Lecture 35: The Birch and Swinnerton-Dyer Conjecture, Part 2

William Stein

Math 124 Harvard University **Fall 2001**

1 The BSD Conjecture

Let E be an elliptic curve over $\mathbb{Q}$ given by an equation

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

with $a, b \in \mathbb{Z}$. For $p \nmid \Delta = -16(4a^3 + 27b^2)$, let $a_p = p + 1 - \#E(\mathbb{Z}/p\mathbb{Z})$. Let

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

Theorem 1.1 (Breuil, Conrad, Diamond, Taylor, Wiles). *$L(E, s)$ extends to an analytic function on all of $\mathbb{C}$.*

Conjecture 1.2 (Birch and Swinnerton-Dyer). *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 $c \neq 0$ and $E(\mathbb{Q}) \approx \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tor}}$.

A special case of the conjecture is the assertion that $L(E, 1) = 0$ if and only if $E(\mathbb{Q})$ is infinite. The assertion "$L(E, 1) = 0$ implies that $E(\mathbb{Q})$ is infinite" is the part of the conjecture that secretely motives much of my own research.

2 What is Known

On page 5 of Wiles's paper, he discusses the history of the following theorem.

Theorem 2.1 (Gross, Kolyvagin, Zagier, et al.). *Suppose that*

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

with $r \leq 1$. Then the Birch and Swinnerton-Dyer conjecture is true for E, that is, $E(\mathbb{Q}) \approx \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$.

I suspect that most elliptic curves satisfy the hypothesis of the above theorem, i.e., they have rank 0 or 1. For example, almost 96% of the “first 78198” elliptic curves have $r \leq 1$. I suspect that the curves with $r > 1$ have “density” 0 amongst all elliptic curves. This doesn't mean that we are done. In practice it is often the curves with $r > 1$ that are interesting and useful, and experts can still be observed saying “almost nothing is known about the Birch and Swinnerton-Dyer conjecture”.

3 How to Compute $L(E, s)$ with a Computer

3.1 Best Models

Let E be an elliptic curve over $\mathbb{Q}$, defined by a Weierstrass equation

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

There are many choices of Weierstrass equations that define an elliptic curve that is “essentially the same” as E. E.g., you found others by completing the square. Among all of these, there is a best possible model, which is the one with smallest discriminant. It can be computed in PARI as follows:

```
? E = ellinit([0,0,0,-43,166]);
? E.disc
%61 = -6815744
? E = ellchangecurve(E,ellglobalred(E)[2])
%62 = [1, -1, 1, -3, 3, ...]
? E.disc
%63 = -1664
```

Thus $y^2 + xy + y = x^3 - x^2 - 3x + 3$ is a “better” model than $y^2 = x^3 - 43x + 166$.

WARNING: Some of the elliptic curves functions in PARI will *LIE* if you give as input an elliptic curve that is defined by a model that isn't the best possible. These devious liars include `elltors, ellap, ellak`, and `elllseries`.

3.2 Formula for $L(E, s)$

As mentioned before, the PARI function `elllseries` can compute $L(E, s)$. I figured out how this function works, and explain it below.

Because E is modular, one can show that we have the following rapidly-converging series expression for $L(E, s)$, for $s > 0$:

$$L(E, s) = N^{-s/2} \cdot (2\pi)^s \cdot \Gamma(s)^{-1} \cdot \sum_{n=1}^{\infty} a_n \cdot (F_n(s-1) - \varepsilon F_n(1-s))$$

where

$$F_n(t) = \Gamma\left(t+1, \frac{2\pi n}{\sqrt{N}}\right) \cdot \left(\frac{\sqrt{N}}{2\pi n}\right)^{t+1}.$$

Here

$$\Gamma(z) = \int_0^\infty t^{z-1} e^{-t} dt$$

is the Γ-*function* (e.g., $\Gamma(n) = (n-1)!$), and

$$\Gamma(z, \alpha) = \int_\alpha^\infty t^{z-1} e^{-t} dt$$

is the *incomplete* Γ-*function*. The number N is called the *conductor* of E and is very similar to the discriminant of E; it is only divisible by primes that divide the best possible discriminant of E. You can compute N using the PARI command `ellglobalred(E)[1]`.

As usual, for $p \nmid \Delta$, we have

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

for $r \geq 2$,

$$a_{p^r} = a_{p^{r-1}} a_p - p a_{p^{r-2}},$$

and $a_{nm} = a_n a_m$ if $\gcd(n, m) = 1$, (I won't define the a_p when $p \mid \Delta$, but it's not difficult.) Finally, ε depends only on E and is either $+1$ or -1. I won't define ε either, but you can compute it in PARI using `ellrootno(E)`.

At $s = 1$, the formula can be massively simplified, and we have

$$L(E, 1) = (1 + \varepsilon) \cdot \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}}.$$

This sum converges rapidly, because $e^{-2\pi n/\sqrt{N}} \to 0$ quickly as $n \to \infty$.

4 A Rationality Theorem

In the last lecture, I mentioned that it is incredibly difficult to say anything precise about $L(E, s)$, even with the above formulas. For example, it is a very deep theorem (Gross-Zagier) that there is an elliptic curve such that

$$L(E, s) = c(s-1)^3 + \text{ higher terms},$$

and nobody has any idea how to prove that there is an elliptic curve with

$$L(E, s) = c(s-1)^4 + \text{ higher terms}.$$

Fortunately, it is possible to decide whether or not $L(E, 1) = 0$.

Theorem 4.1. *Let $y^2 = x^3 + ax + b$ be an elliptic curve. Let*

$$\Omega_E = \int_\gamma^\infty \frac{dx}{\sqrt{x^3 + ax + b}},$$

where γ is the largest real root of $x^3 + ax + b$. Then

$$\frac{L(E,1)}{\Omega_E} \in \mathbb{Q}$$

and it is straightforward in any particular case to bound the denominator of that rational number.

In practice, one computes this integral using the "Arithmetic-Geometric Mean". In PARI, Ω_E is approximated by `E.omega[1]` (times a small power of 2).

Example 4.2. Let E be the elliptic curve $y^2 = x^3 - 43x + 166$. We compute $L(E,1)$ using the above formula and observe that $L(E,1)/\Omega_E$ appears to be a rational number, as predicted by the theorem.

```
? E = ellinit([0,0,0,-43,166]);
? E = ellchangecurve(E, ellglobalred(E)[2]);
? eps = ellrootno(E)
%77 = 1
? N = ellglobalred(E)[1]
%78 = 26
? L = (1+eps) * sum(n=1,100, ellak(E,n)/n * exp(-2*Pi*n/sqrt(N)))
%79 = 0.6209653495490554663758626727
? Om = E.omega[1]
%80 = 4.346757446843388264631038710
? L/Om
%81 = 0.1428571428571428571428571427
? contfrac(L/Om)
%84 = [0, 7]
? 1/7.0
%85 = 0.1428571428571428571428571428
? elltors(E)
%86 = [7, [7], [[1, 0]]]
```

Notice that in this example, $L(E,1)/\Omega_E = 1/7 = 1/\#E(\mathbb{Q})$. This is shadow of a more refined conjecture of Birch and Swinnerton-Dyer.

Monday's lecture will be filled with numerical examples and numerical evidence for the Birch and Swinnerton-Dyer conjecture. Wednesday's lecture will be a review for the take-home **FINAL EXAM**.