

NUMBER THEORY, L-FUNCTIONS AND MODULAR FORMS

BROOKS ROBERTS

ABSTRACT. Perhaps one of the oldest problems in mathematics and certainly the most basic problem in number theory is this: what are the integer solutions to a polynomial equation with integer coefficients? One famous example is Fermat's Last Theorem. One might start by examining the equation modulo a prime, and we begin our survey of some aspects of this problem by recalling the powerful Weil conjectures, proven by Deligne, for equations over finite fields. The Weil conjectures motivate the introduction of the L-function of our problem, which is an invariant analogous to the Riemann zeta function. We describe the standard conjectures for such L-functions. A philosophy due to Langlands introduces modular forms as a tool for proving these conjectures. We briefly recall this idea, and point out its success in the recent work of Wiles for equations that define curves of genus 1. We close by mentioning the context of our own work, which applies to equations that define surfaces and proves results analogous to older results in the theory of curves.

A very difficult and famous problem in number theory was Fermat's Last Theorem: If M is a positive integer with $M \geq 3$ and x, y, z are integers then

$$x^M + y^M = z^M \implies xyz = 0.$$

Fermat's Last Theorem is a special case of a *diophantine problem*: Given a polynomial $P(x_0, x_1, \dots, x_n)$ with integer coefficients, what can we say about the integer solutions to

$$P(x_0, x_1, \dots, x_n) = 0?$$

The approach I'm going to talk about has three parts. First, I'm going to look at the problem mod p for each prime p . I'll describe the Weil conjectures which give a solution to the problem mod p . Then using that solution, I'll define an invariant, called the Hasse-Weil L -function of the problem, which will encode all the information about the problem for each prime p . I'll state the standard conjectures for such L -functions, and give some examples of how knowledge about the L -functions implies results about our original diophantine problem over the integers. Finally, I'll mention one approach to proving some of the standard conjectures, which is the theory of automorphic L -functions.

1. Diophantine problems mod p

Notes from my University of Idaho colloquium talk from November 12, 1998.

As in solving any problem, a natural thing to do is to look for necessary conditions. If p is a prime, we can look at the above equation mod p . That is, we can look for solutions to the congruence

$$P(x_0, \dots, x_n) \equiv 0 \pmod{p}.$$

A necessary condition that $P(x_0, \dots, x_n) = 0$ have a solution in the integers is that it have a solution mod p , because any solution in the integers gives a solution mod p . What are really doing when we look at the equation mod p ? When we work mod p we are regarding $P(x_0, \dots, x_n)$ as a polynomial with coefficients in the *field* $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, and we are looking for solutions in \mathbb{F}_p . Since \mathbb{F}_p is finite, we can even count the number of solutions in \mathbb{F}_p (for example by going through all the possibilities). We'll try to say something about the number of solutions. But, as in many parts of mathematics, it'll be important to count the number in the right way. To do that we need to recall some algebraic geometry.

As might be familiar to you if you've had an advanced course in classical Euclidean geometry, theorems have nicer statements and proofs if one allows ideal points, i.e., points at infinity. For example, by adding points at infinity we can say that any two lines in the plane intersect in a point. One thing everyone is familiar with Descartes' insight into ordinary Euclidean geometry: he introduced coordinate systems, so that when we do Euclidean geometry we are really working in \mathbb{R}^2 or \mathbb{R}^3 . How can we introduce coordinates for space with points at infinity? Let F be any field, and let n be a nonnegative integer. Then *projective n -space over F* , denoted $\mathbb{P}^n(F)$, is the set of all $(n+1)$ -tuples

