What is. . . an L-function?

Peter Bruin, Universität Zürich
Zurich Graduate Colloquium, 30 October 2012

1. Introduction

1.1. The Riemann ζ-function

The prototypical example of an L-function is Riemann's ζ-function

$$\zeta(s) = \sum_{n\ge 1} n^{-s} \quad (\Re s > 1). \tag{1.1}$$

By an easy argument using the fact that every $n \ge 1$ has a unique prime factorisation, one shows that $\zeta(s)$ can be written as an *Euler product*

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1} \quad (\Re s > 1).$$

This shows that $\zeta(s)$ does not have any zeroes in the region $\Re s > 1$.

We define the *completed ζ-function* by

$$\mathrm{Z}(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s).$$

Here we have used the Γ-function

$$\Gamma(s) = \int_0^\infty \exp(-t) t^s \frac{dt}{t} \quad (\Re s > 0). \tag{1.2}$$

Since $\pi^{-s/2}$ is an nowhere-vanishing entire function and $\Gamma(s)$ is a nowhere-vanishing meromorphic function with poles at the non-positive integers and no other poles, $\mathrm{Z}(s)$ is a nowhere-vanishing holomorphic function on the region $\Re s > 1$.

Remark. We recall that the set of *places* of $\mathbf{Q}$ is the set of non-trivial absolute values on $\mathbf{Q}$ up to equivalence. By Ostrowski's theorem, this set consists of the *finite places*, corresponding to the p-adic absolute values $|\ |_p$ for prime numbers p, and one *infinite place*, corresponding to the usual absolute value $|\ |_\infty$ on $\mathbf{Q}$. The standard ζ-function can be viewed a product over the finite places of $\mathbf{Q}$, while the completed ζ-function $\mathrm{Z}(s)$ is a product over all places, the factor $\pi^{-s/2}\Gamma(s/2)$ being the analogue at the infinite place of the factors $(1 - p^{-s})^{-1}$ at the finite places.

Theorem 1.1 (Riemann [7]). *The function $\mathrm{Z}(s)$ can be continued to a meromorphic function on the whole complex plane with a simple pole at $s = 1$ with residue 1, a simple pole at $s = 0$ with residue -1, and no other poles. It satisfies the functional equation*

$$\mathrm{Z}(s) = \mathrm{Z}(1 - s).$$

Proof. The idea of the proof is as follows: we express $\mathrm{Z}(s)$ as the *Mellin transform* (a certain integral transform, in fact a variant of the Fourier transform) of a *modular form.* Modular forms are functions living on the complex upper half-plane enjoying certain transformation properties, which will lead to the meromorphic continuation and the functional equation.

The modular form we need is *Jacobi's ϑ-function*, which is defined for $\tau \in \mathbf{C}$ with $\Im\tau > 0$ by

$$\begin{aligned}\vartheta(\tau) &= \sum_{n\in\mathbf{Z}} \exp(\pi i n^2 \tau) \\ &= 1 + 2\sum_{n\ge 1} \exp(\pi i n^2 \tau).\end{aligned} \tag{1.3}$$

Using the *Poisson summation formula*, one can prove that $\vartheta(s)$ satisfies the functional equation

$$\vartheta\left(-\frac{1}{\tau}\right) = \sqrt{\frac{\tau}{i}}\vartheta(\tau). \tag{1.4}$$

We now consider the Mellin transform of ϑ, defined as

$$\tilde{\vartheta}(s) = \int_{t=0}^{\infty} (\vartheta(it) - 1) t^s \frac{dt}{t} \quad (\Re s > 1/2).$$

We compute $\tilde{\vartheta}(s)$ as follows, using (1.1), (1.3) and (1.2):

$$\begin{aligned}\tilde{\vartheta}(s) &= 2 \sum_{n\ge 1} \int_{t=0}^{\infty} \exp(-\pi n^2 t) t^s \frac{dt}{t} \\ &= 2 \sum_{n\ge 1} (\pi n^2)^{-s} \int_{u=0}^{\infty} \exp(-u) u^s \frac{du}{u} \\ &= 2\pi^{-s}\Gamma(s)\zeta(2s).\end{aligned}$$

