A n00b'S GUIDE TO THE BSD CONJECTURE.

TOM BOOTHBY

TO ME, ONE YEAR AGO

1. Internal Monologue (Prologue)

For some time now, I have been doing various computations and taking classes involving elliptic curves and the BSD conjecture. During this time, I have seen various definitions of the quantities involved in the BSD conjecture, but they haven't "stuck". When I sit down and work on a problem in number theory, it takes me a while to recall the definitions, or worse, I have to look them up. To date, I have not found a decent reference which spells everything out in *clear* and *concise* terms. Rather, I have found a number of wonderful references that are either very explicit, or very concise and as a result, send the beginner on long side-quests to unravel definitions of seemingly obscure notations that seem very natural to the author and other experts in the field.

My goal in writing this document is to present every quantity in the BSD conjecture in terms that I would have understood on my first day as a graduate student. Preferably, something that I would have immediately recognized as a reference that I should packrat away onto my desktop and print out a few copies for my various workspaces. In discussing this paper with colleagues, I have recognized a secondary goal: to make it useful for other students in the same position.

To that end, I assume that the reader has attended introductory courses in algebra, analysis, and geometry. That is, an understanding of

- elementary set theory
- arithmetic over finite fields,
- groups and quotient groups,
- calculus, (limits, derivatives and integrals)
- a little complex analysis,
- the genus of a curve.

All in all, the coverage of any topic is the bare minimum. I have attempted to streamline the definitions so they are comprehensible, easy to find in the document: that is, the fewer pages to thumb through, the easier. Finally, a note on the references. For almost every definition, I consulted each of [1, 4, 5, 6, 7], as well as Wikipedia and PlanetMath. Wherever I wasn't satisfied by the definitions there, I consulted William Stein.

2. A Little Background

The typical undergraduate education may have left a hole that we need to fill before we can begin. The p-adic numbers are often covered in analysis, or even

Date: June 5, 2009.

topology, but truly shine in a number-theoretic setting. We do not do the topic justice, and the reader is strongly encouraged to read [2]. Before that, we define a couple of bits of notation:

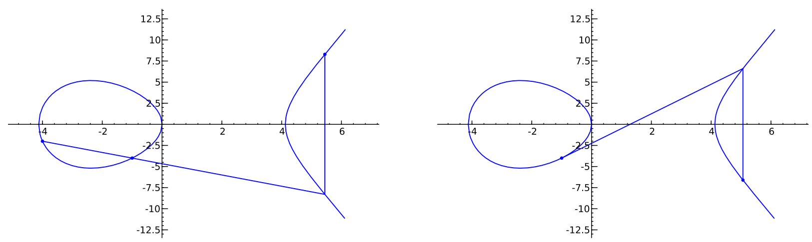
(1) Given a set S and an equivalence relation $\sim$ on the set, we can define a quotient
$$S/\sim \stackrel{\text{def}}{=} \{\{x \sim y : y \in S\} : x \in S\}.$$
(2) If a set has a finite cardinality, we write $\#S \stackrel{\text{def}}{=} |S|$.

2.1. **p-Adic Numbers.** We recall a definition of the real numbers as "the" analytic completion of the rationals; we denote the Cauchy sequences in $\mathbb{Q}$ by
$$S = \left\{\{x_0, x_1, \cdots\} \subset \mathbb{Q} : \lim_{n\to\infty} \sup_{m>n} |x_n - x_m| = 0\right\},$$
then we can define an equivalence relation on S: if $x = \{x_0, x_1, \cdots\}$ and $y = \{y_0, y_1, \cdots\}$, then $x \sim y$ if
$$\lim_{n\to\infty} x_n - y_n = 0.$$
Then,
$$\mathbb{R} \stackrel{\text{def}}{=} S/\sim$$
That is, a real number is represented by the equivalence classes of rational sequences which converge to that number.

