The Birch and Swinnerton-Dyer Conjecture

Magnus Ridder Olsen

April 2024

> This remarkable conjecture relates the behaviour of a function L, at a point it is not a present know to be defined, to the order of a group Sha that is not know to be finite.
>
> John Tate on the Birch and Swinnerton-Dyer conjecture

1 Elliptic curves

To probably talk about elliptic curves we need the most basic algebraic geometry. This is introduced in the following, which can easily be skipped. A good reference is [Gat23] or [Har77].

1.1 Crash course in algebraic geometry

Let us fix a field K, an algebraic closure $\overline{K}$ of K and an integer n.

***Definition* 1.1:** *Affine n-space over K* is the set

$$\mathbb{A}^n = \mathbb{A}^n\left(\overline{K}\right) = \{P = (x_1, \dots, x_n) : x_i \in \overline{K}\}.$$

Similarly any algebraic extension L/K the set of *L-rational points of* $\mathbb{A}^n$ is the set

$$\mathbb{A}^n\left(\overline{L}\right) = \{P = (x_1, \dots, x_n) \in \mathbb{A}^n : x_i \in L\}.$$

In other words the set of L-rational points is just the set of points with coordinates in L.

Let $\overline{K}[X]$ be the polynomial ring $K[x_1, \dots, x_n]$. For an ideal I in $\overline{K}[X]$ we set

$$V(I) = \{P \in \mathbb{A}^n \mid f(P) = 0, \forall f \in I\},$$

for vanishing locus of the ideal I.

***Definition* 1.2:** An *affine variety* is any set of the form $V(I)$ for some I.

Notice that we do not require the ideal I to be part of the data of the affine variety. We, however, can always recover an ideal which has the set as vanishing locus.

Proposition 1.3

Let V be an affine variety. Then the set

$$I(V) = \{f \in \overline{K}[X] \mid f(P) = 0, \forall p \in V\},$$

is an ideal in $\overline{K}[X]$ and $V(I(V)) = V$.

Proof. See [Gat23, Proposition 1.10]. □

We call the set $I(V)$ for the ideal of V. Notice that by Hilberts basis theorem $I(V)$ is finitely generated.

***Definition* 1.4:** Let V be an affine variety. We say that V is defined over K if $I(V)$ can be generated by polynomials with coefficients in K and denote this by V/K. If V is defined over K and L/K is an algebraic extension then the set of L-rational points on V is the set

$$V(L) = V \cap \mathbb{A}^n(L)$$

.

In arithmetical geometry one is particarly interested in understanding the sets $V(K)$ for affine varietys V defined over $\mathbb{Q}$ and for number fields K. Having defined affine varietys we are almost in the position to actually work with elliptic curves over arbitrary fields. The only problem is that these affine varietys, lack certain completeness properties. To fix this we will take the projective closure of them.

***Definition* 1.5:** *Projective n-space over K* is the set

$$\mathbb{P}^n = \mathbb{P}^n\left(\overline{K}\right) = \mathbb{A}^{n+1} \setminus \{(0,0,\dots,0)\}/\sim,$$

where the equivalence relation $\sim$ identifies two points $P \sim Q$ if and only if there exists $t \in \overline{K}^*$, such that $tP = Q$. For a point $P = (x_0, x_1 \dots x_n) \in \mathbb{A}^{n+1} \setminus \{(0,0,\dots,0)\}$ we denote its equivalence class in $\mathbb{P}^n$ as $[x_0 : x_1 : \dots : x_n]$.

One should think of $\mathbb{P}^n\left(\overline{K}\right)$ as the set of all lines through the origin in $\mathbb{A}^{n+1}$. Like in the case of affine space it is also possible to define subsets cut out by polynomials. We however need to be careful, as we want the zero sets of these polynomials to be independent of choice of representative of the projective point. This leads us to the following definition.

***Definition* 1.6:** A polynomial $f \in \overline{K}[x_0, \dots x_n]$ is *homogeneous of degree d* if for all $t \in \overline{K}$ and $(x_0, x_1, \dots, x_n) \in \mathbb{A}^n$ we have that

$$f(tx_0, tx_1, \dots, tx_n) = t^d f(x_0, \dots, x_n).$$

An ideal $I \in \overline{K}[x_0, \dots x_n]$ is homogeneous if it can be generated by homogeneous polynomials and is nonzero.

Notice that it makes sense to ask for a point $P \in \mathbb{P}^n$ and a homogeneous polynomial f if $f(p) = 0$. Therefore, we are in a position to define projective varietys

***Definition* 1.7:** Let I be a homogeneous ideal in $\overline{K}[x_0, \dots x_n]$. Then the *projective vanishing locus of I* is the set

$$\overline{V}(I) = \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all } f \in I \text{ homogeneous}\}.$$

A projective variety is a set of the form $V(I)$ for some homogeneous ideal I. If V is a projective variety, the *homogeneous ideal of* V, $I(V)$ is the ideal of $\overline{K}[x_0, \dots x_n]$ defined by the homogeneous polynomials vanishing at V. Such a V is defined over K if the ideal $I(V)$ can be generated by homogeneous polynomials defined over K.

Example 1.8

Let $I = (a_0x_0 + \dots + a_nx_n)$ be the ideal generated by the homogeneous ideal of degree 1, $a_0x_0 + \dots + a_nx_n$ for some $a_0, \dots, a_n \in \overline{K}$ not all zero. We call $\overline{V}(I)$ a hyperplane and furthermore if $n = 2$ we call it a line. One can check that in the case $n = 2$ all lines intersect in precisely one point.

We now want to study how affine space and projective space interact. Notice that for any $0 \leq 1 \leq n$ we have a map

$$\Phi : \mathbb{A}^n \to \mathbb{P}^n,$$

given by

$$(x_1, \dots x_n) \mapsto [x_0 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_n].$$

If we let $H = \overline{V}(x_i) \subset \mathbb{P}^n$ be the hyperplane where $x_i = 0$ and $U_i = \mathbb{P}^n \setminus H_i$ we see that Φ induces a bijection between $\mathbb{A}^n$ and U_i. Indeed an inverse to Φ on U_i is the map given by

$$[x_0 : x_1 : \dots : x_n] \mapsto \left(\frac{x_0}{x_i}, \dots \frac{x_n}{x_i} \right),$$

where we omit the x_i variable.

