An Introduction to the Birch–Swinnerton-Dyer Conjecture, Part I

Sebastian Pancratz

18 May 2009

1 Foreword

In the next two talks, Frank Gounelas and I will try to give a brief introduction to the Birch–Swinnerton-Dyer Conjecture, largely if not exclusively following a short series of lectures held recently by Tim Dokchitser at the workshop *Counting Points on Varieties* at Leiden.

2 Elliptic Curves

Let K be a field, which we will usually take to be $\mathbb{Q}$ or more generally a number field.

Definition 1. An *elliptic curve* E/K in *Weierstrass form* is given by a non-singular equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_1, \dots, a_6 \in K$. If the characteristic of K is not 2 or 3 this can be simplified to

$$y^2 = x^3 + Ax + B.$$

The *discriminant* Δ is a quantity associated to the defining equation of an elliptic curve, which in case of the simplified form is given by $-16(4A^3 + 27B^2)$. Note that a curve is non-singular if and only if $\Delta \neq 0$.

Definition 2. The set of K-rational points of an elliptic curve is

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}_E\},$$

where $\mathcal{O}_E$ is the point at infinity.

One can endow $E(K)$ with an abelian group structure and we have the following result.

Theorem 3 (Mordell–Weil)**.** Let K be a number field. Then $E(K)$ is a finitely generated abelian group, that is, we can write $E(K) \cong \mathbb{Z}^r \oplus T$, where $T = E(K)_{\mathrm{tors}}$ is the *torsion group* and $r = \operatorname{rank} E/K$ is the *Mordell–Weil rank*.

3 Elliptic Curves over Finite Fields

In this section, we let $K = \mathbb{F}_q$. Then $E(K)$ is a finite abelian group.

Theorem 4 (Hasse–Weil)**.** Let $E/\mathbb{F}_q$ be an elliptic curve. Then there exist $\alpha, \beta \in \mathbb{C}$ such that, for all $n \in \mathbb{N}$,

$$\#E(\mathbb{F}_{q^n}) = q^n - \alpha^n - \beta^n + 1.$$

Moreover, $|\alpha| = |\beta| = \sqrt{q}$.

Corollary 5. Continuing with the notation from above, if we set $a_q = \alpha+\beta$ then $\#E(\mathbb{F}_q) = q+1-a_q$ and $|a_q| \le 2\sqrt{q}$.

This is equivalent to the statement that the ζ-function of $E/\mathbb{F}_q$

$$\zeta_{E/\mathbb{F}_q}(T) = \exp\left(\sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{q^n})}{n} T^n\right)$$

has the form

$$\zeta_{E/\mathbb{F}_q}(T) = \frac{(1-\alpha T)(1-\beta T)}{(1-T)(1-qT)} = \frac{1-a_qT+qT^2}{(1-T)(1-qT)}.$$

This is checked in Problem 1.

At this point, we have gathered enough information to present a very simple form of the BSD Conjecture. Given an elliptic curve $E/\mathbb{Q}$, we can apply a change of co-ordinates such that $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. For primes p of good reduction, in particular when $p \nmid \Delta$, we obtain an elliptic curve $\tilde{E}/\mathbb{F}_p$ by reducing the coefficients A and B modulo p. We consider the quantity $f_E(x) = \prod_{p<x} \#\tilde{E}(\mathbb{F}_p)/p$.

Definition 6 (Birch–Swinnerton-Dyer; Naive form)**.** For an elliptic curve $E/\mathbb{Q}$, there is a constant K_E such that

$$f_E(x) \sim K_E(\log x)^{\operatorname{rank} E/\mathbb{Q}}.$$

4 The Global ζ-function of an Elliptic Curve

Definition 7. A Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

of an elliptic curve $E/\mathbb{Q}$ is *globally minimal* if $a_1, \dots, a_6 \in \mathbb{Z}$ and $|\Delta| \in \mathbb{N}$ is minimal among all such models.

For a general number field K, a model is *minimal at* a prime P of K if $v_P(a_i) \ge 0$ for all $i = 1, \dots, 6$ and $v_P(\Delta)$ is minimal among all such models. It is *globally minimal* if it is minimal at all primes P of K.

Definition 8. With the above notation, if $v_P(a_i) \ge 0$ for all $i = 1, \dots, 6$ and $v_P(\Delta) < 12$ then the model is minimal at P. The converse fails for $P \nmid 2, 3$.