$$(x_0, \dots, x_n) \in F^{n+1}$$

such that at least one x_i is nonzero, modulo the equivalence relation

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

if and only if there exists a nonzero λ such that $\lambda(x_0, \dots, x_n) = (y_0, \dots, y_n)$. In other words, $\mathbb{P}^n(F)$ is the set of all lines in F^{n+1} going through the origin. We'll denote the equivalence class determined by (x_0, \dots, x_n) by $[x_0, \dots, x_n]$. This is a point in projective space, and x_0, \dots, x_n are called the homogeneous coordinates of the point; note that they are only determined up to a nonzero multiple. Let's look at some examples: $\mathbb{P}^0(F)$ is just a point; the projective line $\mathbb{P}^1(F)$ is the line F , consisting of all the points $[x, 1]$ with $x \in F$, and the "point at infinity" $[1, 0]$; and the projective plane $\mathbb{P}^2(F)$ is the plane $F \times F$, consisting of the points $[x, y, 1]$ with $x, y \in F$ and the "line at infinity", of all points $[x, y, 0]$ with $[x, y] \in \mathbb{P}^1(F)$.

The Cartesian approach to ordinary Euclidean geometry not only provides a space to work in, but also a way to describe objects like lines and curves: these are the solutions to equations in the coordinates. Equations in the coordinates $P(x_0, \dots, x_n) = 0$ also define objects in projective space. However, because the coordinates of a point in projective space are ambiguous, we require $P(x_0, \dots, x_n)$ to be *homogeneous*: all the monomials of which $P(x_0, \dots, x_n)$ is a sum must have the same degree d . In that case,

$$P(\lambda x_0, \dots, \lambda x_n) = \lambda^d P(x_0, \dots, x_n),$$

so it's meaningful to talk about $P(x) = 0$ for any $x = [x_0, \dots, x_n]$ in $\mathbb{P}^n(F)$. One might wonder, for example, how the usual lines and curves that one works with in \mathbb{R}^2 fit into this picture. As it turns out, any equation in, for example, \mathbb{R}^2 , gives rise to a homogeneous equation in such a way that every solution to the old equation gives a solution to the new homogeneous equation, and moreover, there may be some new solutions at infinity. To do this, one picks a new variable and adds suitable powers of it to each term, so as to make all the terms of the same degree. For example, for $y = x + 1$ we introduce the new variable z , to get the new equation $y = x + z$. The solutions to this equation in $\mathbb{P}^2(\mathbb{R})$ are the previous solutions $[x, x + 1, 1]$, along with the point at infinity $[1, 1, 0]$. Any other line with the same slope will also pass through this point at infinity. In this way, any two lines in \mathbb{R}^2 intersect in a unique point, possibly at infinity.

Let's go back to our original problem. If we now have a homogeneous polynomial $P(x_0, \dots, x_n)$ with coefficients in \mathbb{F}_p , then we can talk about the number N of solutions to $P(x_0, \dots, x_n) = 0$ in $\mathbb{P}^n(\mathbb{F}_p)$. The number N exists, but except for very special examples it is impossible to find a simple formula for N in terms of n and the coefficients of $P(x_0, \dots, x_n)$. However, one can try to find a conceptual or theoretical description of N . This was accomplished by Andre Weil in 1949 in the Bulletin of the AMS. In this paper, Weil began by looking at the example

$$P(x_0, \dots, x_n) = a_0 x_0^d + \dots + a_n x_n^d = 0, \quad a_0, \dots, a_n \in \mathbb{F}_p^\times.$$

The solutions to such equations are said to define *Fermat hypersurfaces*. Weil computed that

$$N = 1 + p + \dots + p^{n-1} + \text{a term involving characters of } \mathbb{F}_p^\times \text{ and Gauss sums.}$$

This formula is satisfying enough if one accepts Gauss sums as primitive. However, Weil was able to say more. He noticed that a similar formula was valid for the number of solutions in *any* finite field containing \mathbb{F}_p . He asked the following question: does the sequence consisting of the number of solutions in the various finite fields containing \mathbb{F}_p have some structure? To explain what Weil discovered, let me remind you of just a bit of the theory of finite fields. Recall that for each positive integer k , there exists exactly one field inside the algebraic closure $\overline{\mathbb{F}_p}$ of \mathbb{F}_p which is an extension of degree k of \mathbb{F}_p . This field is called \mathbb{F}_{p^k} :

$$\begin{array}{c} \overline{\mathbb{F}_p} \\ \uparrow \\ \mathbb{F}_{p^k} \\ \uparrow \\ k \quad \mathbb{F}_p \end{array}$$

