The Relationship between Conductor and Discriminant of an Elliptic Curve over $\mathbb{Q}$

Nico Adamo

A paper presented to SciJAS 2018

Heathwood Hall
Columbia, SC
Febuary 9th, 2018

The Relationship between Conductor and Discriminant of an Elliptic Curve over $\mathbb{Q}$

Nico Adamo

Abstract

Saito (1988) establishes a relationship between two invariants associated with a smooth projective curve, the conductor and discriminant. Saito defined the conductor of an arbitrary scheme of finite type using p-adic etale cohomology. He also defined the discriminant as measuring defects in a canonical isomorphism between powers of relative dualizing sheaf of smooth projective curves. The researcher in this paper shows that this relationship is analogous to that of conductor to discriminant in the case of elliptic curves, and uses it as well as analysis of data on conductors and discriminants to find out whether patterns exist between discriminant and conductor of elliptic curves. The researcher finds such patterns do in fact exist, and discusses two main ones - that of the conductor dividing the discriminant and that of the conductor "branching" in a predictable way. This allows for easier algorithms for computing conductors.

Contents

1 Introduction and Definitions

Definition 1.1. An elliptic curve over a number field K is defined as a cubic, projective curve of the form:

$$f(x,y)\ :\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

When the characteristic of K is different from 2 or 3, this curve can be written in the form:

$$y^2 = x^3 + Ax + B$$

The main purpose of the study of elliptic curves is looking at rational solutions to $f(x,y) = 0$. There is no general, efficient algorithm for finding these points of an elliptic curve, which is deeply related to the Discrete Logarithm Problem. For this reason, elliptic curves are used all over mathematics, physics, and computer science.

Definition 1.2. We define the *discriminant* of an elliptic curve $y^2 = x^3+Ax+B$ to be the constant:

$$\Delta = -16(4A^3 + 27B^2)$$

When considered on the projective plane, the discriminant has a geometric interpretation. If Δ is nonzero, the elliptic curve has three roots of multiplicity one. Otherwise, the elliptic curve has a singularity, which is either additive (if it is a cusp) or multiplicative (if it is a node).

Definition 1.3. The *conductor* of an elliptic curve is a measure of the ramification of the field extensions of the curve generated by the torsion points (the points of finite order under our group law for elliptic curves, which we omit for brevity's sake).

It can be written as a product of primes with exponent $\epsilon + \delta$, where ϵ is the tame reduction and δ the wild reduction of the curve at that prime. The tame reduction is simple - $\epsilon = 0$ for good reduction, $\epsilon = 1$ for multiplicative reduction and $\epsilon = 2$ for additive reduction.

The wild reduction vanishes if and only if the p-Sylow acts trivially on the Tate module and is given by:

$$\delta = \dim_{Z/pZ} Hom_{Z_p[G]}(P, M).$$

Where M is the group of points on the elliptic curve of order p for a prime p, P is the Swan representation, and G the Galois group of a finite extension of K such that the points of M are defined over it (Weil 1967)

By the Néron–Ogg–Shafarevich criterion, the primes that divide the conductor of an elliptic curve are the primes of bad reduction for that curve (bad reduction for a prime p meaning a singularity when considering the curve over $\mathbb{F}_p$).

This means we can give a relatively simple formula for the conductor of an elliptic curve E:

$$f(E) = \prod_{\mathbf{p}} \mathbf{p}^{f_{\mathbf{p}}}$$

Where the product is taken over the $\mathbf{p}$ for which the curve has bad reduction, and the exponent $f_{\mathbf{p}}$ is a measure of how "bad" the reduction is, equal to the sum $\epsilon + \delta$ we saw above.

The conductor of an elliptic curve comes up in many different scenarios, perhaps most notably as the least level of the modular form with a nontrivial map to the elliptic curve. It also appears in the L-function of an elliptic curve.

2 Purpose

As the conductor appears in the L-function of the elliptic curve as well as the functional equation for it's associated modular form, we can already see it has connections to many of the big conjectures (and ex-conjectures) in algebraic geometry (BSD, Tanyiama-Shimura, Szpiro, etc).

The conductor and discriminant are undoubtedly the most referenced invariants when talking about elliptic curves, so it is natural to ask if there is a relationship between the two. The subject of this paper will be to study the relationship between elliptic discriminant and conductor through various experimental methods.

My hypothesis in this experiment is that the conductor will vary linearly with the discriminant, and the null hypothesis in this experiment is that there is no quantifiable relationship between the two numbers.

