## 13.3 Computing $L(E,s)$ with a Computer

There is a way to define $a_p$ for $p \mid \Delta$ which we will not describe here. The $L$-function of $E$ is

$$L(E,s) = L^*(E,s) \cdot \prod_{p|\Delta} L_p(E,s)$$

where the factors $L_p(E,s)$ are either $1/(1-a_p p^{-s}+p^{1-2s})$ or $1/(1-a_p p^{-s})$. This section is about how to compute $L(E,s)$, for positive $s \in \mathbb{R}$, using a computer.

Let

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

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

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

be the *incomplete* $\Gamma$-*function*. The following proposition is proved using that $E$ is modular.

**Proposition 13.3.1.** *There is an explicitly computable integer $N$ (called the conductor of $E$) and $\varepsilon \in \{1,-1\}$ such that*

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

*where*

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

You can compute $N$ using the MAGMA command `Conductor(E)`. It appears that MAGMA currently has no command to compute $\varepsilon$, which is a shame, but there is an efficient algorithm to compute it.

I have mentioned several times that the $a_n$ for composite $n$ are determined by the $a_p$, but not said exactly how. 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 $\gcd(n,m) = 1$

At $s = 1$, the formula of Proposition 13.3.1 simplifies to

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

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

## 13.4 A Rationality Theorem

It is difficult to say anything precise about $L(E,s)$, even with the above formulas. For example, it is a deep theorem of Dick Gross and Don Zagier that the elliptic curve $E$ defined by $y^2 = x^3 - 9072x + 291600$ has analytic rank 3, i.e., that

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

**Open Problem 13.4.1.** *Prove that there is an elliptic curve $E$ with analytic rank at least 4, that is, for which*

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

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

**Theorem 13.4.2.** *Let $y^2 = x^3 + ax + b$ be an elliptic curve, and let*

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

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

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

*with denominator that can be a priori bounded.*

A computer computes $\Omega_E$ using Gauss's arithmetic-geometric mean, not numerical integration (see the MAGMA command `RealPeriod`).

*Example* 13.4.3. 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. One can show that $\varepsilon = +1$ and $N = 26$.

```
> E := EllipticCurve([-43,166]);
> N := Conductor(E); N;
26
> f  := qEigenform(E,101);
> pi := Pi(ComplexField());
> L1 := (1+1) * &+[Coefficient(f,n)/n * Exp(-2*pi*n/Sqrt(N)) :
                   n in [1..100]];
> L1;
0.62096534954905546637586267 27
> R := RealPeriod(E);
4.346757446843388264631038708906494390976115 76340854513133
> L1/R;
0.14285714285714285714285714285
> 1/7.0;
0.14285714285714285714285714285
```

## 13.5 A Way to Approximate the Analytic Rank

Fix an elliptic curve $E$ over $\mathbb{Q}$. In this section we describe a method that uses Proposition 13.3.1, the definition of the derivative, and some calculus to approximate the analytic rank of $E$.

**Proposition 13.5.1.** *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 the limit as $s\to 1$ of a certain smooth function. This limit is extremely subtle; for example, if $E$ is the elliptic curve defined by

$$y^2 = x^3 - 102627x + 12560670$$

then nobody has yet succeeded in proving that this limit is 4 even though we can prove that $E$ has algebraic rank 4. Also, one can prove that the limit is either 2 or 4, so showing that the limit is not 2 is a major open problem.

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 13.5.2.** Does

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

MAGMA doesn't yet have good functionality for efficiently computing $L(E,s)$, so I'm going to use PARI to illustrate computation of $L(E,s)$ in order to compute the rank. Now let's try the curve $y^2 = x^3 - 102627x + 12560670$ of rank 4 (we use a different better model $y^2+xy = x^3 - x^2 - 79x + 289$ for the curve):

```
? E=ellinit([ 1,-1,0,-79,289]);
? r(E,1.001)          \\ takes 6 seconds on PIII 1Ghz
%1 = 4.00222237451908561089644O642
? r(E,1.00001)
%2 = 4.000016181256911064613006133
```

It looks like $\lim_{s\to 1} r(s) = 4$. We know 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. Computing this limit has stumped mathematicians for years. The first examples of analytic rank 3 were obtained by interpreting $L'(E,1)$ as the "size" of a certain point on $E$, but no similar interpretation of $L''(E,1)$ has ever been found.

### *13.5.1 Notes On The Final Exam*

You will receive the final by the evening of Friday, January 10 and it will be due at 5pm on Sunday, January 12. I'll send it to you via email and post it on the web page. The instructions on the final exam will look roughly as follows:

> This is the Fall 2002 Math 124 take-home final examination. You may not talk to anyone about the problems. You are allowed to look at books, course notes, use a computer, etc., but please acknowledge any source you use. The complete course notes are available at `...124/stein`.
>
> Each problem is worth 10 points. Choose and do **ONLY FIVE** of the following problems. Clearly indicate which problem you are attempting and which you are omiting. (If you are having trouble getting into the math department to hand in your exam, call my office 617-495-1790 or my mobile 617-308-0144.)

How you should study for the final depends a lot on you. Since you won't be allowed to ask people questions during the final, probably the best way to study for it is to read through the lecture notes and record the questions that occur to you. Then discuss those questions with your friends and/or email me.