Birch and Swinnerton-Dyer conjecture

R. van Bommel

Monday 18 April 2016

These are notes for a talk held at the seminar on rational points on elliptic curves in Leiden, The Netherlands, on Monday 18 April. The author apologises for all errors, unclarities, omissions of details and other imperfections and encourages the reader to send them by email to the author at the following address: r.van.bommel@math.leidenuniv.nl. These notes are mainly based on [Tate74], [Silv09] and [Cohe93]; a more comprehensive list of references can be found at the end of these notes.

1 The conjecture

Let us first state the conjecture this talk is about. To quote Tate, the Birch and Swinnerton-Dyer (BSD) conjecture is a remarkable conjecture, which relates the behaviour of a function L at a point where it is not known to be defined to the order of a group that is not known to be finite.

Conjecture 1 (Birch and Swinnerton-Dyer)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then*

$$\lim_{s\to 1} \frac{L_E(s)}{(s-1)^r} = \frac{|Ш| \cdot \Omega \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{|E(\mathbb{Q})_{\mathrm{tors}}|^2}.$$

Here

- $L_E(s)$ is the L-function of E (to be defined in section 2);
- r is the rank of E, i.e. the rank of the free part of the finitely generated abelian group $E(\mathbb{Q})$;
- Ш is the Tate-Shaferevich group as defined in the talk by Van der Lugt in [Lugt16].
- Ω is the real period of E (to be defined in section 3) times the number of connected components of $E(\mathbb{R})$;
- $\mathrm{Reg}(E/\mathbb{Q})$ is the regulator of E (to be defined in section 4);
- c_p is the Tamagawa number of E at p (to be defined in section 5);
- $E(\mathbb{Q})_{\mathrm{tors}}$ is the torsion subgroup of $E(\mathbb{Q})$.

2 L-functions

Let $E/\mathbb{Q}$ be an elliptic curve and let p be a prime number. Then we can take a minimal Weierstraß model of E at p, i.e. a model of the form

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6, \quad c_1, c_2, c_3, c_4, c_6 \in \mathbb{Z},$$

for which the discriminant has a minimal number of factors p. Reducing the coefficients modulo p, we get a (possibly singular) algebraic variety E_p defined over $\mathbb{F}_p$. Then we define the integer $a_p := p + 1 - |E_p(\mathbb{F}_p)|$.

Remark 2. If E has good reduction at p, then $-2\sqrt{p} \leqslant a_p \leqslant 2\sqrt{p}$ by the Hasse bound. If E has additive reduction, then $E_p(\mathbb{F}_p) \cong \mathbb{F}_p \cup \{\text{sing. pt.}\}$ and hence $a_p = 0$. If E has split multiplicative reduction, then $E(\mathbb{F}_p) \cong \mathbb{F}_p^* \cup \{\text{sing. pt.}\}$ and hence $a_p = 1$. Finally, if E has non-split multiplicative reduction then $E(\mathbb{F}_p) \cong \mathbb{F}_{p^2}^*/\mathbb{F}_p^* \cup \{\text{sing. pt.}\}$ and hence $a_p = -1$.

Definition 3 (L-function)**.** Let Δ be the discriminant of E. Then the L-function of $E/\mathbb{Q}$ is defined as

$$L_E(s) = \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \cdot \prod_{p\nmid\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}.$$

Remark 4. By formal expansion we can write $L_E(s)$ as a Dirichlet series $\sum c_n n^{-s}$. Using the modularity theorem, one can prove that the the function $f(\tau) = \sum c_n e^{2\pi i n\tau}$ for $\tau \in \mathbb{H}$ is a modular cusp form of weight 2 for the congruence subgroup $\Gamma_0(N)$ (see [Mart16] for definitions). The L-function of this cusp form is again $L_E(s)$.