The elements of \mathbb{F}_{p^k} are exactly the elements x of $\overline{\mathbb{F}_p}$ which satisfy

$$x^{p^k} = x.$$

Thus, we can also consider the number N_k of solutions to $P(x_0, \dots, x_n) = 0$ in $\mathbb{P}^n(\mathbb{F}_{p^k})$. For example, $N_1 = N$. We then study the increasing sequence

$$N_1 \leq N_2 \leq N_3 \leq \dots$$

Weil looked at the generating function,

$$N_1 + N_2 t + N_3 t^2 + \dots$$

Using his formula, he was able to show that:

$$N_1 + N_2 t + N_3 t^2 + \dots = -\frac{d}{dt} \log(1-t) - \dots - \frac{d}{dt} \log(1-p^{n-1}t) \\ + (-1)^n \text{sum of terms of the form } \frac{d}{dt} \log(1-At^b),$$

where A is an integer and b is a positive integer. Integrating, and then taking exp of both sides one gets:

$$Z(t) = \exp\left(\sum_{k=1}^{\infty} N_k \frac{t^k}{k}\right) = \frac{\prod(1-At^b)^{(-1)^n}}{(1-t) \dots (1-p^{n-1}t)}.$$

We see that $Z(t)$ is a rational function with integer coefficients! Rational functions are simple objects; in particular, it is easy to compute their derivatives. Thus, we can easily compute the N_k via the simple formula:

$$N_k = \frac{1}{(k-1)!} \frac{d^k}{dt^k} \log Z(t)|_{t=0}.$$

Knowledge of the rational function completely determines the sequence of N_k 's.

Weil generalized what he had found. We can define $Z(t)$ as above for any equation $P(x_0, \dots, x_n) = 0$ with coefficients from \mathbb{F}_p . We will call $Z(t)$ the *zeta function* of our equation $P(x_0, \dots, x_n) = 0$. Based on the above and other examples, and deeper theoretical reasons, Weil conjectured the following:

Weil Conjectures. Assume that $P(x_0, \dots, x_n) = 0$ defines a smooth variety in $\mathbb{P}^n(\overline{\mathbb{F}_p})$. Let $D = n - 1$ be its dimension. Then

- (1). (Rationality) $Z(t)$ is a rational function in t with rational coefficients.
- (2). (Functional equation) There is an integer χ such that

$$Z\left(\frac{1}{p^D t}\right) = \pm p^{D\chi/2} t^\chi Z(t).$$

- (3) There is a factorization

$$Z(t) = \frac{Z_1(t) \cdots Z_{2D-1}(t)}{Z_0(t) \cdots Z_{2D}(t)}$$

4

with each $Z_i(t)$ having integer coefficients, $Z_0(t) = 1 - t$, $Z_{2D}(t) = 1 - p^D t$, and for each $0 \leq i \leq 2D$,

$$Z_i(t) = \prod_{j=1}^{b_i} (1 - \alpha_{ij} t).$$

Moreover,

$$|\alpha_{ij}| = p^{i/2} \quad (\text{Riemann Hypothesis}).$$

(Notice that the $Z_i(t)$ are uniquely determined by these conditions and the α_{ij} are algebraic integers.)

(4) If $P(x_0, \dots, x_n)$ is the reduction modulo p of a polynomial with integer coefficients, which we also call $P(x_0, \dots, x_n)$, then b_i is the i^{th} Betti number of the set X of solutions to $P(x_0, \dots, x_n) = 0$ in $\mathbb{P}^n(\mathbb{C})$.

