Excess Rank on Elliptic Curves

Stephen M. Lu[*]

January 20, 2002

Mathematics Department
Princeton University
Princeton, NJ 08544

Abstract

This paper describes computational methods used to determine the analytic ranks of curves in one-parameter families of elliptic curves defined over $\mathbf{Q}$. To do so, we calculate the order of vanishing of the associated L-function at $s = 1$.

By the Birch–Swinnerton-Dyer Conjecture, we can force r points of infinite order on the curve $\mathrm{E}(\mathbf{Q})$ such that we should expect a high rank. Assuming the Parity Conjecture, we would expect to find half the curves of rank r and the other half of rank $r + 1$. However, we are interested to see if can find curves of rank higher than the forced rank r, e.g., $r + 2$ or $r + 3$, and previous investigations seem to indicate that this condition is likely. We are nonetheless concerned with whether this remains true in the limit or is merely a consequence of small numbers. We have looked at published results to verify our methods; however, we will apply our methods to families in which the $a_p(E)$'s vary. This paper describes our progress and results thus far.

[*]E-mail: `slu@princeton.edu`

1 Basic Definitions

1.1 Rank

There are two "types" of rank which are important to consider: analytic and geometric rank.

Definition 1.1.1 (Analytic Rank) *The order of vanishing, r, of the L-function at $s = 1$ is the rank of the elliptic curve.*

Definition 1.1.2 (Geometric Rank) *By the Mordell-Weil Theorem, the group E($\boldsymbol{Q}$) of $\boldsymbol{Q}$-points on an elliptic curve E defined over $\boldsymbol{Q}$ is a finitely generated abelian group: $E(\boldsymbol{Q}) \cong \boldsymbol{Z}^{\rho} \oplus E(\boldsymbol{Q})_{tors}$. Here, $\rho \geq 0$ is the rank of E($\boldsymbol{Q}$) and is the number of finite copies of $\boldsymbol{Z}$. $E(\boldsymbol{Q})_{tors}$ is a finite abelian group. In fact, there are only finitely many torsion groups that can occur (proven by Mazur).*

We can find a lower bound for the geometric rank by forcing points on curves (while verifying that they are linearly independent). This project included calculating the analytic rank by evaluating the L-function and its derivatives at $s = 1$.

1.2 Modular Forms

Definition 1.2.1 (Modular Form) *Let f(z) be a meromorphic function on the upper half-plane* $\mathbf{H}$, *and let* k *be an integer. If f(z) satisfies the relation:*

$$f(\gamma z) = (cz + d)^{2k} f(z) \tag{1.1}$$

for all $\gamma \in \Gamma_0(N)$, where

$$\Gamma_0(N) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \mid c \equiv 0 \,(mod\, N);\ det\, \gamma = 1;\ a, b, c, d \in \boldsymbol{Z} \right\},$$

f(z) is called a modular form of weight 2k and level N.

We are particularly interested in the case where k = 1. Because of the periodicity properties of modular forms (e.g., $f(z + 1) = f(z)$), we can express a weight-two modular form as a Fourier series: $\Sigma_{n=0}^{\infty} a_n e^{2\pi i n z}$. When $a_0 = 0$, i.e., there is no constant term in the series, this type of modular form is called a cusp form. When we substitute $z = x + iy$ (z $\in \mathbf{H}$), we find

$$\sum_{n=1}^{\infty} a_n e^{2\pi i n z} = \sum_{n=1}^{\infty} a_n e^{2\pi i n (x+iy)} \leq \sum_{n=1}^{\infty} |a_n| e^{-2\pi n y}. \tag{1.2}$$

These expressions are thus of exponential decay. It is a theorem (not proven here) that the a_n's have less than an exponential order of growth. Hence, these sums have good convergence properties (this is an important fact for coding later).