Having chosen an index i we will canonically identify $\mathbb{A}^n \simeq U_i \subset \mathbb{P}^n$ as a subset of projective space. If V is a projective variety then the set $V \cap \mathbb{A}^n$ as variety. Indeed it is the zero locus of the ideal

$$\{f\left(x_0, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n\right) \mid f \in I(V)\}.$$

Notice that the sets $U_0, \dots, U_n$ cover all of $\mathbb{P}^n$, so to understand a projective variety V it is enough to look at the sets $U_0 \cap V, \dots, U_n \cap V$. We want to reverse this process and get a projective variety from an affine variety that restricts to the given one.

Let $f \in \overline{K}[x_0, \dots, x_{i-1}, x_{i+1} \dots, x_n]$ be a polynomial of degree d. The homogenization of f with respect to the variable x_i is the homogeneous polynomial of degree d

$$\overline{f}\left(x_0, \dots, x_n\right) = x_i^d f\left(\frac{x_0}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots \frac{x_n}{x_i} \right).$$

***Definition* 1.9:** Let V be a affine variety and regard $\mathbb{A}^n \simeq U_i \subset \mathbb{P}^n$. The *projective closure of* V denoted by $\overline{V}$ is the zero locus of the homogeneous ideal I generated by f^* for $f \in I(V)$.

Proposition 1.10 i) If V is an affine variety then $\overline{V}$ is projective variety.

ii) If V is a projective variety then $V \cap \mathbb{A}^n$ is an affine variety and either $V \cap \mathbb{A}^n$ is empty or

$$\overline{V \cap \mathbb{A}^n} = \overline{V}.$$

iii) If a plane algebraic variety V is defined over K if and only if $\overline{V}$ is defined over K.

Proof. See [Har77, Corallary I 2.3]. □

We therefore have a one-one correspondence between affine varieties and projective varieties given by taking the projective closure and restricting to affine n-space. We will in particular be interested in the following kinds of varieties.

***Definition* 1.11:** A affine variety V defined over K is called *plane algebraic curve* if there exists $f \in K[x, y]$, s.t $I(V) = (f)$. We will say V is defined by f or is the zero locus of f. A projective variety V is called a *plane projective curve* if there exists a homogenous polynomial $f \in K[x, y, z]$, st. $\overline{V}\left((f)\right) = V$.

Notice that the projective closure of a plane algebraic curve is a plane projective curve We will impose a single niceness condition on our projective varieties. Namely we will want them to be smooth. The condition is a bit technical so we will only give it in the case of plane projective curves.

***Definition* 1.12:** A plane algebraic curve V defined by f is *smooth at a point* $p \in V$, if the Jacobian of f is nonvanishing. Furthermore a projective plane curve X is called smooth if $U_1 \cap X$, $U_2 \cap X$ and $U_3 \cap X$ are smooth at all their points.

1.2 Definition of elliptic curves

We are now finally in a position to give the definition for elliptic curves over general fields.

***Definition* 1.13:** An *elliptic curve E over a field K* is a projective plane curve homogeneous polynomial $f(x, y) \in K[x, y]$ of third degree with $E(K) \neq \emptyset$.

It turns out one can (projectively) transform the curve to get a simpler equation.

Proposition 1.14

Let E/K be an elliptic curve. Then there exists $a_1, \ldots, a_6 \in K$, s.t. E is given as the (projective) solution set of

$$Y^2X + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

Such a representation is called a Weierstrass equation and we say that E is given by a Weierstrass equation. Furthermore if the characteristic of K is not 2 or 3 there exists $a, b \in K$, s.t E is given as the projective solution set of

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

In this case we say that E is given by a reduced Weierstrass equation.

Proof. See [Sil09, p. III.1]. □

Oftentimes, we will not give the homogenized Weierstrass equation but just give the equation unhomogenized to the x, y variable. Notice that in both cases $\mathbb{P}^2 \setminus (E \cap U_1)$ consists of a single point, namely $[0 : 1 : 0]$. We notate this point as $\mathcal{O}$ and call it the point at infinity of the elliptic curve.

Suppose that E is given by a reduced Weierstrass equation $Y^2Z = X^3 + aXZ^2 + bZ^3$. The condition that E is smooth corresponds to the cubic $x^3 + ax + b$ not having any multiply roots which is equivalent to the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$.

Recall that earlier in this seminar we saw elliptic curves over the complex numbers corresponds to tori ([Dav24, Prop 1 and 2]). This is true over all fields and makes it possible to extend the definition of elliptic functions to be defined over all rings and more generally schemes. To formulate this one has to give the definition of genus of a projective curve, which is quite technical. However, if the field the curve is defined over is a subfield of the complex numbers then the genus is the same as the topological genus of the complex points of the curve. Therefore, the next theorem greatly generalizes the complex case.

Theorem 1.15

The smooth projective curves of genus 1 over a field K with a distinguished point defined over K are precisely elliptic curves.

Proof. For a proof see [CH22, Proposition 15.10]. □

2 Group structure

Let E/K be an elliptic curve. The geometric group structure defined in [Dav24] carries over to the case over a general field. One can explicitly give the addition formula and check that this defines a group on $E(L)$ for every field extension L of K (See [Sil09, p. III.2]). One can also work more geometrically and prove that E is isomorphic to its Jacobian, which naturally carry a group structure.

Theorem 2.1 (Mordell's theorem)
Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ is finitely generated.

All known proofs of this theorem is structured in 2 steps. A cohomological step often called the 'weak' Mordell's theorem and a descent step.

Lemma 2.2 (Weak Mordell's theorem)
If $E/\mathbb{Q}$ is an elliptic curve over $\mathbb{Q}$ and $n > 1$ an integer, then the group

$$E(Q)/nE(Q)$$

is finite.