Let's look at an example. Suppose $D = 1$, so that $P(x_0, x_1, x_2) = 0$ defines a curve C in $\mathbb{P}^2(\overline{\mathbb{F}}_p)$. In this case we have

$$Z(t) = \frac{Z_1(t)}{Z_0(t)Z_2(t)} = \frac{(1 - \alpha_1 t)(1 - \alpha_2 t) \cdots (1 - \alpha_{2g} t)}{(1 - t)(1 - pt)}.$$

Here, $g = (d - 1)(d - 2)/2$ is the genus of the curve. By some algebra, one finds that

$$N_k = 1 + p^k - (\alpha_1^k + \cdots + \alpha_{2g}^k) = 1 + |\mathbb{F}_{p^k}| - (\alpha_1^k + \cdots + \alpha_{2g}^k),$$

so in particular, $N_k \rightarrow \infty$. The functional equation says essentially that the map $\alpha \mapsto p/\alpha$ permutes the α_i . The Riemann hypothesis says that

$$|\alpha_1| = \cdots = |\alpha_{2g}| = \sqrt{p},$$

i.e., all the α_i lie on the circle of radius \sqrt{p} centered at the origin. Why is this called the Riemann hypothesis? Well, suppose we substitute p^{-s} in $Z(t)$. Then it turns out that $Z(p^{-s})$ is equal to zeta function of the function field of the curve C defined by $P(x_0, x_1, x_2) = 0$ in $\mathbb{P}^2(\overline{\mathbb{F}}_p)$:

$$Z(p^{-s}) = \zeta_C(s) = \sum_{I \subset D} \frac{1}{\text{Norm}(I)^s},$$

Here, the sum is over the ideals of a certain Dedekind domain D . This is a special case of a general definition; another special case is the Riemann zeta function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Evidently, (3) says exactly that zeros of $\zeta_C(s)$ lie on the line $\operatorname{Re}(s) = 1/2$! This is non-trivial evidence that the usual Riemann hypothesis is true. Currently, perhaps the best approach to the usual Riemann hypothesis is that of C. Deninger. See the summary of his Plenary Address to the ICM-98 at <http://www.mathematik.uni-bielefeld.de/documenta/>. Deninger proposes a proof with a strong analogies to the proof of the Weil conjectures.

The Weil conjectures are beautiful, and are the best possible solutions to the original problem. They also have important applications. One application is to prove the Ramanujan conjecture about the growth of coefficients of modular forms, which can also be regarded as a statement about the size of eigenvalues of certain nonarchimedean Laplacians on arithmetically defined Riemann surfaces. Another important application is the growth of exponential sums in several variables. Also, there are some applications to varieties defined over \mathbb{C} , such as new proof of the Hard Lefschetz Theorem. But perhaps the most important thing to come out of the Weil conjectures is the theory that had to be developed to prove them. This theory is quite ingenious, and has had other major applications. For example, it completely revolutionized the representation theory of finite linear groups like $\operatorname{Gl}(n, \mathbb{F}_p)$; it also lead to the theory of topoi, which is important in logic.

How are the Weil conjectures proven, and what is the required theory? The *fundamental point* is that the Weil conjectures follow from a “good” theory of *algebraic topology* for varieties over any field, specifically, a “good” cohomology theory. As one can see from (4), the *shape* of $Z(t)$ is already determined by ordinary algebraic topology. This is quite amazing and startling. The required cohomology theory, called étale cohomology, was invented by Alexander Grothendieck in the 1960’s. For his work, he received the Fields Medal in 1966. While all algebraic varieties over any field come with a topology, called the Zariski topology, this topology is inadequate for varieties over finite fields. Grothendieck replaced the Zariski topology with étale topology, which isn’t actually a topology at all. What Grothendieck did was generalize the concept of an open cover; then one can do a Čech cohomology type construction to arrive at the required cohomology theory. Why should the Weil conjectures follow from a “good” cohomology theory? The basic observation is that the field $\overline{\mathbb{F}_p}$ has a distinguished automorphism, Frob , called the Frobenius automorphism, which is defined by

