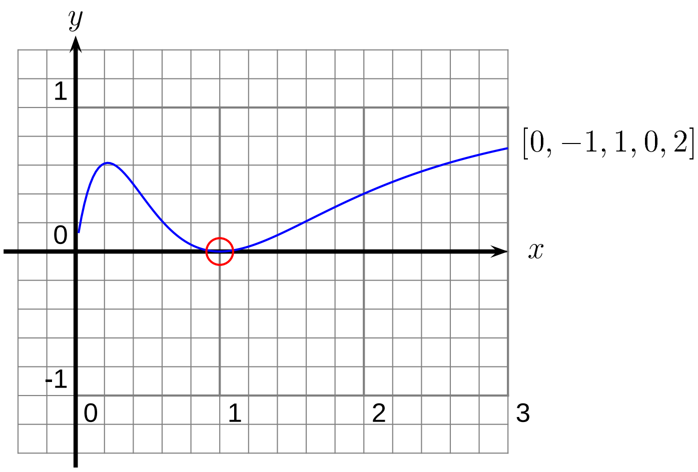
Visualizing $L(E, s)$

Ariel Shwayder

May 14, 2002



Contents

1 Why bother to do this?

Elliptic curves, and the machinery involved in them have been a hot topic in modern mathematics for quite some time. They came to the fore in the public consciousness most prevalently because of their deep involvement in Andrew Wiles's 1994 proof of Fermat's Last Theorem. This is in fact when I first became aware of them. Elliptic curves have become popular perhaps not only because of their deep and interesting properties, but also because of their fairly simple definition. The notion of an L-series attached to an elliptic curve is also a fairly simple notion (as will be explained below), but the study of the correlation between these two objects has led to many of the biggest unsolved problems in mathematics today.

The Birch and Swinnerton-Dyer (BSD) conjecture is the statement that the rank (a simple algebraic invariant) of an elliptic curve is equal to the order of vanishing at zero (a simple analytic property) of the L-series attached to that curve. The conjecture was first formulated in the early 1960s, and today we still don't have a good way of approaching the problem. With Fermat's Last Theorem, even before it was proved, the conjecture was known to hold for many specific cases. With BSD we don't even know how to show it is true for some very seemingly simple cases (for example, curves of rank 4).

Until 1986 it was not even known if the BSD conjecture held for a curve as simple as $y^2 + y = x^3 - 7x + 6$. In fact, the proof that it did hold was so deep that it provided an effective solution to the Gauss class number problem. A seemingly simple problem such as showing that there existed an elliptic curve whose L-series had order 3 was a very deep theorem of Gross and Zagier, and as of this writing, it is an open problem to prove that there is an elliptic curve whose L-series has order 4 or higher.

It is with these questions in mind that we approach the idea of graphing the L-series attached to elliptic curves. While we doubt that anything can be proven through pictures, having pictures as a reference is a very helpful tool when dealing with these series, and perhaps these pictures will give us more insight into what is happening with $L(E, s)$.

2 A quick introduction to Elliptic Curves and the series associated with them

2.1 All about E

The definition of an elliptic curve is the following: An elliptic curve E is a cubic curve of the form

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

where the a_i's are constants from a field K. We define the discriminant of the curve as

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

with

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

We require that $\Delta \neq 0$. For ease of notation we write $[a_1, a_3, a_2, a_4, a_6]$ when referring to the curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Perhaps one of the most interesting properties of an elliptic curve is that the points on an elliptic curve form a group. The key step in seeing this is to note that given any two points on an elliptic curve we can, in a natural way, define what it means to "add" those two points together. On an intuitive level, when you add two points together you draw a line connecting them, and see where that line intersects the elliptic curve. If there is no third point of intersection then we say that those two points add to "the point at infinity," which is the identity element in the group. Otherwise, if they intersect at a third point, (x, y), then we define that the "addition" of those two points to be $(x, -y)$. (The reason that you need to switch the y-coordinate is so that all of the group axioms come out correctly.)