1.3 The L-function and the functional equation

To each cusp form, we associate an L-function $L(f,s)$, convergent in the right half plane for $\mathrm{Re}(s) > x_0$, ($x_0 \in \mathbf{R}$), and defined using the Mellin Transform:

$$L(f,s) = (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z}. \tag{1.3}$$

Substituting the cusp form Fourier expansion $\sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ and integrating term by term, we can represent $L(f,s)$ as a Dirichlet series:

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}. \tag{1.4}$$

We also know that

$$\begin{aligned} f(-1/(Nz)) &= -\epsilon N z^2 f(z) & (1.5)\\ \text{and } f(i/y\sqrt{N}) &= \epsilon y^2 f(iy/\sqrt{N}). & (1.6) \end{aligned}$$

Theorem 1.3.1 (Modularity Theorem) *Every elliptic curve over $\boldsymbol{Q}$ is modular.*

By the Modularity Theorem, we can associate to an elliptic curve E with conductor N, a weight two modular form of level N. Thus the properties of modular forms may be applied to elliptic curves.

Let us attach to E an L-function, $L(E,s)$, and examine its Euler product expansion:

$$L(E,s) = \prod_{p|N} (1 - a_p p^{-s})^{-1} \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1}. \tag{1.7}$$

Let us also define $\Lambda(f,s)$ by

$$\Lambda(f,s) = (2\pi)^{-s} N^{s/2} \Gamma(s) L(f,s) = \int_0^{\infty} f(iy/\sqrt{N}) y^{s-1} dy. \tag{1.8}$$

If we break the integral form of $\Lambda(f,s)$ into $\int_0^1 + \int_1^{\infty}$, and then utilize the transformation property in Equation (1.6), we can rewrite the sum as one integral from one to ∞. (These manipulations will be explicitly shown in Section (2.2).) From the single-integral expression, the functional equation directly follows:

$$\Lambda(f, s) = \epsilon \Lambda(f, 2 - s), \tag{1.9}$$

where $\epsilon = \pm 1$. We call ϵ the *sign of the functional equation*, and this determines whether the function is even ($\epsilon = 1$) or odd ($\epsilon = -1$). Given the functional equation, we have an analytic continuation of $\Lambda(f, s)$ to the entire complex plane, and therefore $L(E, s)$ is defined and can be analytically continued for all $s \in \mathbf{C}$. $L(E, s)$ thus satisfies a similar functional equation with a zero at $s = 1$ of order r, which is the analytic rank.

Proposition 1.3.2 (Birch–Swinnerton-Dyer Conjecture) *The (geometric) rank of an elliptic curve E defined over $\mathbf{Q}$ is equal to the order of the zero of $L(E, s)$ at $s = 1$.*

By the Birch–Swinnerton-Dyer Conjecture, we expect r to equal ρ, each defined as in Section (1.1).

2 Calculating the derivatives of the L-function

We desire to calculate the analytic rank of E($\mathbf{Q}$). Assuming the Birch–Swinnerton-Dyer Conjecture, we expect the geometric rank to be equal to the order of vanishing of the $L-$function at $s = 1$ (i.e., the analytic rank). Hence, we need to calculate the numerical value of the r^{th} derivative of $L^{(r)}(E, 1)$. To do so, we follow an algorithm of Cremona. First, the motivation behind the algorithm, that is, why it works, will be explained. Then the details of the algorithm itself will be elucidated.

2.1 Motivation

We can also expand $L(E, s)$ as a Taylor series: $L(E, s) = \sum_{n=0}^{\infty} b_n (s-1)^n$. Each b_n is defined in the usual way: $b_n = \frac{L^{(r)}(E,s)}{n!}$. Thus, for $s = 1$, we want to find the first non-zero term in the expansion, say the r^{th} term, since the value of r will determine the order of vanishing, and hence the rank, of the curve.

For example, if $L(E, 1) = 0$, this implies that $b_0 = 0$, and so the analytic rank is greater than or equal to one. If $L'(E, 1) = 0$ of the same curve, then $b_1 = 0$ and the rank must be greater than or equal to two. If, however, $L'(E, 1) \neq 0$, then $b_1 \neq 0$, and the rank is equal to 1. The functional equation is helpful here, since if we know that the curve is, for example, even and the value of the L-function at 1 is zero, then we know that the rank must be greater than or equal to *two* and even. Likewise, if the functional equation is odd, the algorithm can start by calculating the first derivative of the L-function, since the L-function will be 0 at $s = 1$. Again, if the value of the first derivative is nonzero, the curve is of rank 1; if it is zero, the rank is greater than or equal to three and odd, and the algorithm can "skip" to calculating the third derivative, and so on, until the value of the derivative is no longer zero. Thus, iterations of this process will provide the order of vanishing of the L-function at $s = 1$, and hence the analytic rank.

