

# Basics of elliptic curves

Matthew P. Young  
American Institute of Mathematics

June 1, 2006

# 1 Definition and Basic Invariants

Elliptic curves are the simplest algebraic curves that are not completely understood. In fact, they have a rich structure that makes their study very attractive. Many important questions remain open yet there has been incredible recent progress towards our understanding of elliptic curves.

In this lecture our primary goal is to describe the conjecture of Birch and Swinnerton-Dyer. In order to reach this goal in one lecture it was necessary to only describe the bare necessities. The books by Knapp [Kn] and Silverman [Si1] are good choices for further study.

## 1.1 Weierstrass equations

An elliptic curve  $E$  over a field  $K$  can be defined explicitly by a Weierstrass equation of the form

$$(1) \quad E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where  $a_1, a_2, a_3, a_4, a_6 \in K$ . In this lecture we are primarily interested in  $K = \mathbb{Q}$ , but even to understand this case it is important to consider  $K = \mathbb{F}_p$  and  $K = \mathbb{C}$ . If the characteristic of  $K$  is not 2 or 3 then a change of variables can put  $E$  in the simpler form

$$(2) \quad y^2 = x^3 + ax + b.$$

### Exercise.

1. Show that if  $K$  does not have characteristic 2 then (1) can be simplified by completing the square on the left hand side to give

$$(3) \quad E : y^2 = x^3 + a'_2x^2 + a'_4x + a'_6,$$

where

$$\begin{aligned} a'_2 &= a_2 + a_1^2/4, \\ a'_4 &= a_4 + a_1a_3/2, \\ a'_6 &= a_6 + a_3^2/4. \end{aligned}$$

2. Show that if  $K$  does not have characteristic 3 then under a change of variables, (3) takes the form

$$(4) \quad E : y^2 = x^3 + a''_4x + a''_6,$$

where

$$\begin{aligned} a''_4 &= a'_4 - a_2'^2/3, \\ a''_6 &= a'_6 - a_2'a'_4/3 + 2a_2'^3/27. \end{aligned}$$

The real locus of solutions of an elliptic curve looks like one of the following (depending on if the cubic polynomial  $x^3 + ax + b$  has one or three real roots):

Not every cubic equation of the form (2) defines an elliptic curve; we require the additional property that the curve be nonsingular. In general, a curve given by an equation of the form  $f(x, y) = 0$  is nonsingular if it has a well-defined tangent line at every point. For example, the curve

$$y^2 = x^3 - 3x + 2 = (x + 2)(x - 1)^2$$

is singular at  $x = 1, y = 0$  since it crosses itself (it has a double root at this point). We say that this curve has a *node*. The curve

$$y^2 = x^3$$

is singular because it has a triple root at  $x = 0, y = 0$ ; we say that it has a *node*.

The *discriminant*  $\Delta$  given by

$$(5) \quad \Delta = -16(4a^3 + 27b^2)$$

is nonzero if and only if (2) is nonsingular.

## 2 Rational points

Number theorists want to understand the set of rational points on an elliptic curve  $E$  over  $\mathbb{Q}$ . Some sample questions:

- Are there any rational solutions? “How many?”
- Can we effectively compute solutions?

More generally we may want to study elliptic curves over a number field  $K$ , but already the case of  $K = \mathbb{Q}$  is plenty difficult and there has been more progress in this case. Of course we are interested in such diophantine problems for other algebraic varieties, but elliptic curves are exceedingly special. The important feature that sets elliptic curves apart is that the set of rational points on an elliptic curve forms a group. In practice this means that if we can find one or more rational points on an elliptic curve, then we can use the group law to find more points (that could be otherwise difficult to detect).