Proof. For a proof see [HS13, p. C]. □

Proof of Mordell's theorem. By the theory of heights (see [HS13, B.5] or [Sil09, VIII §5]) the Tate-canonical height of an elliptic curve $\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$ is a non-negative quadratic form[1] such that for all $C > 0$ the set

$$\{x \in E(\mathbb{Q}) \mid \hat{h}(x) \leq C\}$$

is finite. The following lemma together with the Weak Mordell's theorem proves Mordell's theorem.

Lemma 2.3 (Descent procedure)
Let Γ be an abelian group equipped with a non-negative quadratic form $q : \Gamma \to \mathbb{R}$, such that for all $N \in \mathbb{N}$, the set

$$\{x \in \Gamma \,|\, q(x) \leq N\}$$

is finite. Assume further that $\Gamma/m\Gamma$ is finite for an integer $m \geq 2$. Then Γ is finitely generated.

Proof. Notice that for $m \in \mathbb{Z}$ and $x \in \Gamma$ that $q(mx) = m^2 q(x)$ and therefore the torsion subgroup is finite, since it is contained in the set of elements $x \in \Gamma$ satisfying $q(x) \leq 0$.

The following sequence is exact by properties of the tensor product

$$\begin{tikzcd} 0 \arrow[r] & \Gamma_{\text{tor}} \arrow[r] & \Gamma \arrow[r] & \Gamma \otimes_{\mathbb{Z}} \mathbb{R}. \end{tikzcd}$$

Therefore it is enough to prove that $\Gamma \otimes_{\mathbb{Z}} \mathbb{R}$ is finitely generated. Indeed since $\mathbb{Z}$ is noetherian the image of Γ under the map $\Gamma \to \Gamma \otimes_{\mathbb{Z}} \mathbb{R}$ is finitely generated and now we get a short exact sequence with the first and last term being finitely generated and therefore the middle term is also finitely generated.

We can therefore promote Γ to a $\mathbb{R}$ vector space equipped with a non-negative quadratic form $q : \Gamma \to \mathbb{R}$ and prove it in this case.

Let $a_1, \dots a_n \in \Gamma$ be a set of representatives for $\Gamma/m\Gamma$. Since $q(x)$ is non-negative, we may define

$$|x| = \sqrt{q(x)}, \quad c = \max\{a_1, \dots, a_n\}, \quad S = \{x \in \Gamma \,|\, |x| \leq c\}.$$

Notice that $|\cdot|$ satisfy the triangle inequality. We will prove that the finite set S generates Γ.

Let $x_0 \in \Gamma$. If $x_0 \in S$ we are done. Otherwise $|x_0| > c$. Let a_i be the representative of the coset of x_0 in $\Gamma/m\Gamma$. Then we may write $x_0 = a_i + mx_1$ for some $x_1 \in \Gamma$ and derive

$$\begin{aligned} m|x_1| &= |x_0 - a_i| \\ &\leq |x_0| + |a_i| \\ &< 2|x_0|. \end{aligned}$$

[1] This means there exists a symmetric bilinear map $b : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{R}$ such that $b(x, x) = \hat{h}(x)$ for all $x \in E(\mathbb{Q})$

Therefore $|x_0| > |x_1|$. If $x_1 \in S$, $x_0 = a_i + mx_1$ is in the subgroup generated by S. If not, we can continue in this fashion and obtain a sequence of elements $|x_0| > |x_1| > |x_2| > ... > |x_n| > \dots$, such that x_0 is in the subgroup generated by S and x_t for every t. Since Γ only contains finitely many elements of bounded size, the sequence eventually terminates with an element in S. And so x_0 lies in the subgroup generated by S as desired. □

□

The structure theorem of finitely generated abelian groups now gives us the following corollary.

Corollary 2.4

There exists an integer r such that

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$$

and furthermore the group $E(\mathbb{Q})_{\text{tor}}$ is finite.

***Definition* 2.5:** Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$. The integer r in corallary 2.4 is called the rank of the elliptic curve.

3 Congruent numbers

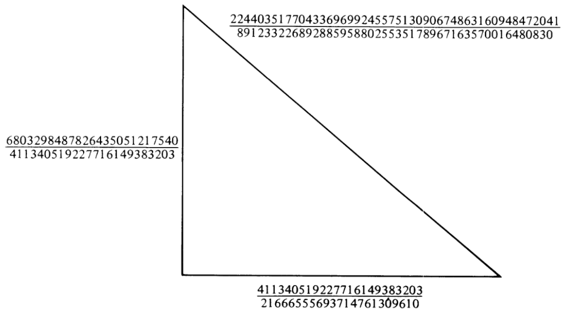
We will now show how this general theory relates to solving the congruent number problem.

***Definition* 3.1:** A natural number n is congruent iff there exits a right triangle with rational sides that has area n.

Notice that if n is congruent then s^2n is congruent for every rational number s, such that s^2n is a natural number, simply by scaling. We are therefore only interested in squarefree congruent numbers. As of now there does not exists an algorithm to determine if a natural number n is congruent.

Example 3.2

The number 157 is congruent since there exists a triangle with the following side lengths.



$\frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}$
$\frac{6803298487826435051217540}{411340519227716149383203}$
$\frac{411340519227716149383203}{21666555693714761309610}$

Furthermore this is the simplest triangle witness 157 as a congruent number in the sense the side lengths has the smallest denominators.

One can easily reframe the condition of n being congruent. Namely a natural number n is congruent if and only if there exists positive rational numbers a, b, c, that solves the following system of equations

$$a^2 + b^2 = c^2 \tag{1}$$

$$ab = 2n. \tag{2}$$

We define E_n to be the projective curve defined by the Weierstrass equation $y^2 = x^3 - n^2x$. Notice that this is an elliptic curve over $\mathbb{Q}$ since the discriminant equals $4n^6$, which is non-zero.

Theorem 3.3

The squarefree number n is congruent if and only if the elliptic curve E_n has rank greater than zero.

To prove this we first need to understand the torsion group if E_n.

