

# Learning Algebraic Number Theory

Sam Ruth

May 28, 2010

## 1 Introduction

After multiple conversations with all levels of mathematicians (undergrads, grad students, and professors), I've discovered that I'm confused about learning modern algebraic number theory. Both to clarify what I need to do for myself and to help younger mathematicians (which at this point, is only undergrads) to have more focus than I had, I've decided to compile a list of what I think is the relevant background. I am obviously not as valuable a resource on this subject as an actual researcher in algebraic number theory, but as much as grad students are a bridge between undergrads and professors, I intend to fulfill that purpose. I know less, but I'm more didactic. If you are someone that knows better and disagrees with what I've written, I invite your comments. In each section, I've listed some jargon that shepherds the area, as well as texts that I've read or intend to read.

## 2 Basic Math

As I'm writing this essay primarily for advanced undergraduates or beginning graduates, I'm assuming most of the material I discuss here has already been encountered. I will use this section merely to highlight which things deserve extra focus, especially if you make the mistake I did of thinking that being a number theorist means there are other branches of math you can safely ignore.

### 2.1 Elementary Number Theory

Even if you never took an undergrad class on this, you can pick up the basics pretty quickly. I think most of this material is going to come off as disorganized, because without a little bit of advanced algebra, you don't see how all these things are connected or how any of them will lead you to modern math. But they're interesting and pleasing on their own right. Personally, I think you find out from elementary number theory if you like number theory or not. I heard secondhand that every branch of math has a dinging room and a kitchen. The dinging room is where you read all the nice theorems and hear about all the great results. The kitchen is where all the actual dirty work is done. If you

don't like the food you're eating, you probably don't care to learn how to make it yourself. So an elementary number theory class will give you a taste (!) of what number theory is like.

It'll be helpful to know some basic things about arithmetic functions, like Euler's phi function and the sigma and tau functions. The Chinese remainder theorem is fun and important. The more you know about quadratic forms, the better. I really enjoyed continued fractions and Pell's equation. And of course, quadratic reciprocity is the crowning glory of this all

Texts: Hardy and Wright is a good read, though it's hard to find a copy. You'd have a strong background if you read that whole book. Apostol's Analytic Number Theory is a little dry, but it will tell you about connections between the arithmetic functions, the Riemann hypothesis, and prime numbers, plus it has exercises. Ireland and Rosen's A Classical Introduction to Modern Number Theory tells you lots of things, and has exercises. I think most books you pick up with titles like Elementary Number Theory will tell you all the relevant information, but some of them will do a better job than others of selling you on the idea that this stuff is interesting. (Don't make the mistake I did, however, of buying Weil's Basic Number Theory-that book is decidedly not for beginners).

## 2.2 Undergraduate/1st Year Graduate Algebra

To call this your bread and butter would grossly underserve it. It would be more appropriate to call it your bread, butter, salad, and appetizer. You won't be able to get anywhere without an understanding of Galois theory. Various results about commutative algebra will be important later, but at this stage, the most important thing is to understand Galois theory in the case of a finite extension. Both the case of number fields and finite fields are important, though I didn't see until much later how the two are connected.

Texts: Dummit & Foote is actually an exceptional text; it does a good job of making the material seem accessible when you first read it, yet it still has enough of a sense of purpose that you're being guided towards more advanced topics. Reading the Galois theory chapters here will be helpful, because I'll later recommend some of the back chapters for commutative and homological algebra. Lang's Algebra is encyclopedic, but it tries too hard to do things in the greatest possible generality. So you may be further removed from what you care about than you realize. Dummit & Foote is better organized, and gives you a steady stream of examples. The other classic text is Artin's Algebra.

## 2.3 Undergraduate/1st Year Graduate Real and Complex Analysis

Even if you want to do algebraic number theory, you'll still need to know analysis pretty well. In the middle of the 19th century, tremendous progress was made on number theory by using analytic methods systematically. If you know anything about the Riemann zeta function or the Riemann hypothesis, or would like to learn, you'll realize the importance of both real and complex analysis.

In real analysis, the thing that comes up frequently is Fourier analysis. Again, you could probably get by accepting all the theory as is, and just allowing yourself Poisson summation. In complex analysis, you need to understand contour integration-this is a harder subject to fake and take as given. Also, eventually for algebraic geometry, it will be important to learn more about complex analysis as complex geometry.

Texts: I haven't read them, but people really like the Stein series. I learned complex analysis from Ahlfors, which I really liked, and I reviewed for my generals from Rudin, which was helpful.