From this we get the following equation, due to Riemann:

$$\mathrm{Z}(s) = \frac{1}{2}\tilde{\vartheta}(s/2).$$

On the other hand, we can rewrite $\tilde{\vartheta}(s)$ as follows. Splitting the integral occurring in the definition of $\tilde{\vartheta}(s)$, we obtain, for $\Re s > 1/2$,

$$\tilde{\vartheta}(s) = \int_{t=0}^{1} (\vartheta(it) - 1) t^s \frac{dt}{t} + \int_{t=1}^{\infty} (\vartheta(it) - 1) t^s \frac{dt}{t}.$$

Using (1.4) and the change of variables $t = 1/u$, we rewrite the first integral as

$$\begin{aligned}\int_{t=0}^{1} (\vartheta(it) - 1) t^s \frac{dt}{t} &= \int_{u=1}^{\infty} (u^{1/2}\vartheta(iu) - 1) u^{-s} \frac{du}{u} \\ &= \int_{u=1}^{\infty} \vartheta(iu) u^{1/2-s} \frac{du}{u} - \int_{u=1}^{\infty} u^{-s} \frac{du}{u} \\ &= \int_{u=1}^{\infty} (\vartheta(iu) - 1) u^{1/2-s} \frac{du}{u} + \int_{u=1}^{\infty} u^{1/2-s} \frac{du}{u} - \int_{u=1}^{\infty} u^{-s} \frac{du}{u} \\ &= \int_{u=1}^{\infty} (\vartheta(iu) - 1) u^{1/2-s} \frac{du}{u} + \frac{1}{s-1/2} - \frac{1}{s}.\end{aligned}$$

From this we get

$$\tilde{\theta}(s) = \frac{1}{s-1/2} - \frac{1}{s} + \int_{t=1}^{\infty} (\vartheta(it) - 1)(t^{1/2-s} + t^s) \frac{dt}{t}.$$

This can be rewritten as

$$\mathrm{Z}(s) = \frac{1}{s-1} - \frac{1}{s} + \frac{1}{2} \int_{t=1}^{\infty} (\vartheta(it) - 1)(t^{(1-s)/2} + t^{s/2}) \frac{dt}{t}. \tag{1.5}$$

The integral converges for all $s \in \mathbf{C}$, so this formula gives the meromorphic continuation of $\mathrm{Z}(s)$. Furthermore, the right-hand side of (1.5) is clearly invariant under $s \leftrightarrow 1-s$, which proves the functional equation. □

Using the functional equation, one can show that $\zeta(s) = 0$ if s is a negative even integer. An $s \in \mathbf{C}$ with $\zeta(s) = 0$ and s not a negative integer is called a *non-trivial zero* of $\zeta(s)$. The non-trivial zeroes of $\zeta(s)$ are precisely the zeroes of $\mathrm{Z}(s)$. The functional equation implies that these all lie in the *critical strip* $\{s \in \mathbf{C} \mid 0 \le \Re s \le 1\}$.

Conjecture 1.2 (Riemann hypothesis [7]). *All non-trivial zeroes of $\zeta(s)$ lie on the line $\Re s = 1/2$.*

The Riemann hypothesis is equivalent to the error term in the prime number theorem

$$\#\{\text{prime numbers} \le x\} = \int_2^x \frac{dt}{\log t} + \text{error term}$$

being as sharp as possible, namely, $O(\sqrt{x}\log x)$ as $x \to \infty$.