We define the p-adic numbers similarly. For any prime $p \in \mathbb{Z}$, we can define the *p-adic valuation* on $\mathbb{Q}$ by
$$\nu_p\left(\frac{a}{b}\right) = p^{\operatorname{ord}_p b - \operatorname{ord}_p a},$$
where $\operatorname{ord}_p x$ is the largest exponent e such that $p^e|x$. It is easy to check that ν_p is a metric, which gives us a natural notion of convergence. As above, we consider the Cauchy sequences in $\mathbb{Q}$,
$$S_p = \left\{\{x_0, x_1, \cdots\} \subset \mathbb{Q} : \lim_{n\to\infty} \sup_{m>n} \nu_p\left(x_n - x_m\right) = 0\right\},$$
and let $x \sim_p y$ if
$$\lim_{n\to\infty} \nu_p\left(x_n - y_n\right) = 0.$$
Then, we define the *p-adic numbers* as the analytic completion of $\mathbb{Q}$ under this metric;
$$\mathbb{Q}_p \stackrel{\text{def}}{=} S_p/\sim_p$$
Similar to the reals, $\mathbb{Q}_p$ is an uncountable field which properly contains $\mathbb{Q}$, in which every Cauchy sequence converges to a limit in $\mathbb{Q}_p$ with respect to the p-adic valuation.

3. Definitions

Throughout this paper, $E(K)$ is an elliptic curve over a field K; that is, a set of points $(x, y) \in K^2$ which satisfy the *Weierstrass equation* with coefficients $a_i \in K$,
$$y^2 + a_1yx + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
along with a formal "point at infinity", $\mathcal{O}$. Further, we will require that the curve is nonsingular and the Weierstrass equation is minimal; these terms are defined



$(-4,-2)+(-1,-4)=\left(\frac{49}{9},\frac{224}{27}\right)$ $\qquad$ $(-1,-4)+(-1,-4)=\left(\frac{81}{16},-\frac{423}{64}\right)$

FIGURE 1. Group law on $y^2 = x^3 - 17x$.

below. For brevity, we denote $E = E(\mathbb{Q})$, and other fields will be noted explicitly. Then, we define the b- and c-*invariants* and *discriminant* Δ of an elliptic curve by

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2, \\
b_4 &= 2a_4 + a_1a_3, \\
b_6 &= a_3^2 + 4a_6, \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_3^2a_2 - a_4^2, \\
c_4 &= b_2^2 - 24b_4, \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.
\end{aligned}$$

If $\mathrm{char}(K) \neq 2, 3$, the elements of E form an abelian group $(E, +)$ with

$$+ : E(K) \times E(K) \to E(K)$$

where $P = (x_1, y_1)$, $Q = (x_2, y_2)$,

(1) Inversion is defined by

$$-P = (x_1, -y_1 - a_1x_1 - a_3)$$

(2) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$,, then

$$P + Q = \mathcal{O}.$$

In particular, $P - P = \mathcal{O}$, and $P + \mathcal{O} = P$.

(3) Otherwise, let

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2, \end{cases}$$

and

$$\nu = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{if } x_1 \neq x_2, \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{if } x_1 = x_2. \end{cases}$$

Then,

$$P + Q = \left((\lambda + a_1)\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3\right).$$

Geometrically, one can view the point addition formula as letting

$$-(P+Q) = E \cap \overline{PQ} \setminus \{P, Q\},$$

where $\overline{PQ}$ is the infinite line through P and Q, or if $P = Q$, the tangent of E at P. Similarly,

$$-P = E \cap \{x_1, y : y \in K, y \neq y_1\},$$

which is roughly the point reflected about the x-axis. Examples of this can be seen in figure 1. Note that any vertical line "intersects" the point at infinity, so $\mathcal{O}$ is the natural choice as the identity element.

By the Mordell-Weil theorem, E is a finitely generated abelian group. Since E is abelian, its torsion subgroup

$$E_{tor} = \{P \in E : \langle P \rangle \approx \mathbb{Z}/n\mathbb{Z}, n < \infty\}$$

is normal, and E/E_{tor} is also an abelian group. Moreover, since E is finitely generated, its torsion subgroup is finite, and

$$E \approx \mathbb{Z}^r \times E_{tor}.$$

Then, r is the *algebraic rank* of E.