## 2.4 Undergraduate Topology

It's unbelievable to me how important topology is in number theory considerations. First of all, a course in abstract point set topology will be helpful, because when doing number theory, and especially algebraic geometry, you'll be dealing with some weird topologies (i.e. non-Hausdorff). Secondly, in the class field theory, cohomology becomes the natural way to define maps. I'll say more about this in the graduate topology section; just know that you'll get plenty of mileage out of your semester of topology.

Texts: Everyone loves Munkers, and I don't know any sensible alternative.

## 2.5 Undergraduate/1st Year Graduate Differential Geometry

What's important to you is Lie groups, so I've included this section to be thorough. If you're pressed for time, this is probably the least useful of everything I've listed, as you can really study Lie groups without going through all the general manifold theory. Additionally, we'll later talk about eigenvectors of differential operators on spaces other than  $\mathbb{R}^n$ , though there too, you can probably make sense of that notion without going through a whole course on it.

## 3 Modern Number Theory

For me, part of the appeal of modern number theory is that it seems to have much more of a unified sense of purpose than any other branch of math. Nevertheless, it seems to me that since that Diophantus and Euclid number theory has concerned itself with two basic questions:

- The properties of the primes, and
- The solutions of polynomial equations.

Now, as for the methods, well, that's where all the work is to be done. Here too I would argue number theorists have an advantage of consistency and unity. I've spent some time trying to learn about the Langlands program, which in various guises is central to much of modern number theory research. This program

connects seemingly separate branches of mathematics, and grandly generalizes most (all?) previous important number theory results. Therefore, what I'm learning and how I'm interpreting what I've learned previously is through this lens. In some book on Fermat's Last Theorem, the author compares the final proof to landing on the moon. The actual landing was certainly impressive, but what was more impressive, and more enduring, was all the technical mastery necessary to get there. This, anyway, is what I tell myself as I struggle to learn all these subjects, some of which, as I've mentioned, seem initially far away from number theory.

Let me begin by laying out what I see as the broad picture, before breaking it down into where I studied each individual pixel. Some of the terms I use here may seem unfamiliar, but I intend to reference them all again in the appropriate subsection below. My rough understanding of Langlands is this. There are two kinds of L-functions. One kind immediately comes from number theory or sometimes geometry-Dirichlet and Dedekind zeta functions, L-functions counting points on elliptic curves, or more generally L-functions that count something. The other kind come from representation theory. For instance, modular forms are some kind of representation of  $SL(2, \mathbb{Z})$ . Associated to these modular forms are L-functions. There are lots of special functions to consider, and you certainly need to look at groups bigger than  $SL(2, \mathbb{Z})$ . Here I'm running up against the edge of what I know, but you actually move beyond matrix groups and Lie groups, at least as far as algebraic groups. Then the conjecture is that these two kinds of L-functions are the same. Every number theory L-function corresponds to some representation theory one. The connection is more sophisticated than that, however. This is what the term functoriality means. You can combine L-functions on one side, and that ought to somehow correspond to combining them on the other side. For instance, if you have L-functions corresponding to field extensions (Dedekind), you can take the composite field extension and now you have a new zeta function that is in some sense a combination of the previous two. Then there ought to be three corresponding L-functions on the other side, with the third function somehow a combination of the first two. Anyway, to even make sense of all these functions, there seems to be a fair amount of necessary background, at least enough to keep me busy well into the foreseeable future.

### 3.1 Classical Algebraic Number Theory

If your number theory class had any hopes of turning some of the students into mathematicians, it spent some time on quadratic reciprocity. This is merely the easiest example of a much larger theory, which again is concerned with our two basic questions. In solving an irreducible polynomial over  $\mathbb{Q}$ , we look at a larger field, say  $K$ . Now corresponding to  $\mathbb{Z}$  inside  $\mathbb{Q}$  are the *algebraic integers* inside  $K$ . Remember that for a field extension  $K$ , we say an element  $\alpha \in K$  is *algebraic* if it satisfied some polynomial  $f(x) \in \mathbb{Q}[x]$ . Now if we ask for a polynomial of smallest degree, and scale so that leading coefficient is 1, we can speak of the minimal polynomial of  $\alpha$ . We form a further distinction by saying

it is *integral* if  $f(x)$  the minimal polynomial, has coefficients in  $\mathbb{Z}$ . Now since  $\mathbb{Q}$  has characteristic 0, every algebraic extension is separable, so by the primitive element theorem every extension  $K$  is of the form  $\mathbb{Q}[\alpha]$ . It is not true in general, however, that  $O_K$ , the ring of algebraic integers, is equal to  $\mathbb{Z}[\alpha]$ . For instance, if  $K = \mathbb{Q}[\sqrt{5}]$ , then  $\mathbb{Z}[\sqrt{5}]$  is contained in, but is not equal to, the ring of integers. In fact,

$$O_K = \mathbb{Z}\left[\frac{1 + \sqrt{5}}{2}\right].$$

In general, it is hard problem to find the ring of integers (though it is easy to do so for quadratic extensions). What is true though is that the ring of integers is a free module over  $\mathbb{Z}$  of dimension  $n = [K : \mathbb{Q}]$ . In fact, much more can be said about the ring of integers as a ring.