### 2.1 The group law

*Example (1).* Let  $E : y^2 = x^3 + x - 1$ . By inspection,  $P = (1, 1) \in E(\mathbb{Q})$ . We compute

$$\begin{aligned} 2P &= (2, -3), \\ 3P &= (13, 47), \\ 4P &= \left(\frac{25}{36}, \frac{37}{216}\right), \\ 5P &= \left(\frac{685}{121}, -\frac{18157}{1331}\right), \\ 6P &= \left(\frac{7082}{2209}, \frac{615609}{103823}\right), \\ 7P &= \left(\frac{154513}{196249}, -\frac{45623219}{86938307}\right), \\ 8P &= \left(\frac{9781441}{197136}, -\frac{30597832799}{87528384}\right), \\ 9P &= \left(\frac{645430801}{468073225}, \frac{17542288296299}{10126764222875}\right), \\ &\vdots \end{aligned}$$

*Example (2).*

$$E : y^2 = x^3 + x + 2.$$

$$\begin{aligned} P &= (1, 2), \\ 2P &= (-1, 0), \\ 3P &= (1, -2), \\ 4P &= O. \end{aligned}$$

## 2.2 The group structure

The structure of the group of rational points  $E(\mathbb{Q})$  is given by

**Theorem (Mordell-Weil).** *Let  $E/\mathbb{Q}$  be an elliptic curve. The group of rational points  $E(\mathbb{Q})$  forms a finitely generated abelian group.*

By the structure theorem for finitely generated abelian groups,

$$(6) \quad E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E_{\text{tors}},$$

where  $r$  is a nonnegative integer called the (*algebraic*) *rank*, and  $E_{\text{tors}}$  is a finite group. Note that  $r > 0$  if and only if  $E$  has infinitely many rational points.

The torsion group is completely understood.

**Theorem (Mazur).**  *$E_{\text{tors}}$  is one of the following groups:*

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z}, & \quad 1 \leq m \leq 10 \text{ or } m = 12, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}, & \quad 1 \leq m \leq 4. \end{aligned}$$

In practice the torsion group can be computed very efficiently.

The rank is much more mysterious. Some questions:

- Is the rank effectively computable?
- Can the rank be arbitrarily large? (Current record is  $\geq 28$ , due to Elkies)
- What is the statistical behavior of the rank? (e.g. what percentage of elliptic curves have rank 0, 1, 2, ...)

$L$ -functions are helpful to understand the rank.

### 3 The $L$ -function

To any elliptic curve  $E$  is associated a degree two  $L$ -function  $L(s, E)$  which contains much of the arithmetical information of  $E$ .

#### 3.1 Some motivation

Determining if an elliptic curve has rational points is very difficult. It is a common practice in number theory to try to understand the global properties of an algebraic object by studying the object locally (i.e. over  $\mathbb{F}_p$  for all primes  $p$ ). For example, this method works very well for quadratic equations with the aid of the Hasse-Minkowski theorem (which states that a quadratic equation has a rational solution if and only if it has a solution in every  $p$ -adic field  $\mathbb{Q}_p$ ).

It is therefore tempting to study an elliptic curve  $E$  over every finite field  $\mathbb{F}_p$  and hope to glean information about  $E(\mathbb{Q})$  by piecing this information together. This idea is powerful yet vague; the key to making this connection precise is the  $L$ -function.

Suppose  $E$  is given by a Weierstrass equation (2) with integer coefficients. By reducing the coefficients  $(\text{mod } p)$ , we may study the structure of the finite group  $E(\mathbb{F}_p)$  (including the point at infinity). For each  $p$  let

$$(7) \quad a_p = p + 1 - |E(\mathbb{F}_p)|.$$

A heuristic argument indicates that  $|E(\mathbb{F}_p)| \approx p + 1$ : For a given  $x \pmod{p}$ , there exists a  $y \pmod{p}$  on  $E(\mathbb{F}_p)$  if and only if  $x^3 + ax + b$  is a square  $(\text{mod } p)$  (in which case there are generally two  $y$ 's satisfying  $y^2 = x^3 + ax + b$ , unless  $x^3 + ax + b \equiv 0 \pmod{p}$ ). The squares form an index 2 subgroup in  $\mathbb{F}_p^*$ , so it should be roughly equally likely that  $x^3 + ax + b$  is a square as it is a non-square.

