Definitions and Theorems from Elliptic Curves

Isaac Martin

Last compiled January 27, 2022

---

§ *21 - Jan - 2022*

Definition 0.1 (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 0.2 (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 0.3. $D \in \mathbb{Q}_{>0}$ is a *congruent number* if there exists a rational triangle Δ with $\text{lcm}(\Delta) = 0$.

§ *24 - Jan - 2022*

Corollary 0.4 (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 □

§ *26 – Jan – 2022*

Definition 0.5 (Riemann-Roch Space)**.** Let C be a smooth projective curve. The Riemann-Roch space of a $D \in (C)$ is

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

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