Millenium Problems: The Birch and Swinnerton-Dyer conjecture (Part II)

**Conjecture:** Let $E$ be an elliptic curve over a number field $K$ with

\[ L_E(K)(s) := \prod_{p \text{ prim}} \frac{1}{1-(p+1-N_p)p^{-s}p^{1-2s)}, s \in \mathbb{C}, \text{Re } s > \frac{3}{2} \]

\[ , N_p = \# \{ \text{solutions of } y^2 \equiv x^3 + ax + b \text{ mod } p \} \]

having an analytic extension to the complex plane. Let $r$ denote the rank of $E(K)$. Then $r$ is equal to the order of the zero of $L_E(K)(s)$ at the point $s = 1$.

**Proposition:** $E(\mathbb{Q})$ is an abelian group with identity element 0 and the composition “+”.

**Theorem (Mordell, 1922):** If $E$ is an elliptic curve over $\mathbb{Q}$, then

\[ E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{Tors}. \]

for some integer $r \geq 0$, where $E(\mathbb{Q})_{Tors.}$ is a finite abelian group.

**Remark:** If we want to study the rational solutions of a curve $C$ it is the genus that tells us how complicated the curve is.

**Theorem:** Let $C$ be an irreducible curve of order $n$ with $m$ double points as its only singularities. Then

\[ g = g(C) = \frac{(n-1)(n-2)}{2} - m \]

is a non-negative integer.

$g(C)$ is called the **genus** of the (irreducible) curve $C$.

**Theorem (Hilbert & Hurwitz, 1890):** If the genus of a curve is zero, then it is birationally equivalent to either a line or a conic and $C(\mathbb{Q})$ is infinite.

**Theorem (Faltings, 1983):** If the genus of $C$ is greater than or equal to 2, then $C(\mathbb{Q})$ is finite.

**Definition:** An elliptic curve $E$ is a curve with genus 1.