A commonly asked test or general question is to name a ring that is not a UFD. The standard answer is  $\mathbb{Z}[\sqrt{-5}]$ . This is a standard mathematical theme: we can gain something by looking at a bigger object, but we lose something as well. For instance, by moving from  $\mathbb{R}$  to  $\mathbb{C}$ , we gain algebraically closed, but we lose our ordering. Similarly, in ring of integers over  $\mathbb{Z}$ , we gain solutions to a polynomial, but we lose unique factorization. Note that factorization is a problem dealing with our other theme, the structure of the primes. While we can no longer uniquely factor elements into prime elements, what we can do is uniquely factor ideals into prime ideals. If we start with a prime ideal  $(p)$  in  $\mathbb{Z}$ , it may or not stay prime—that is, there may be bigger prime ideals containing it, and it may be contained in more than one prime ideal. For instance, in the ring of integers  $\mathbb{Z}[i]$ , there are exactly three things that can happen to a prime  $p$  of  $\mathbb{Z}$ . Note that here by  $(p)$  I mean  $p\mathbb{Z}[i]$ , that is, the ideal generated by  $p$  in this bigger ring.

$$\begin{array}{ll} p = 2 & (p) = (1 + i)^2 & (1) \\ p \equiv 1 \pmod{4} & p = (a + bi)(a - bi) \text{ where } a^2 + b^2 = p & (2) \\ p \equiv 3 \pmod{4} & (p) = (p) & (3) \end{array}$$

In the first case,  $p$  is said to *ramify*, in the second case it *splits*, and in the third case it is *inert*. Note that what happens to  $p$  in  $\mathbb{Z}[i]$  has to do with whether  $-1$  is a square  $\pmod{p}$ . To know whether  $-1$  is a square  $\pmod{p}$ , we use quadratic reciprocity. In general, the behavior of  $(p)$  in  $\mathbb{Z}[\sqrt{q}]$  is related to whether  $x^2 - q$  splits  $\pmod{p}$ .

The idea of primes not remaining prime in a ring extension is an idea that is useful in much more generality than just finite extension of  $\mathbb{Q}$ , which are called *number fields*. This is an example of a map between rings (in this case, the inclusion map  $\mathbb{Z} \subset \mathcal{O}_k$ ) giving rise to a map between prime ideals. These maps are fundamental to algebraic geometry. This also forms the beginning of the connection between number fields and function fields. A (relatively) concrete example of this is the case of *p-adic numbers*  $\mathbb{Q}_p$ , where  $p$  is a prime number. These can be defined in several ways, but I think the most straightforward is to

think of them as formal power series, that is they look like

$$\alpha = \sum_{i=-n}^{\infty} \alpha_i p^i,$$

where  $0 \leq \alpha_i \leq p - 1$ . I won't go into details on these here, but they have the property that the ring of integers  $\mathbb{Z}_p$  has a unique maximal ideal. Such a ring is called a *local ring*. Also,  $\mathbb{Z}_p$  is a PID. A local ring that is also a PID is called a *discrete valuation ring*. One way of thinking about the  $p$ -adic numbers is that powers of  $p$  are getting close to 0-this is some explanation for why the power series should be thought of as converging, because the high powers of  $p$  are small. One reason we study  $p$ -adics is because they can tell us information about  $\mathbb{Q}$ . Here's an example that's encountered early in the study of  $p$ -adics.

**Theorem 3.1.** (*Hasse-Minowski*). *A quadratic form*

$$a_1 x_1^2 + \cdots + a_n x_n^2 = c$$

*has a solution  $(x_1, \dots, x_n) \in \mathbb{Q}^n$  if and only if it has a solution in  $\mathbb{R}$  and  $\mathbb{Q}_p$  for every  $p$ .*

This result characterizes the kinds of results we aim for with  $p$ -adics. We can reduce global questions (solutions over  $\mathbb{Q}$ ) by looking locally (solutions over  $\mathbb{R}$  and  $\mathbb{Q}_p$ ). With a bit more development of the finite extensions of  $\mathbb{Q}_p$ , we can say even more about number fields. A finite extension of  $\mathbb{Q}_p$  is called a  $p$ -adic number field.