Lemma 3.4

The group $(E_n)_{\text{tor}}$ consists of the four points $\mathcal{O}, (0,0)$ and $(\pm n, 0)$ all of order 2.

Proof. For a proof see [Kob93, Proposition 17]. □

Proof of 3.3. We will first prove that if n is congruent then the elliptic curve E_n has rank greater than zero. Suppose that a, b and c are positive rational solutions to the system of equations

$$a^2 + b^2 = c^2 \tag{3}$$
$$ab = 2n. \tag{4}$$

Set $x = \frac{n(a+c)}{b}$ and $y = \frac{2n^2(a+c)}{b^2}$. Then we have that

$$\begin{aligned} y^2 - x^3 + n^2x &= \left(\frac{2n^2(a+c)}{b^2}\right)^2 - \left(\frac{n(a+c)}{b}\right)^3 + n^2\left(\frac{n(a+c)}{b}\right) \\ &= \frac{n^3(a+c)}{b^4}\left(4n(a+c) - b\,(a+c)^2 + b^3\right) \\ &= \frac{n^3(a+c)}{b^4}\left(2ab\,(a+c) - b(a^2+c^2) - 2abc + b^3\right) \\ &= \frac{n^3(a+c)}{b^4}\left(2a^2b + 2abc - b(2a^2+b^2) - 2abc + b^3\right) \\ &= 0 \end{aligned}$$

Therefore the point (x, y) belongs to the elliptic curve E_n. If (x, y) is a torsion point then $\frac{a+c}{b} = 1$ by the positivity of a, b and c and lemma 3.4. Hence we would have that $a + c = b$, but this is clearly absurd as $a^2 + b^2 = c^2$. Therefore (x, y) is a point of infinite order on E_n and hence the rank of E_n is greater than zero.

Suppose now that there exists a point P of infinite order on E_n. As the point has infinite order the point $2P \neq \mathcal{O}$ and hence can be written as $2P = (x, y)$ for some rational numbers x, y. By using the explicit addition law of points on elliptic curves it can be proven that x is the square of a non-zero rational number and hence positive (See [Kob93, Problem 7.2]). We can furthermore assume $y > 0$, since all points with $y = 0$ has order 2. The equation $y^2 = x\left(x^2 - n^2\right)$ gives that $x^2 - n^2 \geq 0$. We can therefore set

$$\begin{aligned} a &= \frac{x^2 - n^2}{y} \\ b &= \frac{2nx}{y} \\ c &= \frac{x^2 + y^2}{y}. \end{aligned}$$

These numbers satisfy that

$$\begin{aligned}
a^2+b^2 &= \left(\frac{x^2-n^2}{y}\right)^2+\left(\frac{2nx}{y}\right)^2\\
&= \frac{1}{y^2}\left((x^2-n^2)^2+(2nx)^2\right)\\
&= \frac{1}{y^2}\left(x^2+y^2\right)^2\\
&= c^2\\
ab &= \frac{x^2-n^2}{y}\frac{2nx}{y}\\
&= 2n\frac{x^3-n^2x}{y^2}\\
&= 2n
\end{aligned}$$

and hence n is congruent as realized by a, b and c. □

We would therefore like to understand the rank of an elliptic curve better. One intuition is that if the rank of an elliptic curve is higher then one would expect more points on the curve. However, if the rank is greater than 1, there is no difference in the cardinality of the set of rational points. One thing we can do is to reduce the curve modulo different primes p and look at how the number of points in $\mathbb{F}_{p^n}$ grow as n grows.

4 Reduction of elliptic curves

Given an elliptic curve $E/\mathbb{Q}$ defined by a Weierstrass equation of the from $y^2 = x^3 + ax + b$ we can make the change of variables $y' = u^{-3}y$ and $x' = u^{-2}x$ and obtain a Weierstrass equation of the form

$$y'^2 = x'^3 + u^4ax' + u^6b$$

still defining the same curve E. By choosing u we can therefore clear denominators and suppose E is given by a Weierstrass equation $y^2 = x^3 + ax + b$ for integers a and b.

***Definition* 4.1:** Let $E/\mathbb{Q}$ be an elliptic defined by a Weierstrass equation $y^2 = x^3 + ax + b$ with a and b integers and a prime p the reduced curve E_p is the projective plane curve given by the projective closure of the zero set of

$$y^2 = x^3 + \overline{a}x + b, ,$$

where $\overline{a}, \overline{b} \in \mathbb{F}_p$ are the residues of a and b.

Notice that E_p is an elliptic curve if and only if $p \neq \Delta$. It turns out one can choose a change of variables such that the reduced curve E_p is smooth for the maximal amount of primes p. For a more precise statement and proof See [Sil09, p. VIII.8.3].

The first formulation of the Birch and Swinnerton-Dyer conjecture is that

$$\prod_{p \text{ prime less than } x} \frac{|E_p(\mathbb{F}_p)|}{p}$$

grows roughly as $\log(x)^r$. Birch and Swinnerton-Dyer conjectured this in 1965 based on numerical evidence.

Already this makes the idea, that the number of points on the reduced elliptic curve is related to the rank, precise. However, the modern day formulation is quite different from this one. To state it, we have to introduce the notion of L-functions of elliptic curves.

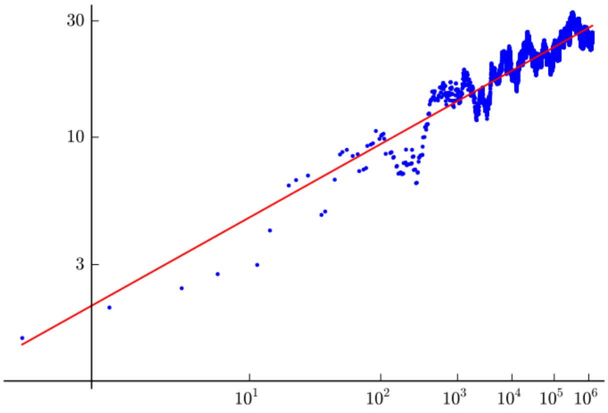


Figure 1: The function $\prod_{p \text{ prime less than } x} \frac{|E_p(\mathbb{F}_p)|}{p}$ in blue for the elliptic curve $y^2 = x^3 - 5x$ drawn on a log(log) to log scale. So the conjecture states that the function should tend to a line with slope 1 drawn in red.