3 Materials and Methods

The materials I will be using in this experiment are:

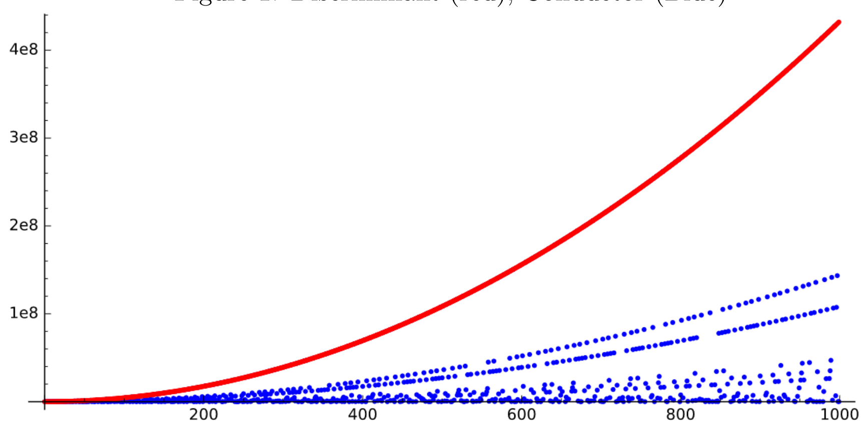
- SageMath (for generating conductors and discriminants)
- Mathematica (for analysis)
- A Dell Inspirion 3000 Laptop (to host the above two)
- ShareLatex (to write the paper)

The procedure for this experiment will be to generate sets of data on the discriminant and conductor of different sets of elliptic curves, and use Mathematica as well as general mathematical analysis to find patterns and make conjectures.

The SageMath code used to generate the discriminants and conductor is:

```
conductors=[EllipticCurve([0, 0, 0, F, j+1]).conductor() for j in
     range(1000)]
discriminants=[abs(EllipticCurve([0, 0, 0, F, (j+1)]).
    discriminant()) for j in range(1000)]
```

Figure 1: Discriminant (red), Conductor (Blue)



4 Results

Fig. 1 above is a plot of the conductor and absolute value of the discriminant for the Mordell curve $y^2 = x^3 + b$ with b varying on the x-axis. The patterns here exemplify what happens for all elliptic curves, so it will be used to show some of the patterns observed.

The conductor, while following an exponential patterns, switches intermittently between different "branches". The researcher observes as a main result that every branch of the conductor **is a factor of the discriminant**, and in fact there is a blue branch exactly following the discriminant not visible in the figure.

Upon further investigation, this fact follows from Saito (1988) who gives the following result:

Let R by a discrete valuation ring with perfect residue field, let C be a projective smooth and geometrically connected curve of positive genus over the field of fractions of R and let X be the minimal regular projective model of C over R. One defines the Artin conductor $Art(X/R)$ which turns out to be $f + n - 1$, where f is the conductor associated to the Jacobian of C and n is the number of irreducible components of the fiber at p of the minimal regular projective model of E over $\mathbb{Z}$. Saito proved that

$$Art(X/R) = \nu(\Delta)$$

where $\Delta \in R$ is the "discriminant" of X which measures the defect of a functorial isomorphism which involves powers of the relative dualizing sheaf of X/R. When C is an elliptic curve, Saito also proves that Δ is the discriminant (in the way we defined in the introduction) of the minimal Weierstrass equation of C. This means, for a prime p:

$$\nu_p(\Delta) = f_p + 1 - n$$

Table 1: For a curve $y^2 = x^3 + Ax + b$

Branch of Order:	Requirement for A:
1	All A
2	$A \not\equiv 0 \text{ mod } 4$
3	$A \equiv 0 \text{ mod } 3$
4	$A \equiv 0, 3 \text{ mod } 4$
5	$A \equiv 0, 2, 3 \text{ mod } 5$
6	$A \equiv 0 \text{ mod } 3$
7	$A \equiv 0, 1, 2, 4 \text{ mod } 7$
8	$A \equiv 0 \text{ mod } 3$

Where f_p is the exponent of the conductor at p and once again n is the number of irreducible components of the fiber at p of the minimal regular projective model of E over $\mathbb{Z}$

And, in particular:

$$f_p = \nu_p(\Delta) - n + 1 \tag{1}$$

Meaning the primes that divide the conductor are exactly those dividing the discriminant, and the exponent of each prime dividing the conductor is less than or equal to the exponent of that prime in the discriminant.

Formula (1) is referred to as Ogg's Formula, referencing Ogg (1967), where it was conjectured and discussed in Weil (1967).