2.2 The Algorithm

Starting with Equation (1.8) and utilizing Equation (1.6), we see that

$$\begin{aligned} \Lambda(f,s) &= \int_0^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_0^1 f(iy/\sqrt{N})y^{s-1}dy + \int_1^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_1^\infty f(iy/\sqrt{N})(y^{s-1} + \epsilon y^{1-s})dy. \end{aligned} \tag{2.10}$$

If we differentiate this expression k times with respect to s, we get

$$\Lambda^{(k)}(f,s) = \int_1^\infty f(iy/\sqrt{N})(\log y)^k(y^{s-1} + \epsilon(-1)^k y^{1-s})dy. \tag{2.11}$$

At $s = 1$,

$$\Lambda^{(k)}(f,1) = (1 + \epsilon(-1)^k)\int_1^\infty f(iy/\sqrt{N})(log\, y)^k dy. \tag{2.12}$$

Observe that $\Lambda^{(k)}(f,1) = 0$ if $\epsilon = (-1)^{k+1}$. We can also see that $(-1)^r = \epsilon$, so r is even if and only if $\epsilon = 1$. Hence, for even functional equation ($\epsilon = 1$) and $r \geq 1$, we have

$$\begin{aligned} \Lambda^{(r)}(f,1) &= 2\int_1^\infty f(iy/\sqrt{N})(log\, y)^r dy \\ &= 2\sum_{n=1}^\infty a_n \int_1^\infty e^{(-2\pi ny/\sqrt{N})}(log\, y)^r dy. \end{aligned} \tag{2.13}$$

For $r = 0$,

$$\Lambda(f,1) = \frac{\sqrt{N}}{\pi}\sum_{n=1}^\infty \frac{a_n}{n} e^{(-2\pi ny/\sqrt{N})}. \tag{2.14}$$

Integrating Equation (2.13) by parts,

$$\Lambda^{(r)}(f,1)=\frac{\sqrt{N}}{\pi}\sum_{n=1}^{\infty}\frac{a_n}{n}\int_1^{\infty}e^{(-2\pi ny/\sqrt{N})}(log\,y)^{r-1}\frac{dy}{y}. \tag{2.15}$$

Then, since $\Lambda(f,s)$ vanishes to order r at $s=1$, $L^{(r)}(f,1)=(2\pi/\sqrt{N})\Lambda^{(r)}(f,1)$. Thus, applying to an elliptic curve,

$$L^{(r)}(E,1)=2r!\sum_{n=1}^{\infty}\frac{a_n}{n}G_r\left(\frac{2\pi n}{\sqrt{N}}\right), \tag{2.16}$$

where

$$G_r(x)=\frac{1}{(r-1)!}\int_1^{\infty}e^{-xy}(\log y)^{r-1}\frac{dy}{y}. \tag{2.17}$$

The functions $G_r(x)$ can be expanded by a power series for small x and are generated by

$$G_r(x)=P_r\left(\log\frac{1}{x}\right)+\sum_{n=1}^{\infty}\frac{(-1)^{n-r}}{n^r\cdot n!}x^n \tag{2.18}$$

where $P_r(t)$ is a polynomial of degree r, defined (here only up to $r=5$) by the relation $P_r(t)=Q_r(t-\gamma)$, where γ is Euler's constant and the $Q_r(t)$'s are defined as follows:

$$\begin{aligned}
Q_1(t) &= t;\\
Q_2(t) &= \frac{1}{2}t^2+\frac{\pi^2}{12};\\
Q_3(t) &= \frac{1}{6}t^3+\frac{\pi^2}{12}t-\frac{\zeta(3)}{3};\\
Q_4(t) &= \frac{1}{24}t^4+\frac{\pi^2}{24}t^2-\frac{\zeta(3)}{3}t+\frac{\pi^4}{160};\\
Q_5(t) &= \frac{1}{120}t^5+\frac{\pi^2}{72}t^3-\frac{\zeta(3)}{6}t^2+\frac{\pi^4}{160}t-\frac{\zeta(5)}{5}-\frac{\zeta(3)\pi^2}{36}.
\end{aligned}$$

These are all the elements needed for the algorithm.