1.2. Special values

The *Bernoulli numbers* B_k for $k \geq 0$ are rational numbers defined by

$$\sum_{k=0}^{\infty} B_k \frac{t^k}{k!} = \frac{t}{\exp(t) - 1}.$$

We have $B_k = 0$ for $k \geq 3$ odd, and

$$\begin{gathered} B_0 = 1, \quad B_1 = -1/2, \quad B_2 = 1/6, \quad B_4 = -1/30, \\ B_6 = 1/42, \quad B_8 = -1/30, \quad B_{10} = 5/66, \quad B_{12} = -691/2730. \end{gathered}$$

Theorem 1.3 (Euler). *The values of the ζ-function at even positive integers are given by the formula*

$$\zeta(2m) = (-1)^{m-1} \frac{(2\pi)^{2m}}{2(2m)!} B_{2m} \quad (m \geq 1). \tag{1.6}$$

The first few examples are

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945}, \quad \zeta(8) = \frac{\pi^8}{9450},$$

the first of which is Euler's solution to the "Basel problem" of determining $\sum_{n\geq 1} n^{-2}$.

The functional equation translates (1.6) into a formula for the ζ-function at odd negative integers:

$$\zeta(1 - 2m) = -\frac{B_{2m}}{2m} \quad (m \geq 1).$$

1.3. More general L-functions

I will not give a general definition of L-functions. The reason is that an L-function is usually thought of as being "attached to something". Let us denote this "something" by X for the moment; this X can for example be a number field, a Dirichlet character, an elliptic curve, a modular form, an automorphic representation, or even a "motive".

The one thing that they all have in common is a *Dirichlet series* expansion

$$L(X, s) = \sum_{n\geq 1} a_n n^{-s}, \tag{1.7}$$

where s is a complex variable and the a_n are complex numbers determined by X and growing at most polynomially as $n \to \infty$. This growth condition implies that for some $c > 0$, the above series converges for $\Re s > c$ and defines $L(X, s)$ as a holomorphic function in the right half-plane $\{s \in \mathbf{C} \mid \Re s > c\}$.

Here are some nice properties that we would like L-functions to have (but which are often not known to hold).

- *Euler product.* If $a_{mn} = a_m a_n$ whenever m and n are coprime, and moreover the a_{p^r} for p prime and $r \geq 1$ satisfy a suitable recurrence relation, then we can write

  $$L(X, s) = \prod_{p \text{ prime}} \frac{1}{F_p(p^{-s})},$$

  where $F_p \in \mathbf{C}[t]$ is a polynomial of the form $1 - a_p t + \cdots$.
- *Analytic continuation.* We say that an L-series of the form (1.7) has an *analytic continuation* if there exists a meromorphic function on the whole complex plane that coincides with the given series in its domain of convergence.
- *Functional equation.* In many cases, one can define a *dual object* X^*, a completed L-function $\Lambda(X, s)$ which is a "simple" modification of the original $L(X, s)$ (the product of $L(X, s)$ with

certain exponentials and Γ-functions), an integer k and a complex number $\epsilon(X)$ such that (assuming analytic continuation)

$$\Lambda(X, s) = \epsilon(X)\Lambda(X^*, k - s).$$

In the case where $L(X, s)$ admits (or is expected to admit) such a functional equation, the vertical line $\{s \in \mathbf{C} \mid \Re s = k/2\}$ is called the *critical line*.

- *Riemann hypothesis*. For "most" L-functions, one expects that all the zeroes of the meromorphic function $L(X, s)$, except the well-understood *trivial zeroes*, lie on the critical line. There is a lot of numerical data supporting the Riemann hypothesis, as well as other heuristic reasons to believe it. Unfortunately, it hasn't been proved even for the simplest L-function, the Riemann ζ-function. (The analogue of the Riemann hypothesis was proved by Deligne in the setting of ζ-functions of algebraic varieties over finite fields; so far, a proof for the ζ-function of anything defined over a number field does not seem to be in sight.)
- *Special values*. There are many results and conjectures concerning values of L-functions at the integers. The prototypical example is Euler's formula (1.6).

There are essentially two ways of constructing L-functions:

(1) from *number theory and arithmetic geometry*;

(2) from *automorphic forms and automorphic representations*.

We call L-functions arising in this way *arithmetic* or *automorphic*, respectively. In many cases, arithmetic L-functions can be shown to be automorphic. This is useful because an L-function defined by a Dirichlet series (1.7) is a priori only defined on some right half-plane, and only for automorphic L-functions do we know how to construct the analytic continuation.