Once you determine that the points do indeed form a group, then the natural question to ask is, what is this group? If we are considering our curve over $\mathbb{R}$ then the story becomes less interesting. In this case the group is infinite, as given any $x \in \mathbb{R}$ one can find $y \in \mathbb{R}$ such that (x, y) lies on the curve. It being infinite is not what makes it uninteresting, but it is the fact that the group is infinitely generated that makes it so. Because it is infinitely generated there is not much we can say about the group. In fact for any elliptic curve, the group $E(\mathbb{R})$ is always either S^1 or $S^1 \times \mathbb{Z}/2\mathbb{Z}$. Where S^1 is the group formed by the points in the complex plane on the circle of radius 1 under multiplication.

Since the problem of $E(\mathbb{R})$ has been solved, we turn our attention to what happens when we consider our curve over $\mathbb{Q}$. In this case Mordell's theorem tells us that the group $E(\mathbb{Q})$ is finitely generated and hence that

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$$

where r is a non-negative integer, and $E(\mathbb{Q})_{\text{tors}}$ is the finite subgroup of points of finite order in $E(\mathbb{Q})$. Professor Barry Mazur, in a 1976 theorem, showed that $E(\mathbb{Q})_{\text{tors}}$ must be isomorphic to one of the following groups:

$$\begin{aligned} \mathbb{Z}/n\,\mathbb{Z}, &\qquad \text{for } n \leq 10 \text{ or } n = 12. \\ (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/2n\,\mathbb{Z}), &\qquad \text{for } n \leq 4. \end{aligned}$$

The integer r is called the rank of the elliptic curve. It is a folklore conjecture that r can be arbitrarily large, however, the current record is a curve of rank at least 24. This was discovered by Roland Martin and William McMillen of the National Security Agency in January 2000.
(See `http://listserv.nodak.edu/scripts/wa.exe?A2=ind0005&L=nmbrthry&P=R182`)

2.2 The mysterious L

To every elliptic curve one can attach a certain series that we call $L(E,s)$. To define $L(E,s)$ recall that we have previously discussed points on an elliptic curve over such fields as $\mathbb{Q}$ or $\mathbb{R}$. However, the notion of points on an elliptic curve is not limited to these fields. One can consider the number of points on an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ for any prime p (that does not divide the discriminant of the curve). We denote the number of points on E over $\mathbb{Z}/p\mathbb{Z}$ as $\#E(\mathbb{Z}/p\mathbb{Z})$. We can now define a sequence of numbers a_p such that $a_p = p + 1 - \#E(\mathbb{Z}/p\mathbb{Z})$. There is also a slightly more complicated way to define a_n for any number. These a_n can be found in PARI by using the `ellan` command.

Once we have these a_n we can now define $L(E,s)$:

$$L(E,s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

It is a theorem of Breuil, Conrad, Diamond, Taylor, and Wiles that $L(E,s)$ can be extended to an analytic function on all of $\mathbb{C}$. As with any other analytic function we can ask what the order of vanishing of $L(E,s)$ is at any point. It turns out that the order of vanishing of $L(E, s)$ at $s = 1$ is a rather interesting story. In fact the Birch and Swinnerton-Dyer conjecture is that the order of vanishing at $s = 1$ is exactly equal to the rank of the elliptic curve.

In other words, for any elliptic curve, E,

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

at $s = 1$. Where here $k \neq 0$ and r is such that $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$.

The BSD conjecture is fairly amazing in that it asserts the equality of two seemingly very different quantities.

So far, the BSD conjecture has been proved when $\text{ord}_{s=1} L(E, s) \leq 1$ by Gross, Kolyvagin, Zagier, et al. However, for ord > 1 it is still an open problem, and as was mentioned above, it has yet to be proven that any elliptic curve has rank 4.

2.3 How I learned to stop worrying and love the Λ

Using our L-series, and in fact using any L-series one can define the notion of a Λ function that is very similar to $L(E, s)$, except that it has more symmetries. It is defined as follows:

$$\Lambda(Es) = N^{\frac{s}{2}}(2\pi)^{-s}\Gamma(s)L(E, s).$$

Where N is the conductor of the curve and $\Gamma(s)$ is the complete Γ function evaluated at s.

However, when only considering those L-series that come from elliptic curves the associated Λ-series obeys the following symmetry:

$$\Lambda(E, s) = \varepsilon\Lambda(E, 2-s)$$

where $\varepsilon \in \{\pm 1\}$ is the root number of E (which can be found using `ellrootno` in PARI). Because of this symmetry, the graphs of $\Lambda(E, s)$ can look "nicer" then those of $L(E, s)$ and in the graphs below we produce graphs of both $L(E, s)$ and $\Lambda(E, s)$ for this reason.