$$\operatorname{Frob}(x) = x^p.$$

The fixed points of Frob^k are exactly the elements of \mathbb{F}_{p^k} . We can also think of Frob or Frob^k as a function from $\mathbb{P}^n(\overline{\mathbb{F}_p})$ to itself by acting on the coordinates. Moreover, we see that

$$N_k = \begin{array}{l} \text{fixed points of } \operatorname{Frob}^k \text{ restricted to the set of} \\ \text{solutions to } P(x_0, \dots, x_n) = 0 \text{ in } \mathbb{P}^n(\overline{\mathbb{F}_p}). \end{array}$$

Conveniently enough, in algebraic topology, for a good cohomology theory there is a formula, called the Lefschetz fixed point formula, that computes the number of fixed points of a map in terms of an alternating sum of traces of the induced maps on the cohomology groups. Using the Lefschetz fixed point formula, one can prove (1) and the formula in (3). The functional equation (2) also follows from another cohomological property, namely

Poincaré duality. The statement (4) follows from a theorem that compares étale cohomology with ordinary cohomology. The remaining claim, the Riemann hypothesis $|\alpha_{ij}| = p^{i/2}$, would also follow from more complicated properties for étale cohomology involving algebraic cycles. However, to this day, these properties haven't been proven. Instead, in the mid 1970's, Deligne proved the Riemann hypothesis directly, which was quite unexpected. For this he received the Fields Medal in 1978.

2. L -functions of diophantine problems over the integers

Having considered diophantine problems mod p , we turn back to our original topic of diophantine problems over the integers. Suppose again that $P(x_0, \dots, x_n)$ is a polynomial with integer coefficients. We want to try say something about integer solutions to

$$P(x_0, \dots, x_n) = 0.$$

Since we assume that $P(x_0, \dots, x_n)$ is homogeneous, this amounts to looking for solutions to the equation in $\mathbb{P}^n(\mathbb{Q})$.

The approach we are going to talk about goes back to Riemann, who made the following proposal. Suppose we are given a sequence of integers, or more generally, algebraic integers, indexed by the primes:

$$\alpha_2, \alpha_3, \alpha_5, \dots$$

Then we might try to do what we did before: study this sequence using a generating function. Since Riemann studied functions of a complex variable, he had in mind a function which wasn't just a formal power series, but was instead a function of a complex variable. So, for example, we might try

$$\alpha_2 z^2 + \alpha_3 z^3 + \alpha_5 z^5 + \dots$$

However, studying this function doesn't seem to be useful. Instead, Riemann proposed looking at the function

$$f(s) = \frac{\alpha_2}{2^s} + \frac{\alpha_3}{3^s} + \frac{\alpha_5}{5^s} + \dots$$

He suggested that the analytic behavior of this function, especially at singular points, should say something about the sequence (α_p) . Of course, this series will not converge everywhere. In general, it will converge in some right half plane: if $\alpha_p = O(p^\sigma)$, then it will converge absolutely to an analytic function in $\operatorname{Re}(s) > 1 + \sigma$. However, such a function may very well have a meromorphic continuation to the region to the left of the line $\operatorname{Re}(s) = 1 + \sigma$. This turns out to be true for the sequence that Riemann had in mind:

$$a_2 = 1, a_3 = 1, a_5 = 1, \dots$$

Riemann showed that for this sequence, the poles of his original generating function $f(s)$ in $\text{Re}(s) > 1/2$ are the same as the poles *and* zeros of

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots,$$

which will converge absolutely in $\text{Re}(s) > 1$, and which has a meromorphic continuation to the complex plane, with a simple pole at $s = 1$. The pole at $s = 1$ immediately implies the number of primes is infinite. But Riemann showed much more: he showed that if the zeros of $\zeta(s)$ has no zeros in $\text{Re}(s) > 1/2$, then the number $\pi(x)$ of primes up to x is given by

$$\pi(x) = \text{Li}(x) + O(\sqrt{x} \log x), \quad \text{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

Now $\text{Li}(x) \sim x/\log x$, and we know now by another argument that $\pi(x) \sim x/\log(x) \sim \text{Li}(x)$. However, we still don't know the validity of the error term that would follow from the Riemann hypothesis.