3.1. **Singularities.** Let

$$F(x,y) = y^2 + a_1yx + a_3y - x^3 - a_2x^2 - a_4x - a_6,$$

so $E(K)$ is precisely the solution set of F with an additional point $\mathcal{O}$. Then, we call a point (x,y) *singular* if

$$\frac{\partial F}{\partial x}(x,y) = \frac{\partial F}{\partial y}(x,y) = 0,$$

that is, if

$$a_1x + a_3 + 2y = a_1y - 2a_2x - 3x^2 - a_4 = 0.$$

If a point is not singular, we call it *nonsingular*. We compute the Taylor expansion of F at a singular point $P = (x_0, y_0)$,

$$F(x,y) = [(y-y_0) - \alpha(x-x_0)][(y-y_0) - \beta(x-x_0)] - (x-x_0)^3 \tag{1}$$

where $\alpha, \beta \in \overline{K}$, and if (x,y) is a singular point, and call P a *cusp* if $\alpha = \beta$, or a *node* if $\alpha \neq \beta$. See Figure 2 for a visual interpretation of this.

Similarly, if $\Delta = 0$, then we call E singular, otherwise E is nonsingular. This precisely corresponds to the curve having a singular point – if $c_4 = 0$, then E has a *cusp*, and if $c_4 \neq 0$, then E has a *node*.

3.2. **Minimal Weierstrass Equation and the Real Period.** If we parametrize a Weierstrass equation with coefficients in K via

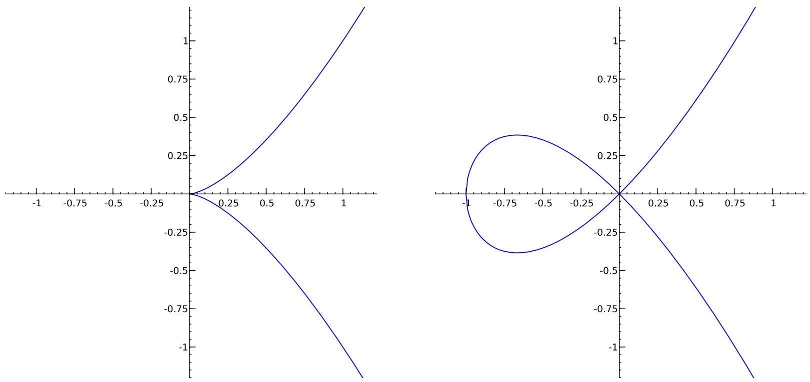
$$x = u^2x' + r, \qquad y = u^3y' + su^2x' + t \tag{2}$$

with $u, r, s, t \in K$, we obtain another Weierstrass equation for an elliptic curve E',

$$y'^2 + \overline{a}_1x'y' + \overline{a}_3y' = x'^3 + \overline{a}_2x'^2 + \overline{a}_4x' + \overline{a}_6,$$

and from this, another discriminant Δ'. The parametrizations (2) are called *permissible* if the obtained coefficients $\overline{a}_j$ are integral. Denote the family of elliptic curves that can be obtained by permissible parametrizations by $\mathbf{E}$ and if $p \in \mathbb{Z}$ is prime, define

$$\kappa_p(E) = \min\{\operatorname{ord}_p \Delta(E') : E' \in \mathbf{E}\}$$



$y^2 = x^3$ has a cusp at $(0,0)$ $\qquad$ $y^2 = x^3 + x^2$ has a node at $(0,0)$

FIGURE 2. Singular Curves

Then, a *minimal Weierstrass equation* is one such that

$$\Delta(E) = \prod_p p^{\kappa_p(E)}$$

Then, we define the *real period* of E,

$$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{2y + \overline{a}_1 x + \overline{a}_3},$$

where the coefficients $\overline{a}_j$ are obtained from a minimal Weierstrass equation for E.

3.3. **Reduction.** In many problems involving integers and rational numbers, it makes sense to reduce the problem modulo various primes. In the setting of elliptic curves, if p is a prime, we define the curve *reduced modulo* p

$$E(\mathbb{F}_p) = \left\{ (x,y) \in \mathbb{F}_p : y^2 + a_1 yx + a_3 y \equiv x^3 + a_2 x^2 + a_4 x + a_6, \mod p \right\}.$$

We say that the reduced curve has

(1) *Good* reduction if $E(\mathbb{F}_p)$ is non-singular; that is, $\Delta \not\equiv 0 \mod p$. Otherwise, E has *bad* reduction at p. Bad reduction takes a few forms, which follow.
(2) *Multiplicative* reduction if E has a node, that is, if $\Delta \equiv 0$ and $c_4 \not\equiv 0 \mod p$.
(3) *Additive* reduction if E has a cusp, that is, if if $\Delta \equiv c_4 \equiv 0 \mod p$.