3 The formulas and methods used for these graphs

The question that then needs to be asked is "What does $L(E, s)$ look like?" This is the question that we set about to answer. In order to do so we use the free program PARI (available online at `http://www.parigp-home.de/`) to generate a list of points which can then be graphed. Fortunately, PARI has a nice built-in feature for computing $L(E, s)$ which makes the process much easier.

The function used to output the L-series data was:

```
{printellseries(fname, curve) =
E = ellinit(curve);
for(x=1,150,
        s=0.0+x/50;
        write(fname,"(",s,",",
        nice(elllseries(E,s,1)),")"));
}
```

Where the function `nice` is:

```
nice(x)=if(abs(x)<(10^(-25)), return(0), return(x))
```

This `nice` function is necessary because otherwise if the value at a certain point is too small, PARI will output in scientific notation, which makes the data unreadable by the program used to graph it. This way, values that are below a certain tolerance are simply converted to 0.

The `printellseries` function takes as input a filename and a vector defining a curve. It then outputs a list of points for the L-series of that curve, computed at intervals of .02 to the file `fname`.

Using this function, along with a little ingenious shell scripting and the help of the pstricks package of LaTeX, we were able to generate the graphs seen in section 4 along with many others.

This method worked well for graphing $L(E, s)$ for real values of s. However, $L(E, s)$ is in reality a complex analytic function, so it is defined for any complex value s as well. To solve this problem we could not use the built-in `elllseries` function since it was not able to compute $L(E, s)$ for complex-valued s.

In order to compute $L(E, s)$, we look to the following formula:

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

Here N is the conductor of the curve, Γ is the standard Γ-function, ε is as above, and

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

In the formula for $F_n(t)$, $\Gamma(x,y)$ is the standard incomplete Γ function. This formula comes from the solution exercise 24 on page 521 in chapter 10.4 of Henri Cohen's book *Advanced Topics in Computational Number Theory* (Springer-Verlag, March 2000).

The main problem in using PARI for these computations was that the implementation of the Γ-function in PARI does not include complex-valued arguments. For a while we played with trying to use other formulas to represent Γ so that PARI could be used. In the end, however, we discovered that the Γ-function implementation in Mathematica includes the ability to compute for complex-valued arguments, and so we decided to use Mathematica for that part of the computation and simply used the formulas as listed above. In addition, Mathematica has the ability to output three-dimensional graphs.

4 Graphing $L, \Lambda : \mathbb{R} \to \mathbb{R}$

Figure 1 is a graph of the L-series for the curve $y^2 - y = x^3 + x^2 - 10x - 20$. This curve has conductor 11 which is the curve of smallest conductor. The circle on the graph is drawn around the point (1,0), which is the critical point with respect to the BSD conjecture. It is critical in the sense that at this point the L-series should have the same order of vanishing as the rank of the elliptic curve. On this graph note that the graph does not appear to pass through that point. This would indicate that the rank of the L-series at 1 is zero. However, we also know that the rank of this curve is zero. Hence this graph agrees with the BSD conjecture.

Using our data we can compare the L-series for various curves of rank 1. This is shown in Figure 2. The curves show in this graph are $[0, 0, 1, -1, 0]$ with conductor 37, $[0, 1, 1, 0, 0]$ with conductor 43, $[1, -1, 1, 0, 0]$ with conductor 53, and $[0, -1, 1, -2, 2]$ with conductor 57.

We can also compare the L-series of various curves all of rank 2 (Figure 3). The conductors of these curves are 389, 433, 1001, and 3185 respectively. Note how the difference in conductors relates to the peak of the L-series