Using the Hasse bound, it is quite easy to prove that the series $L_E(s)$ converges absolutely for $\mathrm{Re}(s) > \frac{3}{2}$. Now we can use the techniques known for modular forms to extend the L-function holomorphically to $\mathbb{C}$, using something similar to the Riemann functional equation for the ζ-function, see for example [Shim71, Th. 3.66, p. 93].

Now we would like to evaluate the L-series in $s = 1$. It is a well-known fact that the harmonic series is not convergent. Hence, it would be a bad idea to just plug in $s = 1$ in the Dirichlet series of $L_E(s)$. The following trick will help us.

Proposition 5 ([Cohe93, Prop. 7.5.8, p. 405])**.** *Let E be a modular elliptic curve of conductor N. Let $\varepsilon \in \{\pm 1\}$ be the sign of the functional equation for $L_E(s)$.*[1] *Then*

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

This series is converging very quickly and can be used to evaluate the L-series in $s = 1$. We will look at some examples.

Example 1. Let $E_0/\mathbb{Q}$ be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + xy + y = x^3 + x^2 - 352x - 2689.$$

[1] If you don't know what this means, it doesn't matter that much. The important thing is that these invariants are easy to calculate. If you want, you can look them up in the literature.

It has rank 0 and evaluating first million terms of the Dirichlet series of the L-function gives 1.0697, which is quite far the actual value $L_{E_0}(1) \approx 1.10219253$, which calculated using proposition 5 and is accurate up to the indicated precision.

Example 2. Let $E_1/\mathbb{Q}$ be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + y = x^3 - x.$$

It has rank 1 and the sign of the functional equation of $L_{E_1}(s)$ is -1. Hence, $L_{E_1}(1) = 0$ by proposition 5. Now we would like to calculate $L'_{E_1}(1)$. There is a trick similar to proposition 5 that can be found in [Cohe93, Prop. 7.5.9, p. 406] that we can use and we find $L'_{E_1}(1) \approx 0.30599977$.

3 Real periods

The real period of an elliptic curve is very easy to define.

Definition 6 (real period)**.** Let $E/\mathbb{Q}$ be an elliptic curve whose minimal Weierstraß equation is

$$y^2 + c_1xy + c_3y = x^3 + c_2x^2 + c_4x + c_6, \quad c_1, c_2, c_3, c_4, c_6 \in \mathbb{Z},$$

and let $E^0(\mathbb{R})$ be a connected component of $E(\mathbb{R})$. Then the *real period* of E is defined as

$$\int_{E^0(\mathbb{R})} \frac{dx}{2y + c_1x + c_3} \in \mathbb{R}.$$

It is also quite easy to approximate the real period using the following algorithm.

Algorithm 7 ([Cohe93, Alg. 7.4.7, p. 391])**.**

1. *Calculate* $b_2 = c_1^2 + 4c_2$, $b_4 = c_1c_3 + 2c_4$ *and* $b_6 = c_3^3 + 4c_6$.
2. *Consider the polynomial* $4x^3 + b_2x^2 + 2b_4x + b_6$. *Assume it has three real roots (if it does not have three real roots, the algorithm is a bit different, see loc. cit.)* $e_1 > e_2 > e_3$ *and calculate them.*
3. *Set* $(A_0, B_0) = (\sqrt{e_1 - e_3}, \sqrt{e_1 - e_2})$ *and calculate iteratively*

   $$(A_{n+1}, B_{n+1}) = \left(\frac{A_n + B_n}{2}, \sqrt{A_nB_n}\right),$$

   until $|A_n - B_n|$ *is small enough to approximate the limit value*

   $$A = \lim_{n\to\infty} A_n = \lim_{n\to\infty} B_n.$$

4. *Now the real period equals* $\frac{\pi}{A}$.