In the case that E has bad reduction at p, we say that the reduction is *split* if $\alpha, \beta \in \mathbb{F}_p$ as in (1) and *non-split* otherwise.

3.4. **L-series.** We define the *L-series* of an elliptic curve

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

where a_n is a multiplicative series with

$$a_p = p + 1 - \#E(\mathbb{F}_p),$$

and

$$a_{p^m} = \begin{cases} a_p a_{p^{m-1}} - p a_{p^{m-2}}, & \text{if } \Delta \not\equiv 0 \mod p, \\ (a_p)^m, & \text{if } \Delta \equiv 0 \mod p. \end{cases}$$

It is highly nontrivial to prove that L has a holomorphic continuation to all of $\mathbb{C}$ – that is, L has a complex-valued derivative in the entire complex plane. We define the *analytic rank* of E by

$$r_{an} = \min \left\{ r \in \mathbb{Z}_{\geq 0} : L^{(r)}(E, 1) \neq 0 \right\}.$$

3.5. **Tate-Shafarevich Group.** An *algebraic variety*[3] is the solution set of a polynomial equation

$$X = \{x_1, \ldots, x_k \in K : F(x_1, \ldots, x_k) = 0\}$$

where $F \in K[x_1, \ldots, x_k]$, where $\mathbb{Q} \subseteq K$. Similarly, an *algebraic curve* is a one-dimensional algebraic variety. Given any algebraic curve X, we define the genus of X as the genus of the topological manifold

$$X(\mathbb{C}) = \{x_1, \ldots, x_k \in \mathbb{C} : F(x_1, \ldots, x_k) = 0\}.$$

Then, we let $C_1(K)$ denote the set of genus 1 curves X over K such that

$$X(\mathbb{Q}_p) \neq \emptyset \text{ for all prime } p \in \mathbb{Z}.$$

Then, if $X \in C_1$, we call a map

$$i : E \times X \to X$$

a simply transitive group action if for all $x, y \in X$ there is a unique $e \in E$ such that

$$i(e, x) = y,$$

and for all $e, f \in E$ and all $x \in X$,

$$i(f, i(e, x)) = i(f + e, x).$$

Then, we define

$$I(E, X) = \{\text{simply transitive group actions } i : E \times X \to X\}$$

and

$$S = \{(X, i) : X \in C_1(\mathbb{C}), i \in I(E, X)\}.$$

Next, we define an equivalence relation $(\sim)$ by $(X, i) \sim (Y, j)$ when there exists a bijection $\varphi : X \to Y$ such that for all $e \in E$,

$$\varphi(i(e, x)) = j(e, \varphi(x)).$$

Thus, we define

$$Ш = Ш(E/\mathbb{Q}) = S/\sim.$$

For now, we shall treat this as a rather arbitrarily-defined set – a proper discussion of Ш should, at the very least, explain why it is called the Tate-Shafarevich *group*.

3.6. **Tamagawa Numbers.** For a prime $p \in \mathbb{Z}$, define

$$c_p = \left[E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)\right]$$

where $E^0(\mathbb{Q}_p)$ is the subgroup of points in $E(\mathbb{Q}_p)$ whose reduction modulo p is nonsingular. One can prove that

(1) If E has good reduction at p then $c_p = 1$.
(2) If E has additive reduction at p, then $c_p \leq 4$.
(3) If E has non-split multiplicative reduction at p, then

$$c_p = \begin{cases} 1 & \operatorname{ord}_p \Delta \text{ is odd, and} \\ 2 & \text{otherwise.} \end{cases}$$

(4) Otherwise, E has split multiplicative reduction, and $c_p = \operatorname{ord}_p \Delta$.