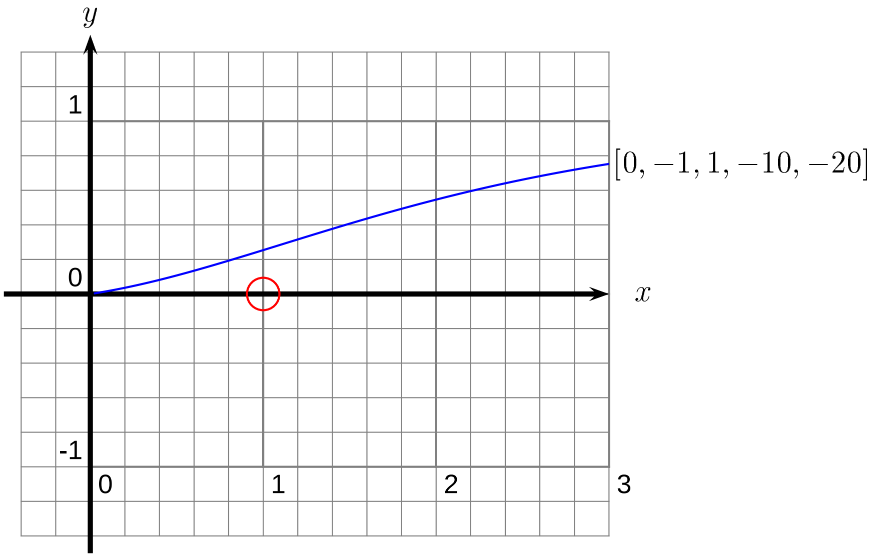


Figure 1: A graph of the L-series for $[0, -1, 1, -10, -20]$

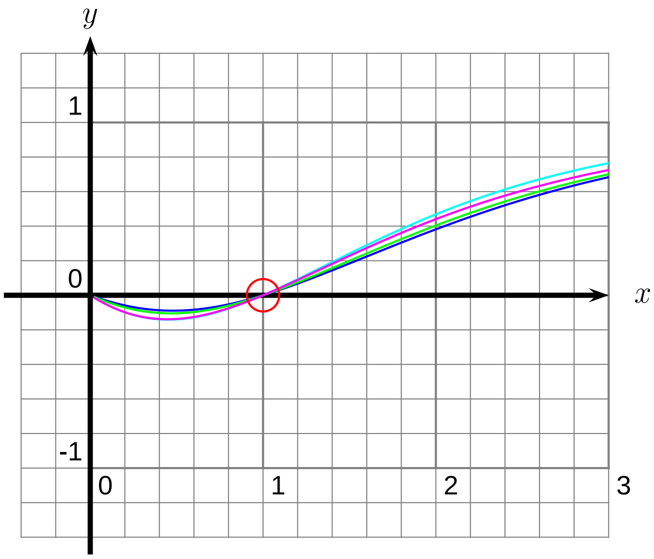
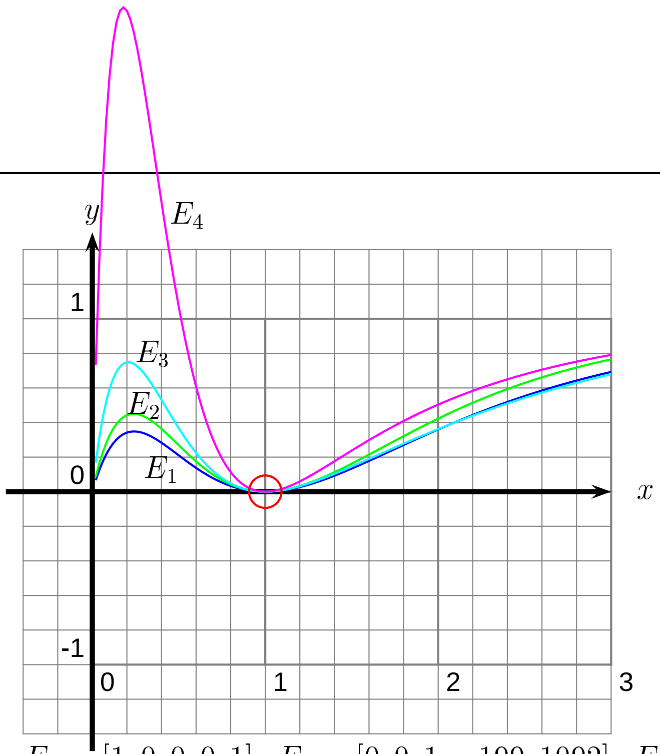


Figure 2: Curves of rank 1



$E_1 = [0, 1, 1, -2, 0]$, $E_2 = [1, 0, 0, 0, 1]$, $E_3 = [0, 0, 1, -199, 1092]$, $E_4 = [1, 0, 0, -1, 6]$

Figure 3: Curves of rank 2

between $x = 0$ and $x = 1$.