Now the fields  $\mathbb{Q}_p$  and its extensions tell us things about the extensions of  $\mathbb{Q}$ . The heart of late 19th, early 20th century number theory is the classification of abelian extensions of  $\mathbb{Q}$ . An *abelian extension* is a Galois extension whose Galois group is abelian. There are multiple approaches to developing this theory, but in any case, it goes by the name of class field theory, and has a local and global component. In the local case, it's easy to state, and hard to say what the maps are explicitly.

**Theorem 3.2.** (*Local Class Field Theory*) *There is a bijection between abelian extensions of  $\mathbb{Q}_p$  and open subgroups of  $\mathbb{Q}_p^*$ .*

The topology on  $\mathbb{Q}_p$  is that given by the valuation. An abelian extension  $L_p$  over  $\mathbb{Q}_p$  gives rise to a subgroup through the norm map,  $N_{\mathbb{Q}_p}^{L_p} L_p$ .

The global case requires a bit more terminology to be able to state; in one sense, the global case corresponds to looking at all the local cases (that is, for every prime  $p$ ) simultaneously. As this is closely related to the important notion of class group, I will define that first.

As discussed earlier, in an arbitrary number field, we do not have factorization of elements, but only factorization of ideals. Now the factorization of ideals into prime ideals would correspond to prime factorization if all ideals were principal. In general, the rings of integers are not PIDs. (In fact, they are PIDs if and only if they are UFDs). However, for any ideal  $A$ , we can find another

ideal  $A'$  such that  $AA'$  is principal. With this multiplication in mind, the set of ideals modulo principal ideals is in fact a group. This is called the *ideal class group*.

**Theorem 3.3.** *The ideal class group is finite.*

Computing orders of class groups is a discipline in itself, even in the quadratic case. It is not known if there are infinitely many quadratic extensions with class number 1 (that is, they are PIDs).

Connected to the class group, although it's not at first obvious why, is the idele class group. The *adeles* of a number field  $K$  are the elements of the direct product  $\prod_{\mathfrak{p}} K_{\mathfrak{p}}$ , where the product is over all prime ideals, and the coordinate in the  $\mathfrak{p}$  place is a integer for all but finitely many  $\mathfrak{p}$ . Addition and multiplication are defined componentwise. The *ideles* are a subring of the adeles where almost every (all but finitely many) of the coordinates are units.

Note that  $K$  sits inside all of its completions; there is an embedding of  $K$  into  $K_{\mathfrak{p}}$  for every  $\mathfrak{p}$ . Under this embedding, an element  $\alpha \in K$  is a unit for almost every  $\mathfrak{p}$  (because there are only finitely many primes that divide the numerator of  $\alpha$ ). This means that every element of  $K$  gives rise to an idele. The image of  $K$  in  $\mathbb{A}_K$  is called the *principal ideles*. The ideles modded out by the principal ideles form a group, called the *idele class group*. The ideal class group is isomorphic to a quotient of the idele class group.

**Theorem 3.4** (Global Class Field Theory). *There is a bijection between open subgroups of the idele class group of  $K$  and finite abelian extensions of  $K$ .*

Texts: I started by trying to read Lang's Algebraic Number Theory, which was painful, though I think it helped. In retrospect, I should have started with Marcus' Number Fields or Samuel's Algebraic Integers. These both explain, concretely, why these algebraic constructs should be of any interest to a number theorist, and Samuel has lots of exercises to familiarize yourself with decomposition group, inertia group, and the like. I eventually read Neukirch's Algebraic Number Theory (I think that's the title), which I would highly recommend. He does a lot of things with commutative diagrams and exact sequences, which is annoying, but supposedly better generalizes to higher dimension. I started with almost no algebraic number theory background and I finished this book in one semester, so it's not too serious of a time commitment.

## 3.2 Analytic Number Theory

When I say analytic number theory, I mean the use of analysis in number theory. I think the distinction between the two branches is not as strong as it used to be.

The first order of business is the analytic objects which encode information about number fields. These include the Dirichlet  $L$ -functions, Dedekind zeta functions, Hecke  $L$ -functions (which generalize the first two) and Artin  $L$ -functions (which generalize the Hecke ones). These connect with algebraic

number theory through the class number formula, which relates the class number to the value of a Dirichlet  $L$ -function, and the Tchebatorev density theorem, which tells you about how primes split in extension fields.

