Part III - Elliptic Curves

Lectured by Tom Fisher

Artur Avameri

Contents

0 Introduction

The best books for the course include *The arithmetic of elliptic curves* by Silverman, Springer 1996, and *Lectures on elliptic curves* by Cassels, CUP 1991.

1 Fermat's Method of Infinite Descent

A right–angled triangle Δ has $a^2 + b^2 = c^2$ and $\operatorname{area}(\Delta) = \frac{1}{2}ab$.

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

Note that a primitive triangle has pairwise coprime side lengths because $a^2 + b^2 = c^2$.

Lemma 1.1. Every primitive triangle is of the form $(u^2 - v^2, 2uv, u^2 + v^2)$ for some integers $u > v > 0$.

Proof. WLOG let a, b, c be odd, even, odd. Then $\left(\frac{b}{2}\right)^2 = \frac{c+a}{2}\frac{c-a}{2}$, where we note that the RHS is a product of positive coprime integers. By unique factorization, $\frac{c+a}{2} = u^2$, $\frac{c-a}{2} = v^2$ for $u, v \in \mathbb{Z}$. This gives the desired result. $\square$

Definition 1.2. $D \in \mathbb{Q}_{>0}$ is a **congruent** number if there exists a rational triangle Δ with $\operatorname{area}(\Delta) = D$.

Note that it suffices to consider $D \in \mathbb{Z}_{>0}$ squarefree.

Example 1.1. $D = 5, 6$ are congruent.

Lemma 1.2. $D \in \mathbb{Q}_{>0}$ is congruent $\iff Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}, y \neq 0$.

Proof. Lemma 1.1 shows that D congruent $\implies Dw^2 = uv(u^2 - v^2)$ for some $u, v, w \in \mathbb{Q}, w \neq 0$. This implication also obviously goes the other way. To finish, divide through by w^4 and take $x = \frac{u}{v}, y = \frac{w}{v^2}$. $\square$

Fermat showed that 1 is not a congruent number.

Theorem 1.3. There is no solution to $w^2 = uv(u + v)(u - v)$ for $u, v, w \in \mathbb{Z}, w \neq 0$.

Proof. WLOG assume u, v are coprime and that $u, w > 0$. If $v < 0$, then replace (u, v, w) by $(-v, u, w)$. If u, v are both odd, then replace (u, v, w) by $\left(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2}\right)$. Then $u, v, u+v, u-v$ are pairwise coprime positive integers with their product a square, so by unique factorization in $\mathbb{Z}$, $u = a^2, v = b^2, u + v = c^2, u - v = d^2$ for $a, b, c, d \in \mathbb{Z}$.

Since $u \not\equiv v \pmod 2$, both c and d are odd. Then $\left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2+d^2}{2} = u = a^2$. This gives a primitive triangle with area $\frac{c^2-d^2}{8} = \frac{v}{4} = \left(\frac{b^2}{2}\right)$.

Let $w_1 = \frac{b}{2}$, then by Lemma 1.1, $w_1^2 = u_1 v_1 (u_1 + v_1)(u_1 - v_1)$ for some $u_1, v_1 \in \mathbb{Z}$. Hence we have a new solution to our original question, with $4w_1^2 = b^2 = v \mid w^2 \implies w_1 \le \frac{w}{2}$, so we're done by infinite descent. $\square$

A variant for polynomials. In the above, K is a field with char $K \neq 2$. Let $\overline{K}$ be the algebraic closure of K and consider for this whole section K with char $K \neq 2$.

Lemma 1.4. Let $u, v \in K[t]$ be coprime. If $\alpha u + \beta v$ is a square for 4 distinct $(\alpha : \beta) \in \mathbb{P}^1$, then $u, v \in K$.

Proof. WLOG let $K = \overline{K}$ by extending if necessary. Changing coordinates on $\mathbb{P}^1$ (i.e. multiplying by a 2×2 invertible matrix), we may assume that the points $(\alpha : \beta)$ are $(1 : 0)$, $(0 : 1)$, $(1 : -1)$, $(1 : -\lambda)$ for $\lambda \in K \setminus \{0, 1\}$. Since our field is algebraically closed, let $\mu = \sqrt{\lambda}$. Then $u = a^2, v = b^2, u - v = (a + b)(a - b), u - \lambda v = (a + \mu b)(a - \mu b)$.

Unique factorization in $K[t]$ implies that $a + b, a - b, a + \mu b, a - \mu b$ are squares (since the necessary terms are coprime up to units, i.e. constants). But $\max(\deg(a), \deg(b)) \le \frac{1}{2} \max(\deg(u), \deg(v))$, so by Fermat's method of infinite descent, $u, v \in K$. $\square$

Definition 1.3. (i) An **elliptic curve** E/K is the projective closure of the plane affine curve $y^2 = f(x)$ (this is called a Weierstrass equation) where $f \in K[x]$ is a monic cubic polynomial with distinct roots in $\overline{K}$.

(ii) For L/K any field extension, $E(L) = \{(x, y) \in L^2 \mid y^2 = f(x)\} \cup \{0\}$ (the point at infinity in the projective closure), it turns out that $E(L)$ is naturally an abelian group.

In this course, we study $E(K)$ for K a finite field, local field, number field.

Lemma 1.2 and Theorem 1.3 show that if $E : y^2 = x^3 - x$, then $E(\mathbb{Q}) = \{0, (0, 0), (\pm 1, 0)\}$.

Corollary 1.5. Let E/K be an elliptic curve. Then $E(K(t)) = E(K)$.

Proof. WLOG $K = \overline{K}$. By a change of coordinates, we may assume $y^2 = x(x - 1)(x - \lambda)$ for some $\lambda \in K \setminus \{0, 1\}$. Suppose $(x, y) \in E(K(t))$. Write $x = \frac{u}{v}$ for $u, v \in K(t)$ coprime. Then $w^2 = uv(u - v)(u - \lambda v)$ for some $w \in K[t]$. Unique factorization in $K[t]$ shows that $u, v, u - v, u - \lambda v$ are all squares, so by Lemma 1.4, $u, v \in K$, so $x, y \in K$. $\square$