In fact,  $p + 1$  is a close approximation to  $|E(\mathbb{F}_p)|$ :

**Theorem 3.1 (Hasse's bound).**

$$(8) \quad |a_p| \leq \sqrt{p}.$$

The idea behind studying these  $a_p$ 's is that if  $E$  has large rank (i.e. lots of rational points), then the reductions  $E(\mathbb{F}_p)$  should be more likely to have an excess of points.

### 3.2 Some invariants

One difficulty with studying an elliptic curve modulo different primes is that not all Weierstrass equations are created equal. The problem is that a change of variables over  $\mathbb{Q}$  can alter the behavior of the reductions  $E/\mathbb{F}_p$ . For example, consider the curve

$$E : y^2 = x^3 + 5^4x - 5^6.$$

Reducing  $E \pmod{5}$  clearly gives the curve  $y^2 = x^3$  which has

$$E(\mathbb{F}_5) = \{O, (0, 0), (1, \pm 1), (4, \pm 2)\},$$

which gives  $a_5 = 0$ . The change of variables  $y \rightarrow 5^3y$ ,  $x \rightarrow 5^2x$  gives a  $\mathbb{Q}$ -isomorphic curve

$$E' : y^2 = x^3 + x - 1,$$

which has

$$E'(\mathbb{F}_5) = \{O, (0, \pm 2), (1, \pm 1), (2, \pm 2), (3, \pm 2)\},$$

and therefore  $a_5 = -3$ . The latter choice of Weierstrass equation is superior because the reduction of  $E'$  modulo 5 is nonsingular, whereas  $E(\mathbb{F}_5)$  has a cusp. Another difference between these two Weierstrass equations is that  $E'$  has discriminant  $\Delta' = -2^4 \cdot 31$  and  $E$  has discriminant  $\Delta = 5^{12}\Delta'$ .

Amongst all possible Weierstrass equations, there is a ‘best’ one (not unique) called a *global minimal Weierstrass equation* in which the discriminant is minimized. Global minimal Weierstrass equations are good for studying the reductions of  $E \pmod{p}$  because the structure of the group  $E(\mathbb{F}_p)$  is independent of the choice of minimal equation.

To any elliptic curve  $E$  is associated an invariant called the *conductor*  $N$ . The conductor is a divisor of the (minimal) discriminant but is rather more difficult to describe precisely. The set of primes dividing the minimal discriminant coincides with the set of primes dividing the conductor (which are the primes such that the reduced curve is singular). Except for the primes 2 and 3, the power of the prime  $p$  dividing  $N$  is either 1 or 2, depending on whether  $E$  has a node or a cusp  $\pmod{p}$ , respectively. There is no such simple formulation of the power of 2 or 3 but they can be determined by applying Tate’s algorithm (described in [Si2], Chapter IV §9).

### 3.3 Constructing the $L$ -function

Finally we may define the  $L$ -function associated to an elliptic curve  $E$  given by a global minimal Weierstrass equation as the following Euler product

$$(9) \quad L(s, E) = \prod_{p \nmid N} \left(1 - \frac{a_p/\sqrt{p}}{p^s} + \frac{1}{p^{2s}}\right)^{-1} \prod_{p \mid N} \left(1 - \frac{a_p/\sqrt{p}}{p^s}\right)^{-1}.$$

Hasse’s bound implies  $|a_p/\sqrt{p}| < 2$  so the product converges absolutely in the half-plane  $\text{Re}(s) > 1$ . This Euler product extends the definition of  $a_n$  to composite  $n$  by

$$(10) \quad L(s, E) = \sum_{n=1}^{\infty} \frac{a_n/\sqrt{n}}{n^s}.$$

Further,  $L(s, E)$  extends to an entire function that satisfies the functional equation

$$(11) \quad \Lambda(s, E) := \left( \frac{\sqrt{N}}{2\pi} \right)^s \Gamma\left(s + \frac{1}{2}\right) L(s, E) = \epsilon \Lambda(1 - s, E),$$

where  $\epsilon = \pm 1$  is called the *root number*.

