Lecture 36: The Birch and Swinnerton-Dyer Conjecture, Part 3

William Stein

Math 124 HARVARD UNIVERSITY **Fall 2001**

1 A Rationality Theorem

In the last lecture, I mentioned that it can be surprisingly difficult to say anything precise about $L(E, s)$, even with the above formulas. For example, it is a very deep theorem of Gross and Zagier that for the elliptic curve $y^2 + y = x^3 - 7x + 6$ we have

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

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

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

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

Theorem 1.1. *Let $y^2 = x^3 + ax + b$ be an elliptic curve. Let*

$$\Omega_E = 2^n \int_\gamma^\infty \frac{dx}{\sqrt{x^3 + ax + b}},$$

where γ is the largest real root of $x^3 + ax + b$, and $n = 0$ if $\Delta(E) < 0$, $n = 1$ if $\Delta(E) > 0$. Then

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

and the denominator is ≤ 24.

In practice, one computes Ω_E using the "Arithmetic-Geometric Mean", *NOT* numerical integration. In PARI, Ω_E is approximated by `E.omega[1]*2^(E.disc>0)`.

Remark 1.2. I don't know if the denominator is ever really as big as 24. It would be a fun student project to either find an example, or to understand the proof that the quotient is rational and prove that 24 can be replaced by something smaller.

Example 1.3. 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 = 0.62096534954905546637586267 27
? Om = E.omega[1]*2^(E.disc>0)
%80 = 4.3467574468433882646310387 10
? L/Om
%81 = 0.14285714285714285714285714 27
? contfrac(L/Om)
%84 = [0, 7]
? 1/7.0
%85 = 0.14285714285714285714285714 28
? 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.

Example 1.4. In this example, we verify that $L(E,1) = 0$ computationally.

```
? E=ellinit([0, 1, 1, -2, 0]);
? L1 = elllseries(E,1)
%4 = -6.8812351511334265458947124 38 E-29
? Omega = E.omega[1]*2^(E.disc>0)
%5 = 4.9804251217101101506427155 83
? L1/Omega
%6 = 1.7957323532525030360749276 34 E-20
```

2 Approximating the Rank

Fix an elliptic curve E over $\mathbb{Q}$.

The usual method to *approximate* the rank is to find a series that rapidly converges to $L^{(r)}(E,1)$ for $r = 0, 1, 2, 3, \ldots$, then compute $L(E,1)$, $L'(E,1)$, $L^{(2)}(E,1)$, etc., until one appears to be nonzero. You can read about this method in §2.13 of Cremona's book *Algorithms for Elliptic Curves*. For variety, I will describe a slightly different method that I've played with recently, which uses the formula for $L(E,s)$ from the last lecture, the definition of the derivative, and a little calculus.

Proposition 2.1. *Suppose that*

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

Then

$$\lim_{s\to 1} (s-1) \cdot \frac{L'(E,s)}{L(E,s)} = r.$$

Proof. Write

$$L(s) = L(E,s) = c_r(s-1)^r + c_{r+1}(s-1)^{r+1} + \cdots .$$

Then

$$\begin{aligned}\lim_{s\to 1}(s-1)\cdot\frac{L'(s)}{L(s)} &= \lim_{s\to 1}(s-1)\cdot\frac{rc_r(s-1)^{r-1}+(r+1)c_{r+1}(s-1)^r+\cdots}{c_r(s-1)^r+c_{r+1}(s-1)^{r+1}+\cdots}\\ &= r\cdot\lim_{s\to 1}\frac{c_r(s-1)^r+\frac{(r+1)}{r}c_{r+1}(s-1)^{r+1}+\cdots}{c_r(s-1)^r+c_{r+1}(s-1)^{r+1}+\cdots}\\ &= r.\end{aligned}$$

□

Thus the rank r is "just" the limit as $s \to 1$ of a certain (smooth) function. We know this limit is an integer. But, for example, for the curve

$$y^2 + xy = x^3 - x^2 - 79x + 289$$

nobody has succeeded in proving that this integer limit is 4. (One can prove that the limit is either 2 or 4.)

Using the definition of derivative, we *heuristically* approximate $(s-1)\frac{L'(s)}{L(s)}$ as follows. For $|s-1|$ small, we have

$$\begin{aligned}(s-1)\frac{L'(s)}{L(s)} &= \frac{s-1}{L(s)}\cdot\lim_{h\to 0}\frac{L(s+h)-L(s)}{h}\\ &\approx \frac{s-1}{L(s)}\cdot\frac{L(s+(s-1)^2)-L(s)}{(s-1)^2}\\ &= \frac{L(s^2-s+1)-L(s)}{(s-1)L(s)}\end{aligned}$$

Question 2.2. Does

$$\lim_{s\to 1}(s-1)\cdot\frac{L'(s)}{L(s)} = \lim_{s\to 1}\frac{L(s^2-s+1)-L(s)}{(s-1)L(s)}?$$

In any case, we can use this formula in PARI to "approximate" r.

```
? E = ellinit([ 0, 1, 1, -2, 0 ]);
? r(E,s) = L1=elllseries(E,s); L2=elllseries(E,s^2-s+1); (L2-L1)/((s-1)*L1);
? r(E,1.01)
%8 = 2.0041353424739419286176800 57
? r(E,1.001)
%9 = 2.0004313375472255448193191 04
\\ One can prove that 2 is the correct limit.
```

Now let's try the mysterious curve $y^2 + xy = x^3 - x^2 - 79x + 289$ of rank 4:

```
? E=ellinit([ 1,-1,0,-79,289]);
? r(E,1.001)          \\ takes 6 seconds on PIII 1Ghz
%1 = 4.00222237451908561089644064 2
? r(E,1.00001)
%2 = 4.000016181256911064613006133
```

It certainly looks like $\lim_{s\to 1} r(s) = 4$. We know for a fact that $\lim_{s\to 1} r(s) \in \mathbb{Z}$, and if only there were a good way to bound the error we could conclude that the limit is 4. But this has stumped people for years, and maybe it is impossible without a very deep result that somehow interprets this limit in a different way. This problem has totally stumped the experts for years. We desperately need a new idea!!

If one of you wants to do a reading or research project on this problem in the next year or two, let me know. One could draw pictures of $L^{(3)}(E, s)$ or investigate the analogous problem for other more accessible L-series.