Definitions and Theorems from Elliptic Curves

Isaac Martin

Last compiled February 6, 2022

Contents

1 Fermat's Method of Infinite Descent

Definition 1.1 (Rational Triangle)**.** Let a,b,c be the side lengths of a right triangle Δ.

1. Δ is *rational* if $a,b,c \in \mathbb{Q}$.
2. Δ is *primitive* if $a,b,c \in \mathbb{Z}$ and are pairwise coprime.

Lemma 1.2 (Lemma 1.1)**.** Every primitive triangle has side lengths of the form u^2+v^2, $2uv$, and u^2-v^2 for some integers $u > v > 0$.

Definition 1.3. $D \in \mathbb{Q}_{>0}$ is a *congruent number* if there exists a rational triangle Δ with $\text{area}(\Delta) = 0$.

N.B. it suffices to to consider D a positive integer which is squarefree, e.g. $D = 5,6$ are congruent.

Lemma 1.4 (Lemma 1.2)**.** $D \in \mathbb{Q}_{>0}$ is congruent if and only if $Dy^2 = x^3 - x$ for some $x,y \in \mathbb{Q}$ with $y \neq 0$.

Theorem 1.5. *There is no solution to*

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

for $u,v,w \in \mathbb{Z}$ and $w \neq 0$.

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

Corollary 1.7 (1.6 in Lecture)**.** Let E/K be an elliptic curve. Then $E(K(t)) = E(K)$.

Proof. Without loss of generality may assume $K = \overline{K}$. 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 $x = \frac{u}{v}$ for coprime polynomials $u,v \in K[t]$. Then

$$w^2 = uv(u-v)(u-\lambda v)$$

for some $w \in K[t]$. Because $K[t]$ is a UFD, we get that $u, v, u-v$, and $u-\lambda v$ are all squares in $K[t]$ and then Lemma $\square$

2 Remarks on Algebraic Curves

Definition 2.1. A plane curve $\{f(x,y) = 0 \mid (x,y) \in K = \overline{K}\} \subseteq \mathbb{A}^2$ (with f irreducible over $\overline{K}$) is said to be **rational** if it has a rational parameterization, i.e. $\exists \phi, \psi \in K(t)$ such that

(i) $\mathbb{A}^1 \to \mathbb{A}^2$ defined $t \mapsto (\phi(t), \psi(t))$ is an injection on $\mathbb{A}^1 \setminus \{\text{finite set}\}$

(ii) $f(\phi(t), \psi(t)) = 0$

Definition 2.2 (Riemann-Roch Space)**.** Let C be a smooth projective curve. The Riemann-Roch space of a $D \in \mathrm{Div}(C)$ is

$$\mathcal{L}(D) = \left\{ f \in K(C)^* \;\middle|\; \mathrm{div}(f) + D \geq 0 \right\} \cup \{0\}$$

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

Here, the space $K(C)$ is $\mathrm{Frac}\left(K[x_1, ..., x_n]/(F)\right)$