Before the second pattern found is explored, we must first define some terminology. Given integral A, take $y^2 = x^3 + Ax + b$ and consider the conductor and discriminant of the curve as a function of b (an example of this is Fig. 1 for $A = 0$). We say the curve has a conductor "branch" of order n if there are an infinite number of conductors of $y^2 = x^3 + Ax + b$ that go into the discriminant of $y^2 = x^3 + Ax + b$ exactly n times. Or, put informally, if on the conductor vs discriminant graph (see Fig. 1) there is a "branch" of the conductors that follows the discriminant but divided by n. This curve is uniquely determined by A, as we take b to vary. For example, one only needs to take $A = 3$ to get $y^2 = x^3 + 3x + b$, and look at the plot of the conductor and discriminant as b varies to realize it has a branch of order 2 and a branch of order 3 among others.

The researcher has used sageMath to experimentally verify the pattern laid out in Table 1. Past order 8 you lose statistical integrity because of how close together all the branches are. But with order 1-8, all patterns are verified with 100 percent accuracy looking at values of the branches from 1 to 10000 and A from 0 to 1000.

Mathematically, the researcher has failed to meaningfully prove these patterns. However, investigation reveals some of their nature.

Formally put, a family of elliptic curves having a branch of order n means that the p-adic valuation of the conductor is one less than the p-adic valuation of the discriminant for all prime factors p of n, on all points on the branch.

Using our prime-by-prime product definition of the conductor, this concerns the exponent of the conductor f_p. And applying (1), we know that:

$$f_p = \nu_p(\Delta) - n + 1$$

Where n is the number of irreducible components of the fiber at p of the minimal regular projective model of E over $\mathbb{Z}$ But we are looking for f_p to equal $\nu_p(\Delta) - 1$, so for a point on a branch of order p, n must equal 2 for all primes that divide the order and only those primes.

Investigating patterns in the number of components of fibers is outside the scope of this paper so the researcher leaves it to someone more qualified in topology. Though it is interesting that although branches of prime order take less constraints on n, the A's that satisfy them seem to follow more complicated patterns (as evidenced by Table 1 above).

Acknowledgements

I would like to thank Dr. Matthew Boylan of the USC math department for entertaining my questions about elliptic curves and this pattern when I was just starting to learn, and for turning a dream into a passion.

I would also like to thank my loving girlfriend Mary for supporting me while I was writing, and even accidentally sparking the key insight with a laser pointer. Love forever !

I would also like to thank Mr. Morris and Ms. Norman for running our Science Research class, creating the requirements and deadlines, and keeping us running. I never will understand how you two juggled 17 experiments being done by inexperienced freshmen.

Finally, I'd like to thank my 6th grade teacher Mr. Culberton for many years ago answering a question about the cardinality of infinite sets that captivated me and sparked my passion for mathematics.

A SageMath Code

The code used to generate conductors and discriminants was:

```
conductors=[EllipticCurve([0, 0, 0, F, j+1]).conductor() for j in
     range(1000)]
discriminants=[abs(EllipticCurve([0, 0, 0, F, (j+1)]).
    discriminant()) for j in range(1000)]
```

The code used to check if a certain family of curves had a certain branch was:

```
def branch(A,n):
    conductors=[EllipticCurve([0, 0, 0, F, j+1]).conductor() for j
         in range(1000)]
    discriminants=[abs(EllipticCurve([0, 0, 0, F, (j+1)]).
        discriminant()) for j in range(1000)]
    return [x for x in conductors if n*x in discriminants]
```

Which is runnable using:

```
len(branch(A,o))
```

Where A is A in the curve $y^2 = x^3 + Ax + b$, and o is the order of the branch to check. With the len, it will return a number which is the number of points on that branch taking b from 0 to 1000. The higher the number, the denser the branch.

References

[1] Andrew Ogg. Elliptic curves and wild ramification. *American Journal of Mathematics*, 89:1–21, 1967.

[2] Takeshi Saito. Conductor, discriminant, and the noether formula of arithmetic surfaces. *Duke Math*, 57:151–173, 1988.

[3] John Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. *Lecture Notes in Math*, 467:33–52, 1975.

[4] Shinichi Mochizuki. Arithmetic deformation theory via arithmetic fundamental groups and nonarchimedean theta functions. *The 3rd Mathematical Society of Japan*, Seasonal:1–29, 2015.

[5] Qing Liu. Definition and meaning of the conductor of an elliptic curve.

[6] Á Lozano-Robledo. *Elliptic Curves, Modular Forms, and their L-Functions.*

[7] Joe H. Silverman. Finiteness of elliptic curves of a given conductor.

[8] Dr. Gerry Myerson. Consequences of szpiro's conjecture.

[9] Joe Silverman John Cremona. Conductor of an elliptic curve.

[10] Alina Bucur. Discriminant of an elliptic curve over q.

[11] Joe H. Silverman. *The Arithmetic of Elliptic Curves.*