13.2 The Birch and Swinnerton-Dyer Conjecture

Let E be the elliptic curve over $\mathbb{Q}$ defined by

$$y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$. For $p \nmid \Delta$, let

$$a_p = p + 1 - \#E(\mathbb{Z}/p\mathbb{Z}).$$

Set

$$L^*(E,s) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Theorem 13.2.1 (Breuil, Conrad, Diamond, Taylor, Wiles). *$L^*(E,s)$ extends to an analytic function on all of $\mathbb{C}$.*

Definition 13.2.2 (Algebraic Rank). The *algebra rank* of E is the unique nonnegative integer r such that $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}} \approx \mathbb{Z}^r$.

Definition 13.2.3 (Analytic Rank). The Taylor expansion of $L(E,s)$ at $s = 1$ has the form

$$L^*(E,s) = c(s-1)^r + \text{higher order terms}$$

with $c \neq 0$. This number r is called the *analytic rank* of E.

Conjecture 13.2.4 (Birch and Swinnerton-Dyer). *The analytic and algebraic ranks of E are the same. That is, the order of vanishing of $L^*(E,s)$ at $s = 1$ is the same as the minimal number of generators of $E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tor}}$.*

Note that a special case of the conjecture is the assertion that $L(E,1) = 0$ if and only if $E(\mathbb{Q})$ is infinite. This special case would be enough to give a complete solution to the congruent number problem.

13.2.1 Some of What is Known

Theorem 13.2.5 (Gross, Kolyvagin, Zagier, et al.). *Let E be an elliptic curve. If the analytic rank of E is 0 or 1, then Conjecture 13.2.4 is true.*

It is a folklore conjecture that “most” elliptic curves satisfy the hypothesis of the above theorem, i.e., they have analytic rank 0 or 1. For example, just over 95% of the “first 78198” elliptic curves have analytic rank at most 1. Many mathematicians suspect that the curves with rank bigger than 1 have “density” 0 amongst all elliptic curves. However, in practice it is often the curves of rank bigger than 1 that are interesting.