Elliptic Curves

October 12, 2020

1 Fermat's Method of Infinite Descent

Suppose we have a right-angled triangle Δ 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. *Δ 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 $a^2 + b^2 \equiv 2 \mod 4$, 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. □

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. □

Fermat showed that 1 is not a congruent number.

Theorem 1.5. *There is no solution to*

$$w^2 = uv(u + v)(u - v) \tag{$*$}$$

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 $u \not\equiv v \mod 2$, 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 $\lightning$. Hence there is no solution to $(*)$. □

1.1 A Variant for Polynomials

Here, K is a field with $\operatorname{char} K \neq 2$. 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 $u, v \in K$. □

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

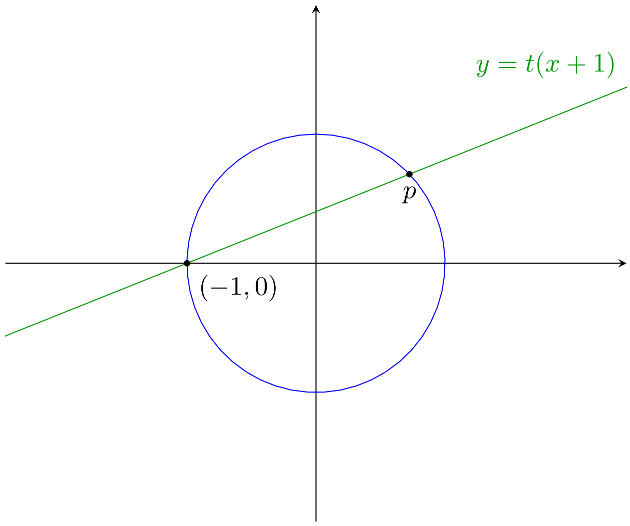
We will be working over an algebraically closed field K.

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

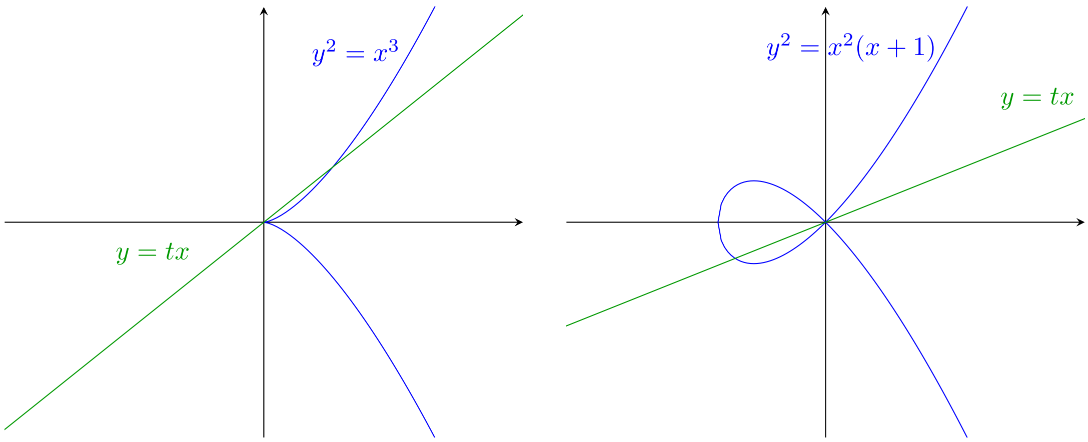
Examples 2.2.

1. 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 $(x,y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$

2. Any singular plane cubic is rational.



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

(b) Left as an example on the first sheet

3. 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 $g(C) =$ 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 $\mathrm{ord}_P(f)$ to mean the order of vanishing of $f \in K(C)$ at P (negative if f has a pole).

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

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

Example 2.5. Let $C = \{g(x, y) = 0\} \subseteq \mathbb{A}^2$, where $g \in K[x, y]$ is irreducible. Then $K(C) = \mathrm{Frac}\, \frac{K[x,y]}{(g)}$, with $g = g_0 + g_1(x, y) + g_2(x, y) + \ldots$, 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 α, β 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 $\mathrm{ord}_P(x)$ and $\mathrm{ord}_P(y)$. 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 $\mathrm{ord}_P(t) = \mathrm{ord}_P(t-2) = \mathrm{ord}_P(t-\lambda w) = 1$, and $\mathrm{ord}_P(w) = 1+1+1 = 3$.

Then:

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

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 $\mathrm{Div}(C)$.

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 $\mathrm{div}(f) = \sum_{P\in C} \mathrm{ord}_P(f) P$.

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

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

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)**.**

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

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 $\mathrm{ord}_P(x) = -2, \mathrm{ord}_P(x) = -3$.

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