But then they have their own properties and applications. The Dirichlet  $L$ -functions include the Riemann zeta function, and they are used similarly to answer questions on the distribution of prime numbers (including the prime number theorem). They also share the important properties of meromorphic (or analytic) continuation, functional equations, and Euler factorization. More specifically, let  $\chi$  be a homomorphism from  $G = (\mathbb{Z}/n\mathbb{Z})^*$  to  $\mathbb{C}$ . Because  $\chi$  is a homomorphism and every element in  $G$  has finite order, the image is actually contained in  $\mu_{\phi(n)}$ , the  $\phi(n)$ th roots of unity. Extend this function to all of  $\mathbb{Z}/n\mathbb{Z}$  by letting  $\chi(m) = 0$  if  $(m, n) > 1$ . Now we can turn this into a function of  $\mathbb{Z}$  by composing  $\mathbb{Z} \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{C}$ . Now define the function

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

If we picked the right  $\chi$  (we want it to be primitive), then this function will be nice. Specifically, if  $n = p$ , some prime  $p$ , then all the  $\chi$  are primitive. By being clever about adding together the different  $\chi$  corresponding to a fixed  $p$ , we can get a sum that only picks out terms  $n$  that are congruent to  $a \pmod{p}$ . This is how one shows that

$$\sum_{\chi} L(\chi, s) \sim \sum_{q \equiv a \pmod{p}} \frac{1}{q^s},$$

where the sum on the right is over prime  $q$ . Then since the sum on the left diverges to  $\infty$  as  $s \rightarrow 1^+$  (it includes a term that is essentially the Riemann zeta function), there must be infinitely many  $q \equiv a \pmod{p}$ . This is how one proves

**Theorem 3.5** (Dirichlet's Theorem on Primes in Arithmetic Progressions). *If  $(s, r) = 1$ , then there are infinitely many primes of the form  $s + nr$ , and*

$$\lim_{x \rightarrow \infty} \frac{\#\{\text{primes less than } x \text{ and } \equiv t \pmod{s}\}}{\#\{\text{primes less than } x\}} = \frac{1}{\phi(r)}.$$

More generally, there are a lot of ways to build functions that are initially convergent on some right half-plane, but then have meromorphic (or analytic) continuation to the whole complex plane. These also have functional equations and sometimes Euler factorizations. The study of such functions and the connections between them is central to the Langlands program. I'll spend some time here on the ones I think I know something about.

The Riemann zeta function is first encountered as

$$\zeta_{\mathbb{Q}}(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

This can be reinterpreted as summing over all ideals in  $\mathbb{Z}$ . The reason for this reinterpretation is that it allows us to define a  $L$ -function for a number field

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N\mathfrak{a}^s}.$$

This requires some work to define the norm of an ideal. A prime ideal  $\mathfrak{p} \subset \mathcal{O}_K$  sits over some prime ideal  $(p) \in \mathbb{Z}$ , and has some inertia degree,  $f = [\mathcal{O}_K/\mathfrak{p} : \mathbb{Z}/(p)]$ . Define  $N\mathfrak{p}$  to be  $p^f$ . Now as the set of ideals is the free abelian group generated by the prime ideals, this definition can be extended to an arbitrary ideal. Note that information about this ideal, the inertia degree, is included in the definition of the Dedekind zeta function. Now, the study of the Riemann zeta function really began when Euler noticed its prime factorization

$$\zeta_{\mathbb{Q}}(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1}.$$

The Dedekind zeta functions have a similar prime factorization

$$\zeta_K(s) = \prod_{\mathfrak{p} \text{ prime}} (1 - N\mathfrak{p}^{-s}).$$

The Dedekind zeta function can be split into sums among the elements of the class group; the fact that these sums turn out to be roughly equal, regardless of the choice of element of the class group, allows one to say that the primes in  $\mathcal{O}_K$  are evenly distributed among the cosets of the principal ideals. Like the Riemann zeta function, the Dedekind zeta function has a simple pole at  $s = 1$ . The residue of the subsums at  $s = 1$  can be computed in terms of arithmetic information about the ring of integers; then the sum of the residues is equal to  $h_K$ , the class number, times this data. In this way, the  $L$ -function can be used to compute the class number. The  $L$ -functions somehow can tell you a lot about the field then. In the case of quadratic fields, there is a connection between the Dirichlet, Dedekind, and Riemann functions. A quadratic extension is necessarily of the form  $\mathbb{Q}(\sqrt{d})$  for some square-free  $d \in \mathbb{Z}$ . Let  $\chi$  be the unique quadratic character defined  $(\text{mod } d)$ . (Quadratic means that  $\chi^2 = 1$ , so  $\chi$  is real-valued). Then

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s)L(s, \chi).$$

The  $L$ -functions quickly become more complicated. As already mentioned, there are the Hecke and Artin  $L$ -functions. Dirichlet  $L$ -functions arise from characters on the groups  $\mathbb{Z}/n\mathbb{Z}$ . Hecke  $L$ -functions arise from characters on the ray class group (Fix an ideal  $\mathfrak{m}$ . Define  $J_{\mathfrak{m}}$  to be the set of ideals coprime to  $\mathfrak{p}$ , that is, their prime factorizations do not include any of the prime ideals in  $\mathfrak{m}$ . Define  $P_{\mathfrak{m}}$  to be the set of principal ideals generated by  $\alpha$  such that  $\alpha \equiv 1 \pmod{\mathfrak{m}}$ ). The group  $J_{\mathfrak{m}}/P_{\mathfrak{m}}$  is called the *ray class group* with respect to  $\mathfrak{m}$ ). The Hecke  $L$ -functions are defined based on these characters. There is (at least) a hard way and an easy way to prove these have analytic continuations

and functional equations. The hard way is how it was originally done. The new easier way is one of the main results of Tate's thesis, which explains how these global  $L$ -functions are products of local  $L$ -functions.