We now want to collect the information of the number of points in $E_p\left(\mathbb{F}_{p^n}\right)$ for all natural numbers n and primes p in a more sophisticated way than above. In general it is a good idea to use a generating function to do this. We will do the same but be as we are doing number theory we will use a ζ-function.

***Definition* 4.2:** Let $E/\mathbb{Q}$ be an elliptic curve. The ζ-function of E is the function

$$\zeta(E, s) = \prod_{p \text{ prime}} \exp\left(\sum_{k=1}^{\infty} \frac{|E_p(\mathbb{F}_{p^k})|}{k} p^{-ks}\right),$$

which is the product of the local ζ-functions:

$$\zeta_p(E_p, s) = \exp\left(\sum_{k=1}^{\infty} \frac{|E_p(\mathbb{F}_{p^k})|}{k} p^{-ks}\right).$$

Later we will discuss convergence properties of this function. It turns out the product converges to an analytic function for $\Re(s) > \frac{3}{2}$.

On the outset this does not look like a normal ζ-function. However the following computation shows the similarities. Namely for $s \in \mathbb{C}$ with $\Re(s) > 1$.

$$\begin{aligned}\prod_{p \text{ prime}} \exp\left(\sum_{k=1}^{\infty} \frac{1}{k} p^{-ks}\right) &= \prod_{p \text{ prime}} \exp\left(\ln\left(\frac{1}{1-p^{-s}}\right)\right) \\ &= \prod_{p \text{ prime}} \frac{1}{1-p^{-s}} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^s} \\ &= \zeta(s).\end{aligned}$$

Likewise more general ζ-functions can be realized the same way. For a fuller discussion see [BD23].

The expected size of $|E_p(\mathbb{F}_{p^k})|$ is $p^k + 1$. It therefore natural to introduce the correction factors $c(p, k) \in \mathbb{Z}$ defined as

$$c(p, k) = |E_p(\mathbb{F}_{p^k})| - \left(p^k + 1\right).$$

Now we can rewrite the ζ-function of the elliptic curve in terms of these factors

$$\begin{aligned}
\zeta(E,s) &= \prod_{p \text{ prime}} \exp\left(\sum_{k=1}^{\infty} \frac{|E_p(\mathbb{F}_{p^k})|}{k} p^{-ks}\right) && (5)\\
&= \prod_{p \text{ prime}} \exp\left(\sum_{k=1}^{\infty} \frac{p^k+1+c(p,k)}{k} p^{-ks}\right) && (6)\\
&= \prod_{p \text{ prime}} \exp\left(\sum_{k=1}^{\infty} \frac{1}{k} p^{-k(s-1)}\right) \exp\left(\sum_{k=1}^{\infty} \frac{1}{k} p^{-ks}\right) \exp\left(\sum_{k=1}^{\infty} \frac{c(p,k)}{k} p^{-ks}\right) && (7)\\
&= \zeta(s-1)\zeta(s) \prod_{p \text{ prime}} \exp\left(\sum_{k=1}^{\infty} \frac{c(p,k)}{k} p^{-ks}\right) && (8)\\
& && (9)
\end{aligned}$$

The interesting factors we will call the local L-functions.

***Definition* 4.3:** Let $E/\mathbb{Q}$ be an elliptic curve and p a prime. The local L-function is defined as

$$L_p\left(E_p, s\right) = \exp\left(\sum_{k=1}^{\infty} \frac{c(p,k)}{k} p^{-ks}\right).$$

It is possible to give a more precise description of these local L-functions depending on 3 cases. We will explain these in the next 3 sections.

4.1 Good reduction

We say the elliptic curve has good reduction at the prime p if the reduced curve is smooth and therefore remains an elliptic curve. Notice that most primes are primes of good reduction since only finitely many primes divide the discriminant. As an example lets look at the elliptic curve $y^2 + y = x^3 + x$ over the finite field $\mathbb{F}_2$. If we look for solutions in $\mathbb{F}_{2^n}$ we get the following table (From [Bae24]):

n	$q = 2^n$	$\lvert E_p(\mathbb{F}_q)\rvert$
1	2	5
2	4	5
3	8	5
4	16	25
5	32	25
6	64	65
7	128	145

It turns out that

$$|E_p(\mathbb{F}_{2^n})| = 2^n + 1 - (-1+i)^n - (-1-i)^n$$

. Weil conjectures implies this is the behaviour for all smooth varieties over finite fields. The case of elliptic curves was proved by Hasse.

Theorem 4.4 (Hasse)

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime of good reduction. Then there exists a complex number α of norm $\sqrt{p}$, such that

$$|E_p(\mathbb{F}_{p^k})| = p^k + 1 - (\alpha^n + \overline{\alpha}^n).$$

Proof. See [Sil09, Theorem V.2.1.3]. □

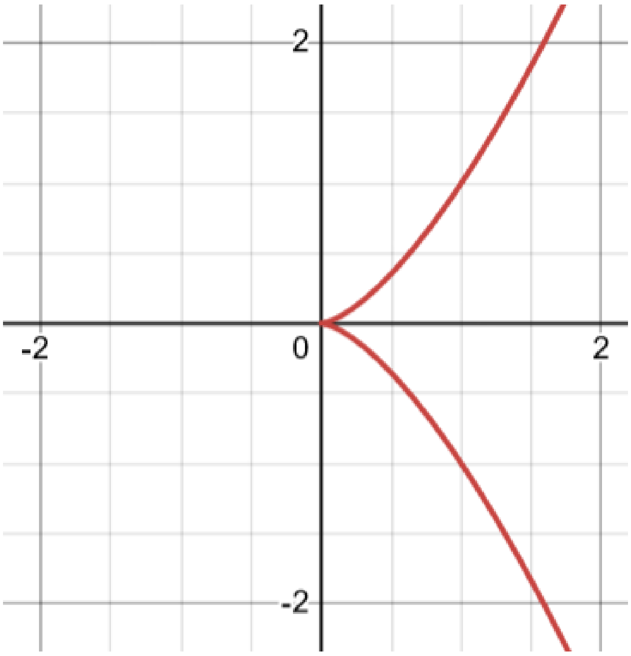
This implies that the correction factor $c(p,k) = -\alpha^k - \overline{\alpha}^k$. Therefore the local L-function is given as