It is hoped that every 'nice' arithmetic L-function is also an automorphic L-function. However, this is in general very hard to prove. A very general and still largely conjectural framework describing how different L-functions should be related to each other and to other objects is the *Langlands program*; see [4] for an introduction.

2. Examples of L-functions

2.1. Dirichlet L-functions

One could say that Dirichlet's famous article [6] on prime numbers in arithmetic progressions marked the beginning of analytic number theory. Dirichlet did not consider L-series as meromorphic functions, but merely as functions of a real variable.

In modern language, Dirichlet L-series are constructed as follows. One takes a positive integer m and a group homomorphism

$$\chi\colon (\mathbf{Z}/m\mathbf{Z})^\times \to \mathbf{C}^\times.$$

One extends this to a function $\chi\colon \mathbf{Z} \to \mathbf{C}$ by putting $\chi(a) = 0$ if a is not coprime to m. One then puts

$$\begin{aligned} L(\chi, s) &= \sum_{n=1}^{\infty} \chi(n) n^{-s} \\ &= \prod_{p \nmid m \text{ prime}} (1 - \chi(p)p^{-s})^{-1}. \end{aligned}$$

Theorem 2.1 (Dirichlet [6]). *Let m be a positive integer, and let $a \in (\mathbf{Z}/m\mathbf{Z})^\times$. Then there are infinitely many prime numbers p such that $p \bmod m = a$.*

Dirichlet's proof of this goes via L-functions. The central fact about L-functions that is needed is that if χ as above is non-trivial, then $L(\chi, 1)$ is finite and non-zero.

2.2. The Dedekind ζ-function of a number field

The Dedekind ζ-function is a generalisation of the Riemann ζ-function to an arbitrary number field K (the Riemann ζ-function being the case $K = \mathbf{Q}$). It is defined by

$$\begin{aligned}\zeta_K(s) &= \prod_{\mathfrak{p}\subset \mathbf{Z}_K} (1 - (\mathrm{N}\mathfrak{p})^{-s})^{-1} \\ &= \sum_{\mathfrak{a}\subseteq \mathbf{Z}_K} (\mathrm{N}\mathfrak{a})^{-s}.\end{aligned}$$

Here $\mathbf{Z}_K$ is the ring of integers of K, $\mathfrak{p}$ runs over all non-zero prime ideals of $\mathbf{Z}_K$, and $\mathfrak{a}$ runs over all non-zero ideals of $\mathbf{Z}_K$.

Let $\Delta_K \in \mathbf{Z}$ be the discriminant of K, and let r_1 and r_2 denote the number of real and complex places of K, respectively. Then the completed ζ-function

$$\mathrm{Z}_K(s) = |\Delta_K|^{s/2}\bigl(\pi^{-s/2}\Gamma(s/2)\bigr)^{r_1}\bigl((2\pi)^{1-s}\Gamma(s)\bigr)^{r_2}\zeta_K(s)$$

satisfies

$$\mathrm{Z}_K(s) = \mathrm{Z}_K(1-s).$$

Theorem 2.2 (class number formula). *Let K be a number field. In addition to the above notation, let h_K denote the class number, R_K the regulator, and w_K the number of roots of unity in K. Then $\zeta_K(s)$ has a simple pole in $s = 1$ with residue*

$$\operatorname*{Res}_{s=1}\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2}h_K R_K}{|\Delta_K|^{1/2}w_K}.$$

Remark. By the functional equation, this is equivalent to

$$\lim_{s\to 0}\frac{\zeta_K(s)}{s^{r_1+r_2-1}} = -\frac{h_K R_K}{w_K}.$$

2.3. L-functions attached to modular forms

We consider the complex upper half-plane

$$\mathbf{H} = \{x+iy \in \mathbf{C} \mid x \in \mathbf{R}, y > 0\}$$

and the group

$$\mathrm{SL}_2(\mathbf{Z}) = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} \,\middle|\, a,b,c,d \in \mathbf{R}, ad-bc = 1\right\}.$$

We recall that $\mathrm{SL}_2(\mathbf{Z})$ acts on $\mathbf{H}$ by $\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)z = \frac{az+b}{cz+d}$.