Example 1. Let $E_0/\mathbb{Q}$ again be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + xy + y = x^3 + x^2 - 352x - 2689.$$

By calculation we find $(b_2, b_4, b_6) = (5, -703, -10755)$ and by approximating the roots of the polynomial we find $(e_1, e_2, e_3) \approx (21.248077, -11.248077, -11.25)$. Already for $n = 100$, we find that $|A_n - B_n|$ is smaller than the precision of the computer, and we find that the real period is approximately 0.551096265.

Example 2. Let $E_1/\mathbb{Q}$ again be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + y = x^3 - x.$$

By calculation we find $(b_2, b_4, b_6) = (0, -2, 1)$. The roots of the polynomial are $(e_1, e_2, e_3) \approx (0.837565, 0.269594, -1.107160)$. Again we find that $|A_{100} - B_{100}|$ is smaller than the precision of the computer, and we find that the real period is approximately 2.993458646.

4 Regulators

Let $E/\mathbb{Q}$ be an elliptic curve given by its minimal Weierstraß equation. In order to define the regulator of E, we will recall the definition of the canonical height, as treated in the talk by Van der Horst.

Definition 8 (height)**.** For a point $P = (\frac{a}{e^2}, \frac{b}{e^3}) \in E(\mathbb{Q})$, where $a, b, e \in \mathbb{Z}$ and $\gcd(a, e) = \gcd(b, e) = 1$, we define the *Weil height* of P as $h(P) := \log|e|$. We define the *canonical height* of P as

$$\widetilde{h}(P) := \lim_{n\to\infty} \frac{h(2^n P)}{4^n}.$$

Moreover, we define the *canonical height pairing* as the symmetric bilinear form

$$E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R} : \quad (P, Q) \mapsto \langle P, Q\rangle := \widetilde{h}(P + Q) - \widetilde{h}(P) - \widetilde{h}(Q).$$

Remark 9. It is not obvious that this map is a symmetric bilinear form, but this has been treated in the talk by Van der Horst.

Remark 10. It turns out that the canonical height can be expressed as a sum of local functions, one for each place of $\mathbb{Q}$. For each place, there is a very efficient algorithm to compute the function. These methods are too technical for this talk, but can be found in [Cohe93, p. 403–405].

Now to define the regulator of E, recall that $E(\mathbb{Q}) = E_{\text{tors}}(\mathbb{Q}) \oplus \mathbb{Z}^r$. Let $B_1, \ldots, B_r$ be a basis of the free part of $E(\mathbb{Q})$.

Definition 11 (regulator)**.** The *regulator of* E is defined as

$$\text{Reg}(E) := \det\left(\langle B_i, B_j\rangle\right)_{i,j=1}^{r} \in \mathbb{R}.$$

To calculate the regulator, one needs to calculate generators for the free part of $E(\mathbb{Q})$. In small examples, one can use 2-descent, as it was used for example in [Lugt16]. In general, this problem, which seems to be the overarching theme of this seminar, is not easy to solve. It is certainly not in the scope of this talk to discuss this.

Example 1. Let $E_0/\mathbb{Q}$ again be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + xy + y = x^3 + x^2 - 352x - 2689.$$

In this case it turns out that the rank of E_0 is 0. Hence, the regulator of E_0 equals 1.

Example 2. Let $E_1/\mathbb{Q}$ again be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + y = x^3 - x.$$

In this case it turn out that $E_1(\mathbb{Q}) \cong \mathbb{Z}$, hence the rank of E_1 is 1. Moreover, the point $P = (0, 0)$ is a generator of $E_1(\mathbb{Q})$. We could just calculate $h(2^n \cdot P)/4^n$ for n up to 15 and see that $\widetilde{h}(P)$ is approximately 0.025555704. This, however, takes several minutes. Within less than a second this value can be confirmed using the methods described in remark 10 in Magma. Hence, the regulator is $\mathrm{Reg}(E_1) = \widetilde{h}(2P) - 2\widetilde{h}(P) = 2\widetilde{h}(P) \approx 0.051111408$.