These properties of the  $L$ -function follow from the famous

**Theorem 3.2 (Modularity Theorem).** *The function*

$$(12) \quad f(z) = \sum_n a_n e(nz)$$

is a weight two newform on  $\Gamma_0(N)$ .

See [W], [TW], [BCDT].

### 3.4 The conjecture of Birch and Swinnerton-Dyer

A beautiful connection between the arithmetic of  $E$  and analytic properties of its  $L$ -function is spelled out by

**Conjecture (Birch-Swinnerton-Dyer).** *The order of vanishing of  $L(s, E)$  at  $s = \frac{1}{2}$  is equal to the rank of  $E$ .*

Since  $L(s, E)$  is constructed out of local data (the  $a_p$ 's), this conjecture indicates the precise way for the local-global principle to work for elliptic curves.

In fact, there is a more precise version of the conjecture that gives an exact formula for the first nonvanishing coefficient in the power series expansion of  $L(s, E)$  around the point  $s = \frac{1}{2}$  in terms of various arithmetical quantities associated to  $E$ .

**Conjecture (More precise version).**

$$(13) \quad \lim_{s \rightarrow \frac{1}{2}} \left(s - \frac{1}{2}\right)^r L(s, E) = \Omega |\text{III}| 2^r R |E_{\text{tors}}|^{-2} \prod_{p|N} c_p$$

Here  $\Omega$  is a period integral (easy to compute),  $R$  is the regulator (a generalization of the familiar regulator from basic algebraic number theory),  $c_p$  are called the Tamagawa numbers (they are also easy to compute), and  $\text{III}$  is the Tate-Shafarevich group (a very complicated group, only conjectured to be finite). Note the similarity with

### 3.5 Explicit computations

It is instructive (not to mention fun!) to do explicit computations with elliptic curves. PARI/GP [P] is a free program that can perform many useful computations with elliptic curves. Working through the tutorial (<http://pari.math.u-bordeaux.fr/pub/pari/manuals/2.3.0/tutorial.pdf>) is a good place to start.

PARI can easily compute the conductor, the coefficients of the  $L$ -function  $a_n$ , torsion group, Tamagawa numbers, and the period integral (but not  $\text{III}$ , the regulator  $R$ , and the rank  $r$ ).

The central value can be computed using the approximate functional equation:

### Proposition 3.3.

$$(14) \quad L\left(\frac{1}{2}, E\right) = (1 + \epsilon) \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}}.$$

Due to the decay of the exponential this sum may be closely approximated by a finite sum with approximately  $\sqrt{N}$  terms. There are similar formulas for the derivatives of  $L(s, E)$  (with different smoothing functions than the exponential).

M. Rubinstein's  $L$  package [R] can perform many computations with  $L$ -functions. For elliptic curve computations it requires input of basic data (conductor, vector of coefficients  $a_n$ , functional equation) which can be computed with PARI.

## References

- [BCDT] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over  $\mathbb{Q}$ : wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), no. 4, 843–939.
- [IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004. xii+615 pp.
- [Kn] A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992. xvi+427 pp.
- [P] PARI/GP, Version 2.3.0, Bordeaux, 2006, <http://pari.math.u-bordeaux.fr/>.
- [R] M. Rubinstein,  $L$ , [http://pmmac03.math.uwaterloo.ca/mrubinst/L\\_function\\_public/L.html/](http://pmmac03.math.uwaterloo.ca/mrubinst/L_function_public/L.html/).
- [Si1] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.
- [Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.
- [TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) 141 (1995), no. 3, 553–572.
- [W] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (1995), no. 3, 443–551.