Let n and k be positive integers. We write $\Gamma_1(n)$ for the subgroup of $\mathrm{SL}_2(\mathbf{Z})$ defined by

$$\Gamma_1(n) = \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \,\middle|\, \begin{aligned} a \equiv d \equiv 1 &\pmod n\\ c \equiv 0 &\pmod n\end{aligned}\right\}.$$

A *modular form* of weight k and level n is a holomorphic function f on the upper half-plane satisfying the transformation rule

$$f(\gamma z) = (cz+d)^k f(z) \quad \text{for all } \gamma = \begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \Gamma_1(n), z \in \mathbf{H}$$

and a certain growth condition which we will not explain. The definition implies that every modular form f can be written as

$$f(z) = \sum_{m\ge 0} a_m(f)q^m \quad \text{with } q = \exp(2\pi i z)$$

for certain complex numbers $a_m(f)$.

The *L-function* of a modular form f as above is defined by the Dirichlet series

$$L(f,s) = \sum_{m\geq 1} a_m(f)m^{-s}.$$

As before, one can define a completed L-function $\Lambda(f,s)$ by multiplying $L(f,s)$ by certain elementary factors. A very important property of L-functions of modular forms is that one can express $\Lambda(f,s)$ as the Mellin transform of f:

$$\Lambda(f,s) = \int_0^\infty (f(iy) - a_0(f))y^s \frac{dy}{y}.$$

For certain f (so-called *primitive cusp forms*, which in particular satisfy $a_0(f) = 0$ and $a_1(f) = 1$), the L-function $\Lambda(f,s)$ can be analytically continued to an entire function satisfying a certain functional equation linking f with a "dual" form $\bar{f}$ satisfying $\bar{f}(z) = \sum_{m\geq 1} \overline{a_m(f)} q^m$.

2.4. Artin L-functions

An *Artin L-function* is a type of L-function associated to representations of Galois groups as follows. Consider a finite Galois extension E/F of number fields, with Galois group $G = \mathrm{Gal}(E/F)$. Consider a representation

$$\rho\colon G \to \mathrm{Aut}_{\mathbf{C}}(V) \simeq \mathrm{GL}_n(V)$$

of G on an n-dimensional complex vector space V. For every finite place $\mathfrak{p}$ of F, we choose a place $\mathfrak{P}$ of E lying over F, giving us a decomposition group $D_{\mathfrak{P}}$, an inertia group $I_{\mathfrak{P}}$ and a Frobenius element $\sigma_{\mathfrak{P}} \in D_{\mathfrak{P}}/I_{\mathfrak{P}}$. (We recall that $I_{\mathfrak{P}} = 1$ if $\mathfrak{P}$ is unramified, which is the case for all but finitely many $\mathfrak{P}$.) We put

$$\chi_{\mathfrak{p}}(t) = \det(\mathrm{id} - t\rho(\sigma_{\mathfrak{P}}) \mid V^{I_{\mathfrak{P}}}) \in \mathbf{C}[t].$$

This is a polynomial whose coefficients lie in some cyclotomic extension of $\mathbf{Q}$, and which is independent of the choice of prime $\mathfrak{P}$ over $\mathfrak{p}$.

We then define

$$L(\rho,s) = \prod_{\mathfrak{p}} \chi_{\mathfrak{p}}(\mathrm{N}\mathfrak{p})^{-1},$$

where the product runs over all finite places of F.

Example. Let $F = \mathbf{Q}$ and let $E = \mathbf{Q}(\sqrt{-23}, \alpha)$, where α is a root of the polynomial $f = x^3 - x^2 + 1$. Then E is the splitting field of f; it is also the Hilbert class field of $\mathbf{Q}(\sqrt{-23})$. We have $G = \mathrm{Gal}(E/\mathbf{Q}) \simeq S_3 \simeq D_3$. We consider the standard 2-dimensional representation ρ of G.