5 Tamagawa numbers

The last invariants occuring in the BSD conjecture are the Tamagawa numbers. In this section I will define them in two ways. We will assume again that E is an elliptic curve over $\mathbb{Q}$ given by a minimal Weierstraß equation. Let p be a prime number.

For the first definition we will use the theory of local fields. Consider $E(\mathbb{Q}_p)$, where $\mathbb{Q}_p$ is the field of p-adics, i.e. the completion of q at p. Each point in $E(\mathbb{Q}_p)$ can be considered projectively as a point $P = (x : y : z)$ with $x, y, z \in \mathbb{Z}_p$ such that not all of x, y and z are divisible by p. Such a point gives rises to a point $\overline{P}$ of the reduction $E_p(\mathbb{F}_p)$. We let $E^0(\mathbb{Q}_p)$ be the subset of points mapping to the smooth locus of $E_p(\mathbb{F}_p)$.

Definition 12 (Tamagawa number)**.** The *Tamagawa number of E at p* is defined as

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

Another more geometric way to define the Tamagawa numbers is by using Néron models. For those who know about it, let $\mathcal{E}$ be a Néron model of E over $\mathbb{Z}_{(p)}$. The special fibre $\mathcal{E}_{\mathbb{F}_p}$ is a smooth commutative group scheme over $\mathbb{F}_p$. Let $\mathcal{E}^0_{\mathbb{F}_p}$ be its identity component. Let $\Phi_{E,p}$ be the quotient group scheme $\mathcal{E}_{\mathbb{F}_p}/\mathcal{E}^0_{\mathbb{F}_p}$.

Lemma 13. *The Tamagawa number of E at p equals $|\Phi_{E,p}(\mathbb{F}_p)|$.*

Remark 14. In most cases it is very easy to calculate the Tamagawa number. We have

$$c_p = \begin{cases} 1 & \text{if } E \text{ has good reduction at } p; \\ \mathrm{ord}_p(\Delta) & \text{if } E \text{ has split multiplicative reduction at } p; \\ 1 & \text{if } E \text{ has non-split mult. reduction at } p \text{ and } \mathrm{ord}_p(\Delta) \text{ is odd;} \\ 2 & \text{if } E \text{ has non-split mult. reduction at } p \text{ and } \mathrm{ord}_p(\Delta) \text{ is even.} \end{cases}$$

In the case that E has additive reduction, it is known that $c_p \leqslant 4$ and it is computable using more sophisticated techniques.

Example 1. Let $E_0/\mathbb{Q}$ again be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + xy + y = x^3 + x^2 - 352x - 2689.$$

The discriminant of this curve is 66, hence the primes of bad reduction are $2, 3$ and 11. For the primes 2, 3 and 11 you can just count the number of solutions to the equation over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_{11}$, not forgetting the point at infinity. We find that there are 2, 5 and 13 points respectively. Hence, the reduction at 2 is split multiplicative and the reduction at 5 and 11 is non-split multiplicative. As all these primes occur with multipliciy 1 in the discriminant, we have $c_p = 1$ for all primes.

Example 2. Let $E_1/\mathbb{Q}$ again be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + y = x^3 - x.$$

The discriminant of this curve is 37. Hence, 37 is the only prime of bad reduction. Over $\mathbb{F}_{37}$ we can write the equation in reduced Weierstraß form by taking $Y = y + \frac{1}{2}$ to get the equation

$$Y^2 = y^2 + y + \tfrac{1}{4} = x^3 - x + \tfrac{1}{4} = x^3 - x + 28.$$

The polynomial $x^3 - x + 28 \in \mathbb{F}_{37}[x]$ factors as $(x+10)(x+32)^2$. As we do not have a triple root, the reduction is multiplicative. To calculate the tangent directions at the node $(5, 0)$ we use the following trick. We take $x = 5 + \varepsilon \in \mathbb{F}_{37}[\varepsilon]/\varepsilon^2$ and we notice that

$$\begin{aligned} Y^2 - (x^3 - x + 28) &= (Y - \sqrt{x+10}(x+32))(Y + \sqrt{x+10}(x+32)) \\ &= (Y - \varepsilon\sqrt{15+\varepsilon})(Y + \varepsilon\sqrt{15+\varepsilon}). \end{aligned}$$

Then we see that the tangent directions at the node are $\pm\sqrt{15}$ and these are not rational as $15 \in \mathbb{F}_{37}$ is not a square. Hence, the reduction is non-split multiplicative and $c_p = 1$ for all primes.