We also have Artin  $L$ -functions; these are given by taking representations of the Galois group. In case the Galois group is abelian, these coincide with the Hecke  $L$ -functions. From a basic theorem in representation theory, Artin  $L$ -functions can be written as rational functions of simpler  $L$ -functions, which allows one to show they have a functional equation and they are meromorphic. It remains an open problem to show they are in fact entire.

Beyond these, there are the  $L$ -functions coming from other special functions. These include  $L$ -functions from counting the points on an elliptic curve, the  $L$ -functions coming from the Fourier coefficients of modular forms. I'm not entirely clear about these  $L$ -functions, so I'll say a little here about modular forms and devote a later section to elliptic curves.

A modular form is a holomorphic function on the upper half plane of the complex numbers that acts nicely under the action of fractional linear transformations. More precisely, a *modular form of weight  $k$*  is a holomorphic function on  $\mathbb{H} = \{z \in \mathbb{C} | \text{Im}z > 0\}$  such that

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

for  $a, b, c, z \in \mathbb{Z}$  with  $ad - bc \neq 0$ , which is also meromorphic at infinity. I'm still learning the various interpretations of these conditions in terms of differential forms and differential operators and functions on lattices and elliptic curves, so I can't really get into that. There are however several interesting facts about modular forms. For one, the space of modular forms for any fixed weight  $k$  is finite dimensional (in fact, 0 dimensional if  $k$  is odd). The easiest example of a modular form of weight  $k$  are the *Eisenstein series*

$$E_k(z) = \sum_{-\infty < m, n < \infty, (m, n) \neq (0, 0)} \frac{1}{(m + nz)^k}.$$

What is in fact true is that the space of modular forms of any given weight is generated by  $E_4$  and  $E_6$ . Furthermore, since by the modularity condition  $f(z+1) = f(z)$ , the modular forms has Fourier series,  $f(z) = \sum a_n e^{2\pi i n z}$ . We use the Fourier coefficients then to make a  $L$ -function  $\sum a_n n^{-s}$ . Again, because of the modularity conditions and other properties satisfied by the modular forms (including their relationships with the Hecke operators), these  $L$ -functions satisfy certain properties similar to those encountered before (such as a multiplicativity of the Fourier coefficients). This allows to come up with a Euler product of modular forms.

There are a couple of directions of generalizations for modular forms. The first is that what I've described are modular forms of full level, because they're invariant under all of  $SL(2, \mathbb{Z})$ . You could instead ask that they be invariant under a subgroup, one of the congruence subgroups. Much of the theory still goes through. These forms somehow correspond to different surfaces (the ones

of full level are for  $PSL(2, \mathbb{Z})$   $PSL(2, \mathbb{R})/SO(2)$  As I don't really understand these surfaces, that's all I say about this direction.

Another direction is that these modular forms can be seen as functions on  $GL_2$  on the adèles which are trivial on principal elements of  $GL_2$ . This line of thought is the beginning of the theory of automorphic forms, which I also know nothing about. I plan to read more about this in the fall. .

Texts: I cheated by learning the analytic theory the algebraic way. I think again that Serre's A Course in Arithmetic is helpful, as he works through the basic facts about modular forms. The Neukirch book I mentioned earlier will tell you about the different kind of number theory  $L$ -functions. At some point, you'll have to read Tate's thesis. For further study in modular forms and automorphic forms, I intend to read Bump's book Automorphic Forms and Representation theory.

### 3.3 Representation Theory

This comes up in a couple of different ways. First, they're the representation theory of finite groups. As this is how Artin  $L$ -functions are defined, it's helpful to know a little about this.

The more involved way is the representation theory of different kinds of Lie groups. As I discussed earlier, I think this plays a large role in modern Langlands philosophy, but I don't know enough about specific examples to say how exactly it comes up. What I do know is that there are two special cases that are worked out first, compact connected Lie groups and simple Lie algebras. Here again I'm probably not qualified to say any more than that.