We make the similar comparison for some curves of rank 3 in Figure 4. The three curves shown in this Figure are $E_1 = [0, 0, 1, -7, 6]$ which has conductor 5077, $E_2 = [1, -1, 1, -6, 0]$ which has conductor 11197, and $E_3 = [1, -1, 0, -16, 28]$ which has conductor 11642.

Note that as in the case of the curves of rank 2, the graphs are arranged according to conductor. In this case, a curve of higher conductor is always less than a curve of lower conductor. One might be led to turn this observation into a conjecture, and in fact we were at first going to do so. However, closer examination of the evidence shows that while it may sometimes be true, it is not always the case that if the conductor of E_1 is larger than that of E_2 then $|L(E_1, x)| > |L(E_2, x)|$, as might be at first believed. One counter example of this can be seen with two curves of rank 2: Take E_1 to be $[1, 1, 1, -15, 16]$ and E_2 to be $[0, 1, 1, -4, 2]$. Then both have rank 2 and the conductor of E_1 is 563 and the conductor of E_2 is 571. However $L(E_1, 0.5) = 0.34614\ldots$ while $L(E_2, 0.5) = 0.27975\ldots$. Hence the possible conjecture is untrue.

One can also see that the possible conjecture would not hold for curves of rank 4. This can be seen in Figure 5 which is a graph of the curves $[0, 1, 1, -72, 210]$, $[0, 0, 1, -7, 36]$, $[1, 0, 0, -202, 1089]$, and $[0, 1, 1, -2, 42]$. All of the lines in the graph are so close it is hard to make out exactly what is go-