The reduction $\tilde{E}$ of $E/\mathbb{Q}$ at p is the curve over $\mathbb{F}_p$ obtained by reducing a minimal model at p. Similarly, if E/K is an elliptic curve over a number field and P is the unique prime of K lying above p then we reduce a minimal model at P.

Definition 9. The *global ζ-function* of an elliptic curve $E/\mathbb{Q}$ is defined as

$$\zeta_{E/\mathbb{Q}}(s) = \prod_p \zeta_{\tilde{E}/\mathbb{F}_p} = \prod_p \frac{f_p(p^{-s})}{(1-p^{-s})(1-p^{1-s})},$$

where $f_p(T)$ is defined as $1 - a_pT + pT^2$ if $p \nmid \Delta$ and $1 - a_pT$ otherwise.

The *L-function* of $E/\mathbb{Q}$ is denoted $L(E/\mathbb{Q}, s)$ and defined such that

$$\zeta_{E/\mathbb{Q}}(s) = \frac{\zeta(s)\zeta(s-1)}{L(E/\mathbb{Q}, s)},$$

that is,

$$L(E/\mathbb{Q}, s) = \prod_p \frac{1}{f_p(p^{-s})} = \prod_{p|\Delta} \frac{1}{1-a_pp^{-s}} \prod_{p\nmid\Delta} \frac{1}{1-a_pp^{-s}+p^{1-2s}} = \sum_{n\ge1} \frac{a_n}{n^s},$$

on regrouping the terms as a Dirichlet series.

In Problem 5, it is shown that the L-function converges for $\Re(s) > 3/2$. Note that the re-use of the notation for a_q, previously defined as $a_q = q + 1 - \#\tilde{E}(\mathbb{F}_q)$, in the Dirichlet series above is justified as the values coincide.

Over a more general number field K, the definition is modified as follows. We let

$$L(E/K, s) = \prod_P f_P(q^{-s})^{-1}$$

where $q = N(P) = [\mathcal{O}_K : P]$,

$$f_P(T) = \begin{cases} 1 - a_P T + qT^2 & P \nmid \Delta \\ 1 - a_P T & P \mid \Delta \end{cases}$$

and $a_P = q + 1 - \#\tilde{E}(\mathbb{F}_q)$.

5 Problems

Problem 1. Let $E/\mathbb{F}_q$ be an elliptic curve. Show that the Hasse–Weil theorem, namely that, for all $n \geq 1$,

$$\#E(\mathbb{F}_{q^n}) = q^n - \alpha^n - \beta^n + 1,$$

is equivalent to the statement that the ζ-function of $E/\mathbb{F}_q$ has the form

$$\zeta_{E/\mathbb{F}_q}(T) = \frac{1 - a_q T + qT^2}{(1-T)(1-qT)}$$

where $a_q = q + 1 - \#E(\mathbb{F}_q)$. Here, it may be assumed that $\alpha\beta = q$. Assuming the Hasse–Weil inequality $|\#E(\mathbb{F}_{q^n}) - q^n - 1| \leq 2\sqrt{q^n}$ for $n \geq 1$, show furthermore that $|\alpha| = |\beta| = \sqrt{q}$ and that the zeroes of the function $\zeta_{E/\mathbb{F}_q}(q^{-s})$, for $s \in \mathbb{C}$, lie on the line $\mathbb{R}(s) = 1/2$ ("Riemann hypothesis").

Problem 2. Let $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ be an elliptic curve, and $E_d/\mathbb{Q} : dy^2 = x^3 + Ax + B$ its quadratic twist by some square-free integer $d > 1$. Show that

$$\operatorname{rank} E/\mathbb{Q}(\sqrt{d}) = \operatorname{rank} E/\mathbb{Q} + \operatorname{rank} E_d/\mathbb{Q}.$$

Problem 3. Let F/K be an odd degree Galois extension, and E/K an elliptic curve. Show that

$$\operatorname{rank} E/F \equiv \operatorname{rank} E/K \pmod 2.$$

Problem 4. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 1$ and consider its L-series,

$$L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Show that $a_p = 0$ for all primes p congruent to 2 modulo 3. Deduce that $a_n = 0$ for all $n \not\equiv 1 \pmod 3$.

Problem 5. Show that the L-function of an elliptic curve $E/\mathbb{Q}$ converges for $\Re(s) > 3/2$.