We can at least imitate Riemann, and make a similar definition of a zeta function, but now for our original problem. By the Weil conjectures, for every prime p , and every integer i between 0 and $2D$, we have a polynomial $Z_{i,p}(t)$ coming from the zeta function of our problem mod p . We substitute, as in the example of curves in the discussion of the Weil conjectures, p^{-s} for t , and define

$$L^i(s) = \prod_p \frac{1}{Z_{i,p}(p^{-s})},$$

and call $L^i(s)$ the i^{th} *Hasse-Weil L-function* of our problem. By the Riemann hypothesis part of the Weil conjecture, we know that $L^i(s)$ converges absolutely to an analytic function in $\text{Re}(s) > i/2 + 1$. The resemblance to the Riemann zeta function is clear. Indeed, the Riemann zeta function is a special case! Take, for example, $n = 1$ and $P(x_0, x_1) = x_0$. Then the set of points $[x_0, x_1]$ in $\mathbb{P}^1(\mathbb{F}_{p^k})$ which are roots of $P(x_0, x_1) = 0$ has just one element, $[0, 1]$, so that $N_k = 1$. So,

$$\log Z(t) = \sum_{k=1}^{\infty} \frac{t^k}{k} = - \sum_{k=1}^{\infty} (-1)^{k+1} \frac{(-t)^k}{k} = -\log(1-t).$$

Hence, $Z(t) = 1/Z_0(t) = 1/(1-t)$, which gives the Riemann zeta function. The Riemann zeta function is thus just one of many zeta functions, or as they are often called, *L-functions*, that have relevance in number theory.

But are the Hasse-Weil *L-functions* really useful? Do they actually say something about diophantine problems? One recent example is the proof by Wiles of Fermat's Last Theorem. Actually, Fermat's Last Theorem is only one consequence of Wiles main result, which is

about certain Hasse-Weil L -functions. Wiles' main theorem applies to the case when $n = 2$, so that our equation defines a curve, and in addition, the genus of this curve is 1 (this means that the degree of our polynomial is 3). Such curves are called elliptic curves. Wiles showed that the 1st Hasse-Weil zeta function of an elliptic curve is automorphic, a concept we will explain later. Now Frey, Ribet and Serre proved in 1987 that if the 1st Hasse-Weil zeta functions of all elliptic curves are automorphic, then Fermat's Last Theorem is true. Fermat's Last Theorem follows from the combination of these two theorems. Thus, one diophantine problem, Fermat's Last Theorem, is solved via the Hasse-Weil L -functions of other diophantine problems, namely those of elliptic curves!

Though it is very gratifying to have a proof of Fermat's Last Theorem, this proof is atypical of the way in which Hasse-Weil L -functions are relevant for our problem. We'll describe a more typical example, which perhaps can be regarded as the next great problem in the theory. To explain this example, we'll need to recall some conjectural basic properties of Hasse-Weil L -functions. Essentially, just like the Riemann zeta function, they should extend to the whole complex plane with perhaps one pole, and they should satisfy a functional equation. A precise statement requires that we add "factors at infinity", and a "conductor" to "complete" $L^i(s)$. The factor $L_\infty^i(s)$ at infinity is a product of a finite number of slight modifications of the usual Gamma function. For example, for the Riemann zeta function it is just $\pi^{-s/2}\Gamma(s/2)$. The full definition depends, perhaps not suprisingly after the Weil conjectures, on the Hodge structure of the ordinary cohomology of the space of solutions in $\mathbb{P}^n(\mathbb{C})$ to $P(x_0, \dots, x_n) = 0$. The conductor is just a certain positive integer A ; for the Riemann zeta function, $A = 1$. We set

$$\Lambda_i(s) = A^s L_\infty^i(s) L^i(s).$$

Standard conjectures for Hasse-Weil L -functions.