$E_1 = [0, 0, 1, -7, 6]$, $E_2 = [1, -1, 1, -6, 0]$, $E_3 = [1, -1, 0, -16, 28]$

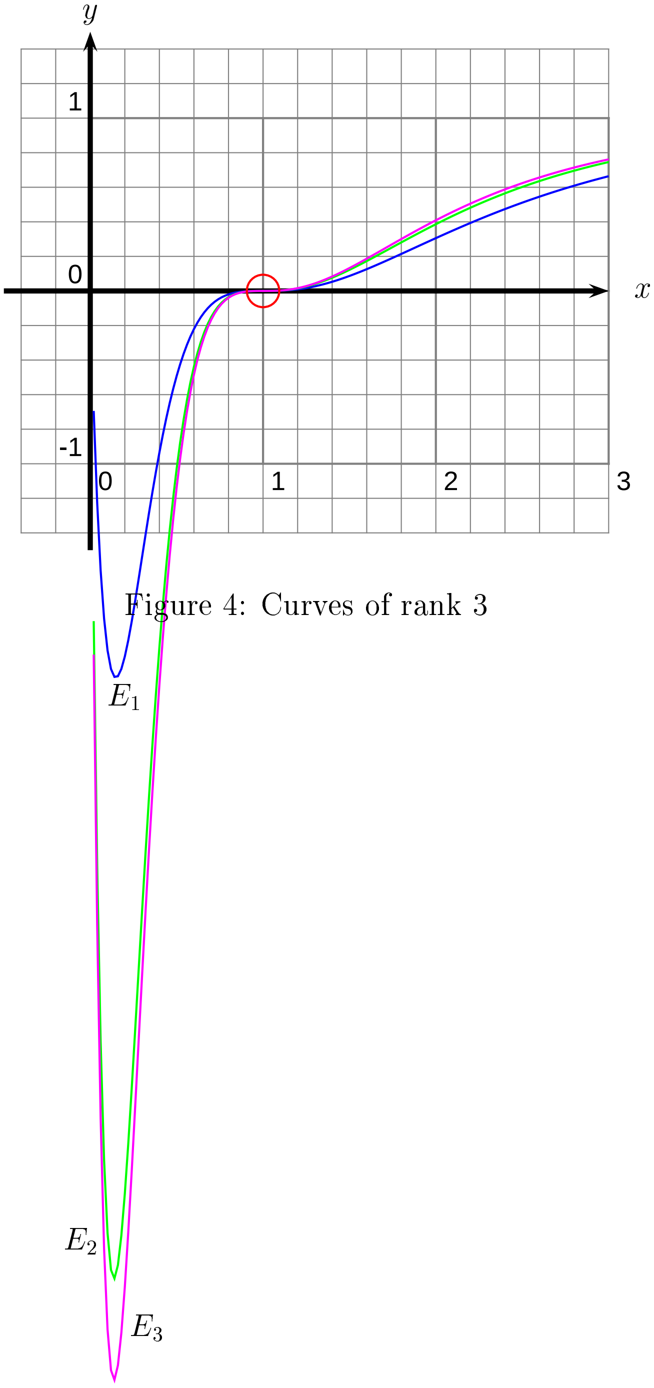


Figure 4: Curves of rank 3

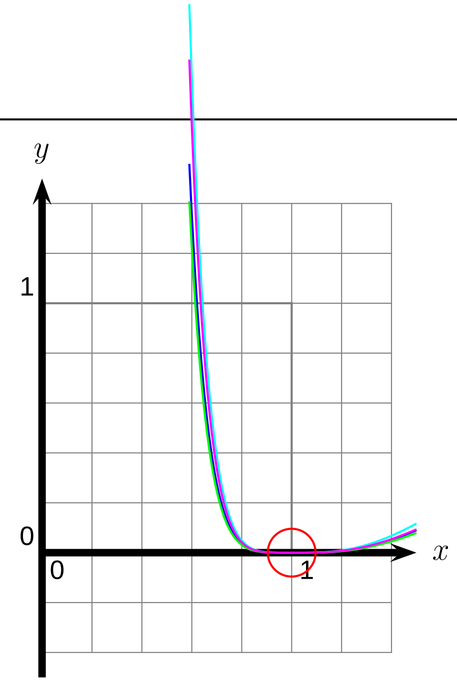


Figure 5: Curves of rank 4

ing on in the graph. However, looking directly at the data we can see that the conjecture does not hold. The curve $[0, 1, 1, -72, 210]$ has conductor 501029. At the point $x = .59$ the L-series has the value 1.558791254529780353650676198. The curve $[0, 0, 1, -7, 36]$ has conductor 545723 which is larger than the first curve. However at $x = .59$ the L-series for this curve has the value 1.408951738645349791068825739. Hence the conjecture does not hold for $N = 4$.

With the help of some powerful computing power, we can even calculate data for curves of rank 5 or higher. An example of a graph of the L-series for a curve of rank 5 is shown in Figure 6. The curve used for this graph is $[0, 1, 1, -30, 390]$ which has rank 5 and conductor 67445803. It was interesting to note that the L-series of all of the curves of rank 5 that we graphed looked amazingly similar to the naked eye.

To see what $\Lambda(E, s)$ looks like in comparison to $L(E, s)$ we graph both the Λ-series and L-series for four curves of different ranks in Figure 7.

In Figure 7, rank(E_n)=n. By looking at the graph of the L-series we can see that the BSD conjecture is plausible: E_0 does not pass through (0,1), E_1 seems to pass through with order 1, E_2 flattens out so that it could be seen as having order 2, and E_3 curve is even flatter, suggesting that it has order 3.

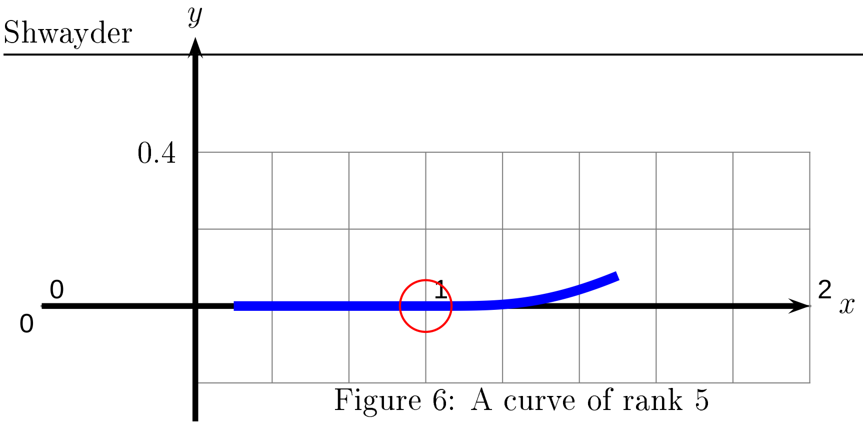


Figure 6: A curve of rank 5

5 Graphing $\Lambda : \mathbb{C} \to \mathbb{C}$

In the above section we graphed $L(E,s)$ as a function of $\mathbb{R}$. In reality however, both $L(E,s)$ and $\Lambda(E,s)$ are defined on $\mathbb{C}$ as well. Using a mixture of PARI and Mathematica we were able to produce graphs of $Arg(\Lambda)$ and $Abs(\Lambda)$ for various elliptic curves.