Let p be a prime. There are four cases:

(1) $p = 23$. Then E has three primes over p with residue field $\mathbf{F}_{23}$ and ramification index 2. The decomposition groups of these primes are the three subgroups of order 2 in G, which are equal to the corresponding inertia groups. The subspace fixed by inertia is 1-dimensional, and the Frobenius action on it is trivial. This implies that $P_{23} = 1 - t$.

(2) $\left(\frac{-23}{p}\right) = 1$ (equivalently, p is a square in $\mathbf{F}_{23}^\times$) and $f = x^3 - x^2 + 1$ has a root modulo p. Then E has six primes over p with residue field degree 1 (and ramification index 1). The decomposition groups are trivial. The image of Frobenius is equal to $\left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right)$. This implies that $P_p(t) = 1 - 2t + t^2$.

(3) $\left(\frac{-23}{p}\right) = 1$ (equivalently, p is a square in $\mathbf{F}_{23}^\times$) and $f = x^3 - x^2 + 1$ has no roots modulo p. Then E has two primes over p with residue field degree 3 (and ramification index 1). The decomposition groups are all equal to the unique subgroup of order 3 in G. The image of Frobenius is conjugate to $\left(\begin{smallmatrix}0 & -1\\ 1 & -1\end{smallmatrix}\right)$. This implies that $P_p(t) = 1 + t + t^2$.

(4) $\left(\frac{-23}{p}\right) = -1$ (equivalently, p is a non-square in $\mathbf{F}_{23}^\times$). Then E has three primes over p with residue field degree 2. The decomposition groups are the three subgroups of order 2 in G. The image of Frobenius is conjugate to $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$. This implies that $P_p(t) = 1 - t^2$.

We compute the Dirichlet series $L(\rho,s)$ using the above information and obtain

$$\begin{aligned} L(\rho,s) &= 1 - 2^{-s} - 3^{-s} + 6^{-s} + 8^{-s} - 13^{-s} - 16^{-s} + \cdots \\ &= \frac{1}{1 + 2^{-s} + 2^{-2s}} \cdot \frac{1}{1 + 3^{-s} + 3^{-2s}} \cdot \frac{1}{1 - 5^{-2s}} \cdot \frac{1}{1 - 7^{-2s}} \cdots. \end{aligned}$$

2.5. L-functions of elliptic curves

An *elliptic curve* over $\mathbf{Q}$ is a certain kind of algebraic curve that can be given by an equation of the form

$$E\colon y^2 = x^3 + ax + b, \quad a, b \in \mathbf{Z}, \quad \Delta = -16(4a^3 + 27b^2) \neq 0.$$

For any prime number $p \nmid \Delta$, we study the solutions of this equation modulo p. More precisely, we define

$$a_p = p - \#\{(x, y) \in \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/p\mathbf{Z} \mid y^2 = x^3 + ax + b\}.$$

Next, we define $L(E, s)$ by the Euler product

$$L(E, s) = \prod_{p \text{ prime}} (1 - a_p p^{-s} + p \cdot p^{-2s})^{-1} \quad (\Re s > 3/2).$$

One can extend this to a completed L-function $\Lambda(E, s)$ using specific factors for primes dividing Δ and for the infinite place of $\mathbf{Q}$.

Theorem 2.3 (modularity of elliptic curves over $\mathbf{Q}$). *Let E be an elliptic curve over $\mathbf{Q}$ of conductor n. Then $L(E, s) = L(f, s)$ for some primitive cusp form f of weight 2 and level n.*

This theorem (formerly the Taniyama–Shimura conjecture) is a very deep result. It was proved first for an important class of elliptic curves (the *semi-stable* ones, corresponding to square-free n) in the work of Wiles, completed by Taylor and Wiles (1995), from which Fermat's last theorem follows. The modularity theorem was then proved in more generality by Diamond (1996), Conrad, Diamond and Taylor (1999) and finally for arbitrary E by Breuil, Conrad, Diamond and Taylor (2001).