6 Numerical verification

Now we have defined, and calculated for our two example, almost all quantities occurring in the BSD-formula. The ones that remain are $|Ш|$ and $|E(\mathbb{Q})_{\text{tors}}|$. The former is very hard to calculate in general. However, recall from Visse's talk, [Viss16], that we do expect $|Ш|$ to be a square. The torsion subgroup, in the contrary, is not impossible to calculate; one could bound the naive height of rational torsion points and do an extensive search, for example. We will give the results.

Example 1. Let $E_0/\mathbb{Q}$ again be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + xy + y = x^3 + x^2 - 352x - 2689.$$

We found the following invariants.

r	$L_{E_0}(1)$	Ω	$\text{Reg}(E_0/\mathbb{Q})$	$\prod_p c_p$	$\lvert E_0(\mathbb{Q})_{\text{tors}}\rvert$
0	1.10219253	$2 \cdot 0.551096265$	1	1	2

Now, we can calculate

$$\frac{L_{E_0}(1) \cdot |E_0(\mathbb{Q})_{\text{tors}}|^2}{\Omega \cdot \text{Reg}(E_0/\mathbb{Q}) \cdot \prod_p c_p} \approx 4,$$

which suggests that $|Ш| = 4$, which is indeed a square.

Example 2. Let $E_1/\mathbb{Q}$ again be the elliptic curve given by the minimal Weierstraß equation

$$y^2 + y = x^3 - x.$$

We found the following invariants.

r	$L'_{E_1}(1)$	Ω	$\text{Reg}(E_1/\mathbb{Q})$	$\prod_p c_p$	$\lvert E_1(\mathbb{Q})_{\text{tors}}\rvert$
1	0.30599977	$2 \cdot 2.993458646$	0.051111408	1	1

Now, we can calculate

$$\frac{L'_{E_1}(1) \cdot |E_1(\mathbb{Q})_{\text{tors}}|^2}{\Omega \cdot \text{Reg}(E_1/\mathbb{Q}) \cdot \prod_p c_p} \approx 1,$$

which suggests that $|Ш| = 1$, which is indeed a square.

References

[Cohe93] H. Cohen. *A course in computational algebraic number theory.* Springer-Verlag, Berlin, 1993.

[Lugt16] S. van der Lugt. *Selmer groups and Tate-Shafarevich groups.* Previous talk in the seminar on rational points on elliptic curves. Notes available at `http://pub.math.leidenuniv.nl/~lugtsvander/notes/tateshafarevichtalk.pdf`.

[Mart16] C. R. Martindale. *Modularity of Elliptic Curves Defined over the Rationals.* Previous talk in the seminar on rational points on elliptic curves. Notes available at `http://pub.math.leidenuniv.nl/~martindalecr/Modularity.pdf`.

[Tate74] J. Tate. The arithmetic of elliptic curves. *Invent. Math.* **23** (1974), 179–206.

[Shim71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, Princeton, New Jersey, 1971.

[Silv09] J. H. Silverman. *The arithmetic of elliptic curves.* Second edition. Springer, Dordrecht, 2009.

[Viss16] H. D. Visse. *The Cassels-Tate pairing.* Previous talk in the seminar on rational points on elliptic curves. Notes available at `http://pub.math.leidenuniv.nl/~vissehd/documents/notes_Cassels_Tate.pdf`.