Texts: For the finite stuff, I think Serre's Linear Representations of Finite Groups is great. For Lie groups, I've read three different texts that have complemented each other well. Humphreys is very pure in its algebraic study of the Lie algebras. It proves everything but it can be difficult to follow what's going on. Fulton & Harris is the opposite extreme-it pushes all the proofs off to the appendix (or doesn't do them at all), but is loaded with examples and tells you the general algorithm for studying the representations of a semi simple Lie algebra. I don't think the phrase Lie group appears at all in Humphreys, and Fulton & Harris is pretty cavalier that taking care of the Lie algebras should be enough. To study the Lie groups, Adams' Lectures on Lie groups is great. It's a little archaic in some of its terminology, and some parts of proofs (like the Peter-Weyl theorem) are pushed out to other sources. However, it's really the groups that you care about, so it's necessary to read.

### 3.4 Commutative Algebra

I'm basically learning this subject as needed for number theory and algebraic geometry. As algebraic geometry frequently tells you geometric facts based on algebraic facts, you need to understand the algebraic facts. However, it's hard to remember the algebraic facts without pairing them with geometry so you have some intuition.

Texts: I found the commutative algebra sections in Dummit and Foote to be extremely helpful. Eventually you'll need to read Atiyah and MacDonald, and as everyone says, do all the exercises. I'll say more about this in the next section.

### 3.5 Algebraic Geometry

This is hard. Modern algebraic number theory has become closely intertwined with algebraic geometry. I'm told two great results of number theory which demonstrate the efficacy of algebraic geometry are Deligne's proof of the Weil conjectures and Falting's proof of the Mordell conjectures. In what I've learned about algebraic geometry, you have to use some light algebraic geometry.

So again I can't say much about how this fits into some grander SCHEME (pun fully intended) of number theory. I'll find this out hopefully within a year or two.

Texts: I started by reading Shafarevich's Into to Algebraic Geometry. This is fairly informal, and it's not always clear where the definitions or theorems are. Also, like other texts in algebraic geometry, you have to be careful to notice when he's using a piece of commutative algebra. The first volume deals with varieties, and I think is pretty helpful for that. I also read the beginning of the second volume, where he begins discussing schemes. A big asset of these books is that they have exercises. I benefited from reading Miranda's Riemann Surfaces, which lays out the definitions quite clearly in the case of curves. I would advise anyone interested in learning their algebraic geometry about curves first, before trying to learn it in the abstract. Everyone says eventually you have to read Hartshorne. Here's a three step process to mastering Hartshorne

- Buy a copy of Hartshorne.
- Try to find a leprachaun who knows Hartshorne and is willing to teach it to you.
- You're screwed.

This book is extremely difficult to read, and it should definitely be read with company and other texts. I'm now reading through Ravi Vakil's online notes on Algebraic Geometry, which I'm finding very helpful. In particular, he develops the category theory and the commutative algebra as he needs it.

### 3.6 Elliptic Curves

On a purely logical standpoint, elliptic curves should probably be treated as a subfield of algebraic geometry. However, there seems to be so much unique about them that does not apply to more general cases that they warrant their own study. In any case, I've found it helpful to learn about elliptic curves, both because the theory itself is interesting and because it gives you concrete examples of the definitions and theorems of algebraic geometry.

Naively, an elliptic curve is a cubic equation in two variables with coefficients over some base field. This naive definition requires some refinement. The first is that we require the curve to be nonsingular—this means there are no double points, no cusps, no points where the curve intersects itself. This also means the curve isn't secretly simpler than a third degree equation should be. This is similar to the case of a degenerate conic—the quadratic  $x^2 - y^2 = 0$  is just the union of two lines, so it shouldn't be thought of like a circle—it should be thought of like two lines.

Many initial questions about elliptic curves are motivated by similar questions about quadratics. For instance, given a quadratic equation like  $x^2 + y^2 = z^2$ , you may ask for the rational solutions. As I said earlier, this is one of the fundamental problems of number theory, to find solutions to equations. To find rational or even integer solutions to this equation, we may in fact divide both sides by  $z^2$  and change variables to get  $x^2 + y^2 = 1$ . Now this is an equation we can graph over the real numbers—we get a circle. It's also an equation where we can easily find a solution, for instance  $(-1, 0)$ . Now the clever part. Suppose  $(x, y)$  is another rational solution to the equation. Then the line connecting  $(-1, 0)$  and  $(x, y)$  has rational slope. It is also true that if we take a line with rational slope, it will intersect the circle at a rational point. This is because the finding the intersection of a line and a circle will give us a quadratic in one variable, which we can solve with the quadratic equation. Since we know one solution is rational,  $x = -1$ , the other one must be as well. Therefore, we have a bijection between the set of rational slopes  $\mathbb{Q}$ , and the rational points on the curve. Note that this bijection depends on the choice of initial point. If we take the line with slope  $t$ , we find the point  $\left(\frac{t^2-1}{1+t^2}, \frac{2t}{1+t^2}\right)$ . Letting  $t = \frac{m}{n}$ , we come back to a well-known parametrization of the integer Pythagorean triples,  $x = m^2 - n^2$ ,  $y = 2mn$ ,  $z = m^2 + n^2$ .