Figure 8 is a graph of the argument of $\Lambda(E,s)$ for the elliptic curve $[0,-1,1,-10,-20]$.

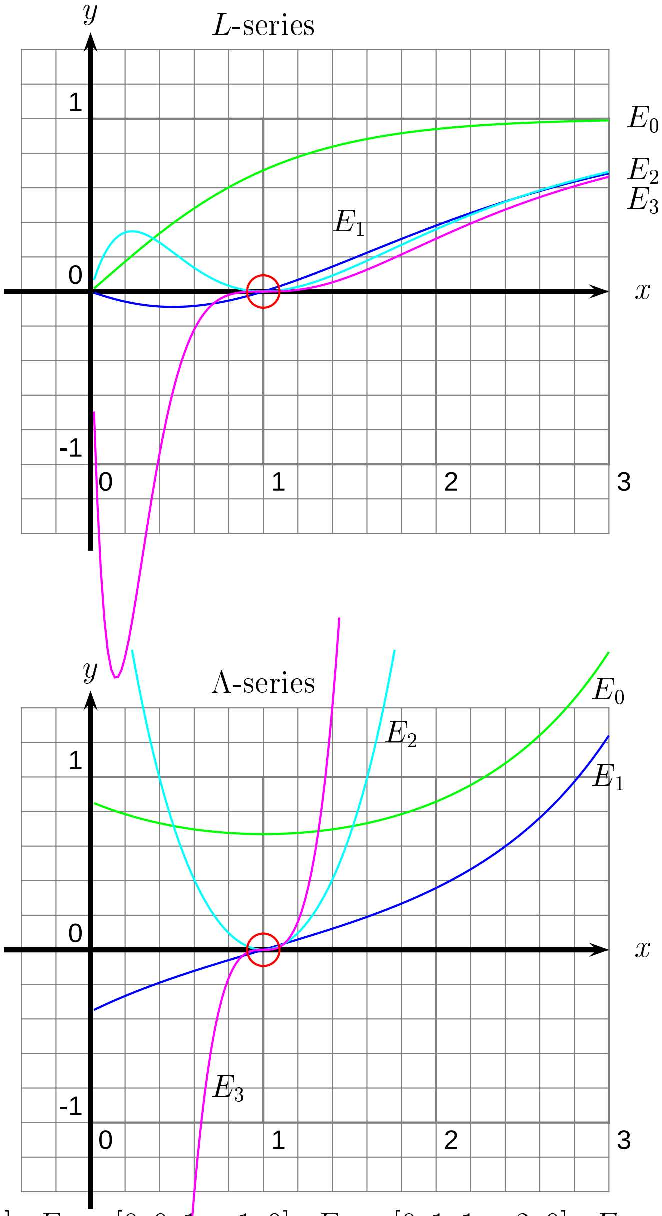
We can also see the absolute value of $\Lambda(E,s)$ for $[0,-1,1,-10,-20]$ in Figure 9.

A The Scripts

This paper and the scripts used to generate both 2D and 3D data are available for general use online at `http://modular.fas.harvard.edu/shwayder/`.

B Acknowledgments

A big, hearty thank you to Dr. William A. Stein (`http://modular.fas.harvard.edu`). Without his inspiration, motivation, and computing power this project would have never happened.