$$\begin{aligned}
L_p(E_p, s) &= \exp\left(\sum_{k=1}^{\infty} \frac{c(p,k)}{k} p^{-ks}\right) \\
&= \exp\left(-\sum_{k=1}^{\infty} \frac{\alpha^k + \overline{\alpha}^k}{k} p^{-ks}\right) \\
&= \exp\left(-\sum_{k=1}^{\infty} \frac{\alpha^k}{k} p^{-ks}\right) \exp\left(-\sum_{k=1}^{\infty} \frac{\overline{\alpha}^k}{k} p^{-ks}\right) \\
&= \exp\left(\ln\left(1 - \alpha p^{s}\right)\right) \exp\left(\ln\left(1 - \overline{\alpha} p^{s}\right)\right) \\
&= \left(1 - \alpha p^{-s}\right)\left(1 - \overline{\alpha} p^{-s}\right) \\
&= 1 - \left(\alpha + \overline{\alpha} p^{-s} + p^{1-2s}\right) \\
&= 1 - a_p p^{-s} + p^{1-2s},
\end{aligned}$$

where $a_p = \alpha + \overline{\alpha} = -c(p,1) = p + 1 - |E_p(\mathbb{F}_p)|$.

4.2 Additive reduction

An elliptic curve has additive reduction at a prime p, if the reduced curve has a cusp.



More precisely this means, that if the elliptic curve is given by a Weierstrass equation of the form $y^2 = x^3 + ax^2 + b$, it has additive reduction modulo p if and only if $p|a$ and $p|b$. Notice that implies that the reduced curve is not smooth.

For example the elliptic curve given by the Weierstrass equation $y^2 = x^3 + 2x$ has additive reduction modulo 2.

n	$q = 2^n$	$\lvert E_p(\mathbb{F}_q)\rvert$
1	2	5
2	4	5
3	8	5
4	16	25
5	32	25
6	64	65
7	128	145

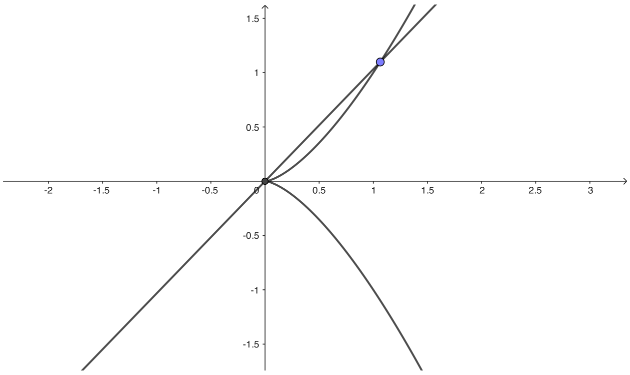
Here the system is quite clear and it holds more generally.

Theorem 4.5

Let $E/\mathbb{Q}$ be an elliptic curve with additive reduction modulo a prime p. Then

$$|E_p(\mathbb{F}_{p^n})| = p^n + 1,$$

for all integers n.



Proof sketch. Let $P = (0,0) \in E_p$ be the cusp of the elliptic curve. A $\mathbb{F}_{p^n}$ rational line through P in $\mathbb{P}^2(\mathbb{F}_{p^n})$, that is not the line $y = 0$ intersects $E_p(\mathbb{F}_{p^n})$, in exactly one other point, as it has multiplicity 2 at P. This therefore establishes a bijection between $\mathbb{P}^2(\mathbb{F}_{p^n}) \setminus \{[0,1,0]\}$ and $E_p(\mathbb{F}_{p^n}) \setminus \{P\}$ and therefore $|E_p(\mathbb{F}_{p^n})| = p^n + 1$.

For another proof see [Sil09, Exercise 3.5], where it is also established that $E_p(\mathbb{F}_{p^n}) \setminus \{P\}$ is isomorphic as a group to the additive group of $\mathbb{F}_{p^n}$, which explains the name of additive reduction. □

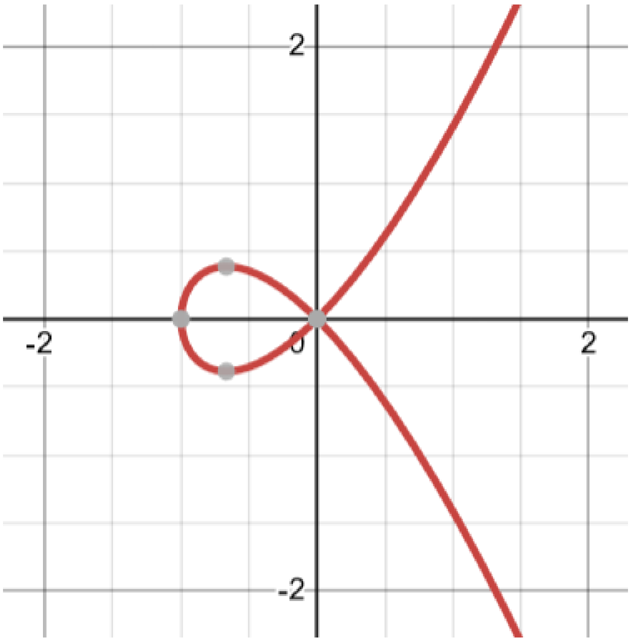
Therefore we have that the correction factor in the case of additive reduction is $c(p,k) = 0$ and therefore $L_p(s) = \exp(0) = 1$ in this case.