The modularity theorem implies that L-functions of elliptic curves over $\mathbf{Q}$ admit an analytic continuation to all of $\mathbf{C}$. This is not at all obvious and there is no known direct way to prove it.

3. Conjectures

We have already encountered the Riemann hypothesis, which predicts that for any 'nice' L-function $L(X, s)$, all non-trivial zeroes of $L(X, s)$ lie on the critical line. We will now mention some more conjectures.

3.1. The Birch–Swinnerton-Dyer conjecture

Let E be an elliptic curve over a number field K. It is known that set $E(K)$ of K-rational points of E has the structure of a finitely generated Abelian group. It therefore has the form

$$E(K) \simeq E(K)_{\text{tor}} \oplus \mathbf{Z}^{\operatorname{rk} E(K)}.$$

Here $E(K)_{\text{tor}}$ is the subgroup of $E(K)$ consisting of elements of finite order (the torsion subgroup) and $\operatorname{rk} E(K)$ is a non-negative integer called the *rank* of E.

On the free Abelian group $E(K)/E(K)_{\text{tor}}$, one has a certain real-valued positive definite bilinear form, the *Néron–Tate height pairing*. From this one can construct a *regulator* $\mathrm{Reg}_{E/K}$, which is the determinant of the matrix of this bilinear form with respect to a basis of $E(K)/E(K)_{\text{tor}}$.

The *Tate–Shafarevich group* of E is a certain Abelian torsion group $\text{Ш}_{E/K}$ attached to E, classifying *locally soluble E-torsors*. This group is conjectured to be finite for every E, but this has not been proved in general. If $\text{Ш}_{E/K}$ is finite, then its order is a square.

One can form an L-function $L(E/K, s)$ in a similar way as we did above for elliptic curves over $\mathbf{Q}$. One can then defined a completed L-function $\Lambda(E/K, s)$ by multiplying $L(E/K, s)$ by a finite number of elementary factors corresponding to the finite places of K at which E has bad reduction and to the infinite places of K.

Conjecture 3.1 (Birch and Swinnerton-Dyer [2], Tate [8]). *Let E be an elliptic curve over a number field K. Then the following holds:*

(1) The function $\Lambda(E/K, s)$ can be continued to an entire function on the complex plane and satisfies the functional equation

$$\Lambda(E/K, s) = \pm\Lambda(E/K, 2 - s).$$

where the sign is $+1$ *or* -1 *depending on whether* $\operatorname{rk} E(K)$ *is even or odd, respectively.*

(2) The Tate–Shafarevich group $Ш_{E/K}$ *is finite.*

(3) We have

$$\operatorname*{ord}_{s=1} \Lambda(E/K, s) = \operatorname{rk} E(K)$$

and the leading term of the power series expansion of $\Lambda(E/K, s)$ *at* $s = 1$ *is given by*

$$\lim_{s\to 1} \frac{\Lambda(E/K, s)}{(s-1)^{\operatorname{rk} E(K)}} = \frac{\# Ш_{E/K} \operatorname{Reg}_{E/K}}{\# E(K)^2_{\mathrm{tor}}}.$$

Remark. A more standard formulation of the above conjecture also involves the product of the Tamagawa numbers at the finite places, and the product of the periods at the infinite places. Following Tate [8], we have absorbed these into the completed L-function $\Lambda(E/K, s)$,

3.2. Application to the congruent number problem

A positive rational number n is called *congruent* if there exists a right-angled triangle with rational side lengths and area n. The *congruent number problem* is the question which n are congruent. This comes down to the question for which n the system of equations

$$a^2 + b^2 = c^2 \quad \text{and} \quad ab = 2n$$

has a solution in non-zero rational numbers a, b, c.

Proposition 3.2. *A positive rational number* n *is congruent if and only if the equation*

$$y^2 = x^3 - n^2 x \tag{3.1}$$

has a solution $(x, y) \in \mathbf{Q} \times \mathbf{Q}$ *with* $y \neq 0$.