- (1) (*Analytic continuation*) $L^i(x)$ has a meromorphic continuation to the complex plane, with at most a simple pole at $s = i/2 + 1$ in the case i is even.
- (2) (*Functional Equation*) $\Lambda^i(s) = \pm \Lambda^i(i + 1 - s)$.

These standard conjectures are much weaker than a Riemann hypothesis type conjecture. Indeed, for the Riemann zeta function they already hold, with sign equal to 1. (Recall that we saw that the Riemann zeta function is a 0th Hasse-Weil L -function.)

To explain the general way in which Hasse-Weil L -functions should be relevant to our original problem we'll consider an example, though there is a conjectural analogue for the general problem. In fact, while general conjectures and some general methods exist, it's fair to say that studying classes of examples represents the state of the art, and that the example we are going to relate is a substantial part of what's known. Again, let us fix a polynomial $P(x_0, x_1, x_2)$ which defines an elliptic curve. As we mentioned above Wiles showed that the 1st Hasse-Weil L -function $L^1(s)$ of our elliptic curve is automorphic; a consequence of that, which is almost equivalent to it, is that $L^1(s)$ satisfies the standard conjecture. Thus, while $L^1(s)$ initially is only defined for $\text{Re}(s) > 3/2$, $L^1(s)$ can actually

be evaluated anywhere in the complex plane. Why is this relevant for the diophantine problem $P(x_0, x_1, x_2) = 0$? To explain that, we'll need to recall an old result of Mordell. Mordell showed that the set S of solutions in $\mathbb{P}^2(\mathbb{Q})$ to $P(x_0, x_1, x_2) = 0$ forms, amazingly enough, a finitely generated abelian group, so that

$$S \cong \mathbb{Z}^r \oplus A$$

where r is a nonnegative integer, and A is a known finite abelian group. Certainly, knowing something about r would represent substantial progress for our problem. The connection between $L^1(s)$ and our original problem is now as follows:

Conjecture (Birch and Swinnerton-Dyer). *The order of vanishing of $L^1(s)$ at $s = 1$ is r .*

This conjecture is known in many cases, but we are still a long way from a proof. This example is typical in the way Hasse-Weil L -functions should be relevant to our problem. There are similar conjectures for all cases of our problem, due to Beilinson and Bloch.

3. Automorphic L -functions

As we saw in the last section, the standard conjectures are the beginning point for the application of Hasse-Weil L -functions to diophantine problems. In this last section we will very briefly summarize, with major simplifications, one approach to proving the standard conjectures.

The idea for this program, due in its full generality to Langlands, is that there are other objects, called *modular forms* or *automorphic forms*, which naturally have associated L -functions. More precisely, for each prime p , an automorphic form f has an associated polynomial like $Z_{i,p}(t)$ from above, and one can define in exactly the same way the L -function associated to f . However, in contrast to Hasse-Weil L -functions, there are methods for proving the standard conjectures for automorphic L -functions. In addition, we know enough to say that, essentially, every automorphic L -function is a Hasse-Weil L -function:

$$\text{automorphic } L\text{-functions} \subset \text{Hasse-Weil } L\text{-functions}.$$

Moreover, based on work in various special cases, we can say that if the Hasse-Weil L -functions satisfy the standard conjectures, then the above inclusion must be an equality. Thus, one promising approach to proving the standard conjectures is to prove that every Hasse-Weil L function is an automorphic L -function, i.e., is automorphic. Wiles' main theorem proves this for elliptic curves. An exposition of automorphic forms would require another lecture. See, for example, the survey article *An elementary introduction to the Langlands program*, by Stephen Gelbart, in the Bulletin of the AMS, **(10)**, 1984.