4.3 Multiplicative reduction

An elliptic curve has multiplicative reduction at a prime p, if the reduced curve has a node.

More precisely we say an elliptic curve has multiplicative reduction at a prime p if it does not have smooth or additive reduction modulo p. It can be shown that this exactly implies that it is has a node. Indeed if the elliptic curve is given by a Weierstrass equation of the form $y^2 = x^3 + ax + b$, it is true that it has good or additive reduction at p if and only if the cubic $x^3 + ax + b$ has 3 or 1 root modulo p respectively. Therefore having multiplicative reduction implies that the cubic $x^3 + ax + b$ has a double root and this is exactly the node of the elliptic curve. At the node it can be proven there is two tangents. These exists as lines in $\mathbb{P}^2\left(\overline{\mathbb{F}_p}\right)$. Let them be denoted l_1 and l_2.

We will distinuges between two cases based on the slope of these lines. Namely we say the elliptic curve has split multiplicative reduction modulo p if the slope of l_1 is in $\mathbb{F}_p$, and non-split otherwise.



Theorem 4.6

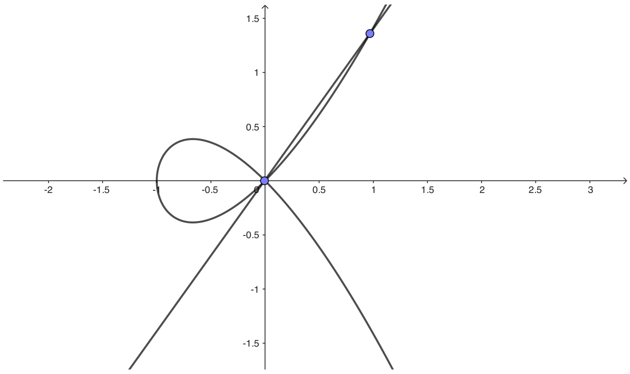
Let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction modulo a prime p. Then

$$|E_p(\mathbb{F}_{p^n})| = p^n,$$

for all integers n, and if it has non-split multiplicative reduction then

$$|E_p(\mathbb{F}_{p^n})| = p^n + 1 - (-1)^n \,,$$

for all integers n.



Proof sketch. Let $P \in E_p$ be the node of the elliptic curve and suppose we have split multiplicative reduction. A $\mathbb{F}_{p^n}$ rational line that isn't l_1 or l_2, through P in $\mathbb{P}^2\left(\mathbb{F}_{p^n}\right)$, intersects $E_p\left(\mathbb{F}_{p^n}\right)$, in exactly one other point, as it has multiplicity 2 at P. This therefore establishes a bijection between $\mathbb{P}^2\left(\mathbb{F}_{p^n}\right) \setminus \{l_1, l_2\}$ and $E_p\left(\mathbb{F}_{p^n}\right) \setminus \{P\}$ and therefore $|E_p(\mathbb{F}_{p^n})| = p^n$ in the case of split multiplicative reduction.

The case of non-split multiplicative reduction is harder to visualize geometrically. For a proof see [Sil09, Exercise 3.5] where it is also proven that $E_p(\overline{\mathbb{F}_p}) \setminus \{P\}$ is isomorphic to the multiplicative group of $\overline{\mathbb{F}_p}$ in both cases, which explains the name of multiplicative reduction. □

In the case of split multiplicative reduction we have the correction factor $c(p, k) = -1$ and therefore in this case the local L-function is given as

$$\begin{aligned} L_p(E_p, s) &= \exp\left(\sum_{k=1}^{\infty} \frac{c(p,k)}{k} p^{-ks}\right) \\ &= \exp\left(\sum_{k=1}^{\infty} \frac{-1}{k} p^{-ks}\right) \\ &= \exp\left(\ln\left(1 - p^{-s}\right)\right) \\ &= 1 - p^{-s} \end{aligned}$$

Likewise we have in the case of non-split multiplicative reduction the correction factor $c(p,k) = -(-1)^k$ and therefore in this case the local L-function is given as

$$\begin{aligned} L_p(E_p, s) &= \exp\left(\sum_{k=1}^{\infty} \frac{c(p,k)}{k} p^{-ks}\right) \\ &= \exp\left(\sum_{k=1}^{\infty} \frac{-(-1)^k}{k} p^{-ks}\right) \\ &= \exp\left(\ln\left(1 - (-1)p^{-s}\right)\right) \\ &= 1 + p^{-s} \end{aligned}$$

Notice that if we set $a_p = p + 1 - |E_p(\mathbb{F}_p)|$ like in the case of good reduction we in both cases have a local L-function of the form

$$L_p(s) = 1 - a_p p^{-s}.$$

All in all we have that the local L-functions is given by the following.

Theorem 4.7

Let $E/\mathbb{Q}$ be an elliptic curve. Then

$$L_p(E_p, s) = \begin{cases} 1 - a_p p^{-s} + p^{1-2s} & \text{if the elliptic curve has good reduction at } p \\ 1 - a_p p^{-s} & \text{if the elliptic curve has multiplicative reduction at } p\ . \\ 1 & \text{if the elliptic curve has additive reduction at } p \end{cases}$$

Proof. See discussion above. □

5 L-functions of elliptic curves

Now we have gathered local information at all primes we want to collect it into global information. As a number theorist does best we multiply the local information to get global information.

Proposition 5.1

Let $E/\mathbb{Q}$ be an elliptic curve. The infinite product

$$L(E, s) := \prod_{p \text{ prime}} L_p\left(E_p, s\right)^{-1},$$

converges absolutely to an analytic function for $s \in \mathbb{C}$, with $\Re(s) > \frac{3}{2}$. This function is called the L-function of the elliptic curve.