It suffices to study the case where n is a square-free positive integer. The equation (3.1) defines an elliptic curve E_n over $\mathbf{Q}$. The congruent number problem was solved by Tunnell [9] assuming the Birch–Swinnerton-Dyer conjecture for elliptic curves of the form E_n. We define sequences of integers $(a_n)_{n\geq 1}$, $(b_n)_{n\geq 1}$ and $(c_n)_{n\geq 1}$ by the following identities of power series in q:

$$\begin{aligned} g &= q \prod_{m\geq 1} \left((1-q^{8m})(1-q^{16m})\right), \\ g \cdot \sum_{n\in\mathbf{Z}} q^{2n^2} &= \sum_{n\geq 1} a_n q^n, \\ g \cdot \sum_{n\in\mathbf{Z}} q^{4n^2} &= \sum_{n\geq 1} b_n q^n, \\ c_n &= \begin{cases} a_n & \text{if } n \text{ is odd,} \\ b_{n/2} & \text{if } n \text{ is even.} \end{cases} \end{aligned}$$

Theorem 3.3 (Tunnell [9]). *Let* n *be a square-free positive integer. If* n *is congruent, then* $c_n = 0$. *The converse is true if the Birch–Swinnerton-Dyer conjecture holds for the elliptic curve* E_n.

Tunnell's proof of the first implication relies on partial results on the Birch–Swinnerton-Dyer conjecture due to Coates and Wiles.

3.3. The conjectures of Deligne and Beilinson, and of Bloch and Kato

For many arithmetic objects X (such as algebraic varieties over $\mathbf{Q}$, and more generally *motives*, although the theory of motives is still largely conjectural), one can define an L-function $L(X, s)$ and a real number $\Omega(X)$ called the *period* of X.

Conjecture 3.4 (Deligne [5], Beilinson [1]). *For suitable* X, *one has*

$$L(X, 0) = \Omega(X) \cdot r(X) \quad \textit{for some } r(X) \in \mathbf{Q}^\times.$$

For X as above, one can also define a real number $T(X)$ called the *Tamagawa number* of X.

Conjecture 3.5 (Bloch, Kato [3]). *For suitable X, the Tamagawa number $T(X)$ is rational, and one has*

$$L(X,0) = \Omega(X) \cdot T(X).$$

References

[1] A. A. Beilinson, Higher regulators and values of L-functions. *Journal of Soviet Mathematics* **30** (1985), 2036–2070.

[2] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves. II. *Journal für die reine und angewandte Mathematik* **218** (1965), 79–108.

[3] S. Bloch and K. Kato, L-functions and Tamagawa numbers of motives. In: P. Cartier, L. Illusie, N. M. Katz, G. Laumon, Yu. I. Manin and K. A. Ribet (editors), *The Grothendieck Festschrift, Volume I.* Progress in Mathematics **86**, Birkhäuser, Boston, Massachusetts, 1990.

[4] J. Bernstein and S. Gelbart (editors), *An Introduction to the Langlands Program.* With contributions by D. Bump, J. W. Cogdell, D. Gaitsgory, E. de Shalit, E. Kowalski and S. S. Kudla. Birkhäuser, Boston, 2004.

[5] P. Deligne, Valeurs de fonctions L et périodes d'intégrales. In: A. Borel and W. Casselman (editors), *Automorphic Forms, Representations, and L-Functions* (Corvallis, Oregon, 1977), Part 2, 313–346. Proceedings of Symposia in Pure Mathematics **33**. American Mathematical Society, Providence, Rhode Island, 1979.

[6] J. P. G. Lejeune Dirichlet, Beweis des Satzes, daß jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Mathematische Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin*, 1837, 45–71.

[7] G. F. B. Riemann, Über die Anzahl der Primzahlen unter einer gegebenen Größe. *Monatsberichte der Königlichen Preußischen Akademie der Wissenschaften zu Berlin*, November 1859, 671–680.

[8] J. T. Tate, On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. Séminaire Bourbaki, 18e année, 1965/66, no. 306.

[9] J. B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2. *Inventiones Mathematicae* **72** (1983), 323–334.