In particular, note that $c_p = 1$ for all but finitely many $p \in \mathbb{Z}$, so

$$\prod_p c_p \in \mathbb{Z}.$$

3.7. **Regulator.** For a point $P = (x, y) \in E(\mathbb{Q})$, we define the *naïve height* of P,

$$h(P) = \max \{\log |a|, \log |b|\}$$

where $x = \frac{a}{b}$ is in reduced terms. Then, we define the *Néron-Tate canonical height*

$$\hat{h}(P) = \lim_{n\to\infty} \frac{h(2^n P)}{4^n},$$

and the *height pairing* on $E \times E$ by

$$\langle P, Q\rangle = \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right).$$

The height pairing is a *bilinear form*, that is,

$$\langle P + P', Q\rangle = \langle P, Q\rangle + \langle P', Q\rangle,$$

and

$$\langle P, Q + Q'\rangle = \langle P, Q\rangle + \langle P, Q'\rangle,$$

so

$$\langle nP, Q\rangle = \langle P, nQ\rangle = n\langle P, Q\rangle.$$

If $P_1, \ldots, P_r$ generates E/E_{tor}, then we define the height matrix to be an $r \times r$ matrix,

$$H = (\langle P_i, P_j\rangle).$$

Then, we define the *regulator* of E by

$$\operatorname{Reg}(E) = \det H.$$

4. Holes

Section 3 introduces a large volume of material, with absolutely no proof in sight. Here, we attempt to list a number of missing proofs, and reasonable questions that one should ask upon seeing these definitions. Since proofs, and resolutions to everything below exist, the reader should treat these as exercises. The author certainly intends to.

4.1. **Missing Proofs.**

(1) E is a group.
(2) E is singular if and only if $\Delta = 0$, classification of singularities based on c_4.
(3) Mordell's theorem, or the more general Mordell-Weil theorem, that E is finitely generated.
(4) L has a holomorphic continuation to all of $\mathbb{C}$.
(5) Ш is a group.
(6) All claims made about Tamagawa numbers.
(7) $E^0(\mathbb{Q}_p)$ is a closed subgroup of $E(\mathbb{Q}_p)$
(8) The N'eron-Tate canonical height is finite.
(9) The height pairing $\langle\cdot,\cdot\rangle$ is a bilinear form.

4.2. **Natural Questions.**

(1) Is there a group law in characteristic 2 or 3?
(2) Is the regulator well-defined? From the definition, it is not obvious that a minimal Weierstrass equation exists, and if one does, that it is the only one.
(3) Is the Néron-Tate canonical height well-defined on E/E_{tor}? It's clear that $\hat{h}(P) = 0$ if P has finite order; but is $\hat{h}(P+Q) = \hat{h}(Q)$ for all $Q \in E$, too?
(4) Is the regulator well-defined? At first glance, it looks like it could depend heavily upon the choice of basis for E.

It is conjectured that Ш is a finite group. Incredibly, it is known that if Ш is finite, its order is square.

5. The Birch and Swinnerton-Dyer Conjecture

Conjecture 5.1. *Let E be an elliptic curve over $\mathbb{Q}$ of algebraic rank r. Then, $r = \operatorname{ord}_1 L(E,s)$, and*

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \operatorname{Reg}(E) \cdot \#\text{Ш} \cdot \prod_p c_p}{\#(E_{tor})^2}.$$

Alternately, we can reformulate this into a statement about the Tate-Shafarevich group, since it is by far the most mysterious object we've defined. That is, we define the *analytic order of* Ш,

$$\#\text{Ш}_{an} = \frac{L^{(r)}(E,1) \cdot \#(E_{tor})^2}{r! \cdot \Omega_E \cdot \operatorname{Reg}(E) \cdot \prod_p c_p}.$$

Of course, we expect a finite group to have an integral order – however, it is not even clear that this is a rational number.

References

[1] F. Diamond and J. Shurman. *A first course in modular forms. GTM 228.* Springer, 2005.
[2] Fernando Quadros Gouvêa. *p-Adic numbers: An Introduction.* Springer, 1997.
[3] B. Mazur. On the passage from local to global in number theory. *AMERICAN MATHEMATICAL SOCIETY*, 29(1):14–50, 1993.
[4] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves (Graduate Texts in Mathematics).* Springer, January 1994.
[5] William A. Stein. *Algebraic Number Theory, a Computational Approach.* wstein.org, June 2009.
[6] William A. Stein. *The Birch and Swinnerton-Dyer Conjecture, a Computational Approach.* wstein.org, June 2009.
[7] L.C. Washington. *Elliptic curves: Number theory and cryptography.* Chapman & Hall/CRC, 2008.