Proof. Notice that by theorem 4.7 we can write the L-function as

$$\begin{aligned} L(E,s) &= \prod_{p|\Delta} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1-a_p p^{-s}+p^{1-2s}} \\ &= \prod_{p|\Delta} \frac{1}{1-a_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1-\alpha_p p^{-s}} \frac{1}{1-\overline{\alpha_p} p^{-s}}, \end{aligned}$$

where α_p are the complex numbers of norm $\sqrt{p}$ from theorem 4.4. It is therefore enough to prove that the product

$$\prod_{p\nmid\Delta} \frac{1}{1-b_p p^{-s}}.$$

converges for positive real numbers b_p s.t $b_p \leq \sqrt{p}$ and $s \in \mathbb{R}$, s.t $s > \frac{3}{2}$. For a natural number n with prime factorization $n = p_1^{e_1} \dots p_k^{e_k}$, define

$$b_n = b_{p_1}^{e_1} \dots b_{p_k}^{e_k},$$

and notice that $b_n \leq \sqrt{n}$. We therefore have that for all natural numbers N, that

$$\begin{aligned} \prod_{p\nmid\Delta, p\leq N} \frac{1}{1-b_p p^{-s}} &\leq \prod_{p \text{ prime}\leq N} \frac{1}{1-b_p p^{-s}} \\ &\leq \sum_{k=1}^{\infty} \frac{b_n}{n^{-s}} \\ &\leq \sum_{k=1}^{\infty} \frac{\sqrt{n}}{n^{-s}} \\ &= \sum_{k=1}^{\infty} \frac{1}{n^{-(s-\frac{1}{2})}}, \end{aligned}$$

Since $s - \frac{1}{2} > 1$ the last term is finite by convergence of the Riemann ζ-function and we therefore have that the product converges absolutely. □

Theorem 5.2

Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists a functional equation relating s and $2-s$, that makes it possible to analytically continue the L-function of E to a meromorphic function on the whole complex plane.

This theorem is due to Eichler and Shimura that proved it for modular elliptic curves. Later Wiles and others showed that all elliptic curves were modular.

Now after all this work we are finally in a position to state the Birch and Swinnerton-Dyer conjecture. This precisely formulates the idea that the L-function should contain information about the rank of the elliptic curve. A modern day formulation is the following.

Conjecture (Birch and Swinnerton-Dyer)

Let $E/\mathbb{Q}$ be an elliptic curve. Then the order of vanishing of the $L(E,s)$ at $s=1$ is equal to the rank of the elliptic curve.

It is furthermore refined to also give a precise shape of the first non-zero Taylor coefficient for $L(E,s)$ at $s=1$.

Conjecture (Refined Birch and Swinnerton-Dyer)

Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$ of rank r. Then the L-function of the elliptic curve have a zero of order r at $s = 1$. Furthermore the r'th Taylor coefficient of the L-function is given by

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\#\operatorname{Sha}(E)\Omega_E R_E \prod_{p|N} c_p}{(\# E_{\text{tor}})^2}.$$

Results of Gross-Zagier (1986) and Kolyvagin (1989) has proved the following cases of the conjecture.

$$\begin{aligned} L(E,1) \neq 0 &\implies \text{rank of } E \text{ is } 0. \\ L(E,1) = 0 \text{ and } L'(E,1) \neq 0 &\implies \text{rank of } E \text{ is } 1. \end{aligned}$$

5.1 Importance for congruent number problem

The importance of the Birch and Swinnerton-Dyer conjecture can not be overstated. For example Tunnel managed to closely examine the L-function of the elliptic curves E_n to prove the following remarkable theorem.

Theorem 5.3 (Tunnel 1983)

Let n be a square-free natural number. Consider the following values

$$\begin{aligned} A_n &:= \#\{(x,y,z) \in \mathbb{Z}^3 \,|\, n = 2x^2 + y^2 + 32z^2\} \\ B_n &:= \#\{(x,y,z) \in \mathbb{Z}^3 \,|\, n = 2x^2 + y^2 + 8z^2\} \\ C_n &:= \#\{(x,y,z) \in \mathbb{Z}^3 \,|\, n = 2x^2 + y^2 + 64z^2\} \\ D_n &:= \#\{(x,y,z) \in \mathbb{Z}^3 \,|\, n = 2x^2 + y^2 + 16z^2\} \end{aligned}$$

1. If n is an odd congruent number, then $2A_n = B_n$.
2. If n is an even congruent number, then $2C_n = D_n$.

Moreover if the Birch-Swinnerton and Dyer conjecture is true then these are sufficient.

This is significant as it gives an efficient algorithm to check whether a given number n is congruent. Therefore, a proof of the Birch and Swinnerton-Dyer conjecture would give a satisfactory solution to the congruent number problem.

References

[Har77] Robin Hartshorne. *Algebraic Geometry*. Vol. 52. Graduate Texts in Mathematics. Springer, 1977.

[Kob93] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Graduate Texts in Mathematics. Springer New York, 1993. ISBN: 9780387979663. URL: `https://books.google.ch/books?id=99v9Xc0jh04C`.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer New York, 2009. ISBN: 9780387094946.

[HS13] M. Hindry and J.H. Silverman. *Diophantine Geometry: An Introduction*. Graduate Texts in Mathematics. Springer New York, 2013. ISBN: 9781461212102.

[CH22] Dustin Clausen and Lars Hesselholt. *Scheme Theory*. `https://www.math.nagoya-u.ac.jp/~larsh/teaching/S2022_A/schemes.pdf`. 2022.

[BD23] John Baez and James Dolan. "Dirichlet species and the Hasse-Weil zeta function". https://ncatlab.org/johnbaez/show/Dirichlet+species+and+the+Hasse-Weil+zeta+function. 2023.

[Gat23] Andreas Gathmann. *Algebraic Geometry*. https://agag-gathmann.math.rptu.de/de/alggeom.php. [Online; accessed 2-May-2024]. 2023.

[Bae24] John Baez. *Counting Points on Elliptic Curves (Part 2)*. 2024. URL: https://golem.ph.utexas.edu/category/2024/03/counting_points_on_elliptic_cu_1.html (visited on 01/06/2024).

[Dav24] Emil Staikov David Blättler. *Complex elliptic curves*. https://people.math.ethz.ch/~mschwagen/ellipticfunctionsmodularforms2024/talks.pdf. [Online; accessed 2-May-2024]. 2024.