f) + D + (O_E) \geq 0$ . Since  $f$  is rational,  $\deg \operatorname{div}(f) = 0$ , and  $\deg D = 0$ . So the coefficients of  $\operatorname{div}(f) + D + (O_E)$  are non-negative and sum to 1, hence one of them is 1 and the rest are 0. So  $\operatorname{div}(f) + D + (O_E) = (P)$  for some  $P \in E$ . But then  $(P) - (O_E) \sim D$ , i.e.  $\psi(P) = [D]$ .

□

So  $\psi$  is a bijection respecting the group law, and so we deduce that  $\oplus$  is associative, and then  $(E, \oplus) \stackrel{\psi}{\cong} (\operatorname{Pic}^0 E, +)$ .

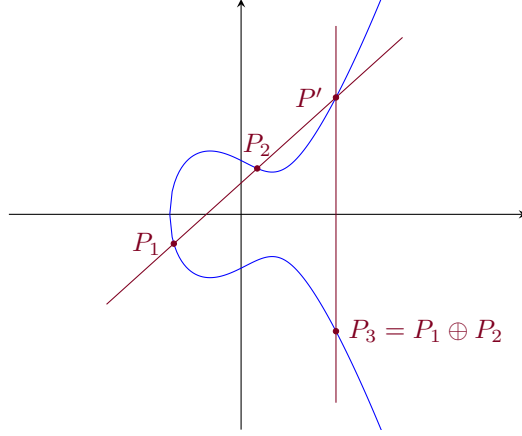
#### 4.1 Explicit Formulae for the Group Law

We consider  $E$  in Weierstrass form, with  $O_E$  the point at infinity:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (*)$$

Note that  $O_E$  is a point of inflection. Now  $P_1 \oplus P_2 \oplus P_3 = O_E \iff P_1, P_2, P_3$  are collinear.

We will use the following notation:



and put  $P_i = (x_i, y_i)$ ,  $P' = (x', y')$ .

Now  $\ominus P_1 = (x_1, -(a_1x_1 + a_3) - y_1)$ , just by setting  $y = -y_1$  in (\*).

The line through  $P_1, P_2$  has equation say  $y = \lambda x + \nu$ . Substituting into (\*) and looking at the coefficient of  $x^2$ , we get:

$$\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x'$$

Since  $x_3 = x'$ , we have:

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(a_1x' + a_3) - y' \\ &= -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

It remains to find  $\lambda$  and  $\nu$ . There are 3 cases:

1.  $x_1 = x_2, P_1 \neq P_2$ .

Then  $P_1 \oplus P_2 = O_E$ .

2.  $x_1 \neq x_2$ .

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = y_1 - \lambda x_1 = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

3.  $P_1 = P_2$ .

Here we have to compute the equation of the tangent line etc. The solutions are:

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_2 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

**Corollary 4.3.**  $E(K)$  is an abelian group.

*Proof.* It is a subgroup of  $E (= E(\bar{K}))$ .

Identity:  $O_E \in E(K)$  by definition.

Closure: See formulae above.

Inverses: See formulae above.

Associativity: Inherited from  $E(\bar{K})$ .

Commutativity: Inherited from  $E(\bar{K})$ .

□

If there is no ambiguity (i.e. we are not also adding numbers at the same time), the circles will be dropped from the group operation.

**Theorem 4.4.** *Elliptic curves are group varieties.*

i.e.,  $[-1] : E \rightarrow E; P \mapsto -P$  and  $+: E \times E \rightarrow E; (P, Q) \mapsto P + Q$  are morphisms of algebraic varieties.

*Proof.* The above formulae show that  $[-1]$  and  $+$  are rational maps. We know immediately that  $[-1]$  is a morphism, as it is a rational map from a smooth curve to a projective variety.

The formulae also show that  $+$  is regular on the set

$$U = \{(P, Q) \in E \times E \mid P, Q, P + Q, P - Q \neq O_E\}$$

For  $P \in E$ , let  $\tau_P : E \rightarrow E; X \mapsto P + X$  be the “translation by  $P$ ” map.

Then  $\tau_P$  is a rational map from a smooth curve to a projective variety, so is a morphism.

We factor  $+$  as:

$$E \times E \xrightarrow{\tau_{-A} \times \tau_{-B}} E \times E \xrightarrow{\tau_{A+B}} E \xrightarrow{\tau_{A+B}} E$$

Now  $+$  is regular on  $(\tau_A \times \tau_B)(U)$  for all  $A, B \in E$ , and so  $+$  is regular on  $E \times E$ . □

**Definition.** For any  $n \in \mathbb{Z}_{>0}$ , let  $[n] : E \rightarrow E; P \mapsto P + \dots + P$ ,  $n$  times, and  $[-n] = [-1] \circ [n]$ ,  $[0] : P \mapsto O_E$  (i.e., the standard way of turning an abelian group into  $\mathbb{Z}$  module).

**Definition.** The  *$n$ -torsion* subgroup of  $E$  is  $E[n] = \ker([n] : E \rightarrow E)$ .

**Lemma 4.5.** *If  $\text{char}(K) \neq 2$ , and  $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$ .*

*Then  $E[2] = (0, (e_1, 0), (e_2, 0), (e_3, 0)) \cong (\mathbb{Z}/2\mathbb{Z})^2$ .*

*Proof.* Let  $P = (x, y) \in E$ . Then  $[2]P = 0 \iff P = -P \iff (x, y) = (x, -y) \iff y = 0$ . □

## 4.2 Elliptic Curves over $\mathbb{C}$

Let  $\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}$ , where  $\omega_1, \omega_2$  form a basis for  $\mathbb{C}$  over  $\mathbb{R}$ .

Then the meromorphic functions on the Riemann surface (or lattice)  $\mathbb{C}/\Lambda$  are the same as the  $\Lambda$ -invariant meromorphic functions on  $\mathbb{C}$  (i.e.  $f(z) = f(z + \lambda)$  for  $\lambda \in \Lambda$ ).

This set of functions is a field, and is generated by  $\wp(z)$  and  $\wp'(z)$ , where:

$$\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \lambda \in \Lambda} \left( \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right)$$

They satisfy  $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ , for some  $g_1, g_3 \in \mathbb{C}$  depending on  $\lambda$ . We call  $\wp$  the **Weierstrass  $p$ -function**.

One can show that  $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ , where  $E$  is the elliptic curve  $y^2 = 4x^3 - g_2x - g_3$ . This is an isomorphism, not only of Riemann surfaces, but moreover of groups

**Theorem 4.6** (Uniformisation Theorem). *Every elliptic curve over  $\mathbb{C}$  arises in this way.*

Thus, for elliptic curves  $E/\mathbb{C}$ , we have:

$$\textcircled{1} \quad E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$$

$$\textcircled{2} \quad \deg[n] = n^2$$

We will show that  $\textcircled{2}$  holds over any field  $K$ , and  $\textcircled{1}$  holds if  $\text{char } K \nmid n$ .