$E_0 = [0, 0, 0, 0, 1]$, $E_1 = [0, 0, 1, -1, 0]$, $E_2 = [0, 1, 1, -2, 0]$, $E_3 = [0, 0, 1, -7, 6]$

Figure 7: Graph of the L-series and Λ-series for various curves

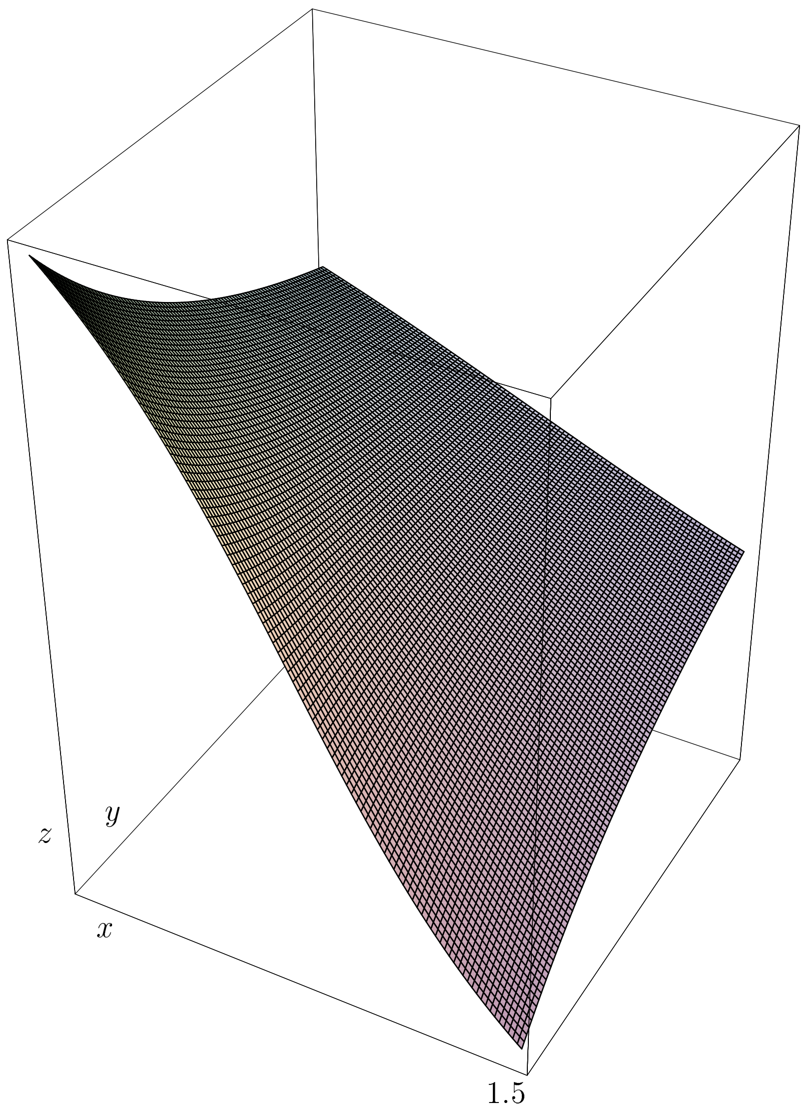


Figure 8: The argument of Λ for $[0, -1, 1, -10, -20]$

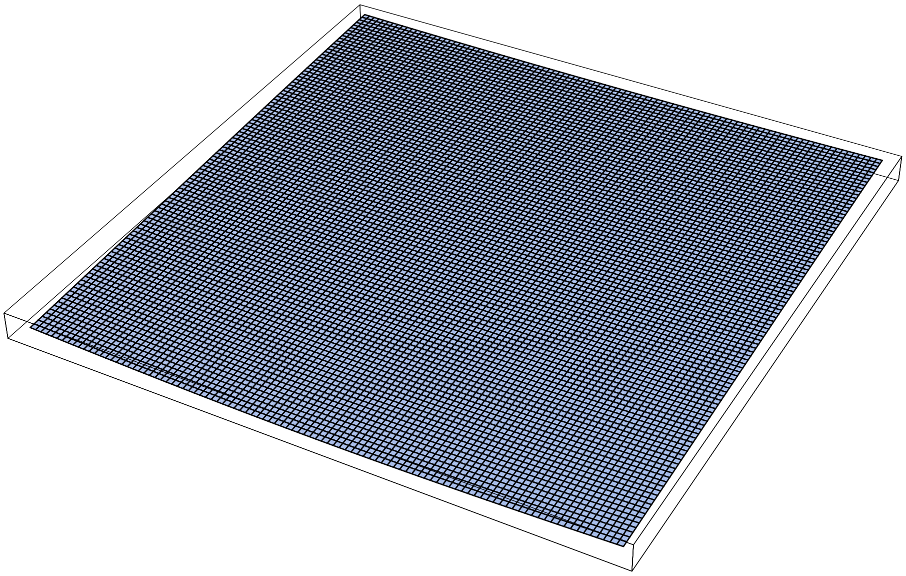


Figure 9: The absolute value of Λ for $[0, -1, 1, -10, -20]$