3 Coding the Algorithm

We start by inputting the components (a_1,a_2,a_3,a_4,a_6) into the elliptic curve equation:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6. \tag{3.19}$$

Typically, at least one of the components has a dependence on t, which we use as our parameter and which can range over the integers. We then use PARI to convert the curve to the "minimal" Weierstrass model and calculate its conductor, N, the value of $L(E,1)$, and the sign of the functional equation. The sign of the functional equation and the value of $L(E,1)$, as noted above, help determine which derivative (if any) we need to calculate. We use the conductor N to estimate how many terms we should include in the sum for calculating $L^{(r)}(E,1)$ (see Equation (2.16)). Because of the good convergence properties cited in Equation (1.2), we choose to sum the a_n's up to an integer close to $(\sqrt{N}\log N)/2\pi$. Next, for each n up to this value, we use PARI again to calculate the value of a_n. We were surprised by the frequency of the value of $a_n = 0$ in early calculations. Then, if $a_n \neq 0$, we move on to calculating the appropriate derivative (assuming we need to).

To calculate the n^{th} derivative, we begin by evaluating the $G_n(x)$ function with $x = \frac{2\pi n}{\sqrt{N}}$. We choose to limit the number of terms ($\sim O(10^2)$) that we take in the sum for each $G_n(x)$, since G decays rapidly with n as $n!$ is in the denominator. We input x, take the value that $G_n(x)$ produces, and multiply it by the corresponding a_n. We then sum over all the n's up to the aforementioned limit, multiply by the appropriate scaling factors, and come up with a value of $L^{(n)}(E,1)$ for a given n. Should this value be less than a certain tolerance above zero (say, 0.001), we "categorize" it as zero and move on the $(n+2)^{th}$ derivative.

This process continues until the value of the (new) n^{th}-derivative is "sufficiently" nonzero, at which point the algorithm can stop and declare the rank of the curve to be $r = n$ at that value of n.

For the purpose of organizing and comparing data, the program also calculates the rank of each curve for a range of t's and tabulates the percentage of curves with each rank. Our program is able to calculate up to the fifth derivative of an L-function.

4 Data

Qualitatively, we tested our program on a variety of families of curves published by Fermigier and found that our percentages matched. Similarly, we tested our program on other curves from the literature and produced equally accurate results. One potential weakness is the slight but noticeable change in results depending on the tolerance we set for a value to be "categorized" as zero; this is particularly an issue when the rank increases above one. Nonetheless, we are confident that our program works and produces meaningful data.

5 The Future

As we choose curves of higher rank, larger conductors, or larger values of t, the calculations involve extremely large numbers. We have thus been working on ways to speed up the calculations by keeping computer memory open, using other properties of modular forms, and storing re-usable data (e.g., prime factorizations) in quickly accessible files. An improved algorithm exists utilizing Modular Form Theory and Hecke Operators. It requires calculation of a_n only for n prime, which then in turn easily allow calculation for all other n. While faster and more efficient, this algorithm requires additional background, so this paper has addressed the former method. More concrete data on more curves with higher numbers from the literature and other "interesting" curves, including those with varying $a_p(E)$'s, should be forthcoming.

The author would like to thank Andrew Wiles, Steven J. Miller, Sal Butt, Leo Goldmakher, and Jonathan Hsu for their help, mentorship, and contributions to this effort.

6 Bibliography

Brumer, Armand and Oisin McGuinness. "The Behavior of the Mordell-Weil Group of Elliptic Curves." *Bulletin of the American Mathematical Society*, Vol. 23, No. 2 (1990). pp375-382.
Cremona, John. *Algorithms for Modular Elliptic Curves.* Cambridge: Cambridge UP, 1992.
Fermigier, Stéfan. "Étude expérimentale du rang de familles de courbes elliptiques sur Q." *Experimental Math*, Vol. 5, No.2 (1996). pp.119-129.
Ireland, Kenneth, and Michael Rosen. *A Classical Introduction to Modern Number Theory.* New York: Springer, 1990.
Knapp, Anthony. *Elliptic Curves.* Princeton: Princeton UP, 1992.
Koblitz, Neal. *Introduction to Elliptic Cuves and Modular Forms.* New York: Springer, 1993.
Ribet, Kenneth. "Galois Representations and Modular Forms." *Bulletin of the American Mathematical Society*, Vol. 32, No. 4 (1995). pp. 375-402.
Serre, J.-P. *A Course in Arithmetic.* New York: Springer, 1973.