In this analysis, there was something special about the fact that our equation was quadratic—namely, it let us say that we had one rational point, we could find the rest of them. Increasing the degree by 1 makes this question much harder. As before, we assume we have one rational point. In fact, this is usually given as the other condition of an elliptic curve—that a base point be given. If our curve has a point over  $\mathbb{Q}$ , we make perform a change of variables and move this point to  $(0, 0)$  (here already we can apply to algebraic geometry, saying this map is a rational map and therefore doesn't change any of the essential properties of the curve). In fact, over  $\mathbb{Q}$ , we can write the equation as  $y^2 = x^3 - g_2x - g_3$ . Again we want to find the rational points on this curve. However, simply drawing a line with rational slope won't work this time—most lines should intersect the curve at three points, but there's no guarantee the other two will be rational (or even real).

The rational points on an elliptic curve have an algebraic property, however, that we can exploit. We can in fact make a group law on the points that turns them into an abelian group. Again, the most natural way to define this law is through algebraic geometry, but it can be defined, albeit mysteriously, through simple planar geometry. For any two points  $P, Q$  on the curve, draw the secant

line connecting them (if  $P = Q$ , take the tangent line through  $P$ ) This line will intersect the curve at a third point. Because of the equation, the curve is symmetric with respect to the  $x$ -axis. Take the reflection of the intersection point with respect to the  $x$ -axis. This point will be defined as  $P + Q$ .

From the equation of the elliptic curve, we can compute explicitly what  $P + Q$  is in terms of the coordinates of  $P$  and  $Q$ . In particular, we find that  $P + Q$  has coordinates that are rational functions of the coordinates of  $P$  and  $Q$ , so if  $P, Q$  are rational points, so is  $P + Q$ . Thus our operation is on the set of rational points.

To make this a group, we need to identify the identity, additive inverse, and verify the associative law. Again, these seem more natural when given from the standpoint of algebraic geometry, but can still be explicitly discussed without it. The identity is the point at infinity of the curve; intuitively, you can think of the point at infinity as being at  $x = 0$ , and  $y = \infty$ . Drawing the secant line from a point  $P$  and the point at infinity  $O$  is then a vertical line going through  $P$ ; the group operation described then gives you back the point  $O$ . It is also clear what the inverse should be—you take  $-P$  to be the reflection of  $P$  with respect to the  $x$ -axis. Finally, with the explicit formula, it is straightforward, though computationally heavy, to verify the operation is associative. It is obviously commutative.

Now that we know the rational points form a group, we can ask what sort of group they are. Though there are some positive results in this area, there are also some frustrations. To begin with,

**Theorem 3.6** (Mordell-Weil). *The group of rational points is finitely generated.*

As a finitely generated abelian group, the rational points admit a decomposition

$$\mathbb{Z}^r \oplus Tor,$$

where  $Tor$  is the torsion part of the group, that is, the points of finite order. There is a theorem of Mazur describing the possibilities for the torsion part. The rank remains more mysterious—it is an open question whether elliptic curves can have arbitrary rank.

All of this has been looking at an elliptic curve over  $\mathbb{Q}$ , but we can also look over other fields. In particular, with a fixed equation, we can look at the number of points the elliptic curve has over a finite field  $\mathbb{F}_p$ . We have to be careful here, as for a finite number of primes, the discriminant will become 0, and so the curve will no longer be nonsingular. Ignoring that, for almost all primes we have an elliptic curve and can count the number of points. For a polynomial equation in two variables, it seems not unreasonable that on average every value of  $x$  will give rise to one in  $y$ ; the equation is of the form  $y^2 = f(x)$ , so intuitively about half the values of  $x$  should give a square, and then there are two corresponding values of  $y$ . This intuition turns out to be correct.

**Theorem 3.7** (Hasse). *If  $N_q$  is the number of points of an elliptic curve over  $\mathbb{F}_q$ , then*

$$|N_q - q - 1| < 2\sqrt{q}.$$

Now as with other problems, we can combine the data at each of the primes together. We start by defining a local  $L$ -function  $L_p(s) = \exp(\sum_{e=1}^{\infty} N_p^e p^{-es})$ , then combine these local factors to get the  $L$ -function associated with the elliptic curve

$$L(s) = \prod_p L_p(s).$$

As before, the arithmetic properties of the elliptic curves are conjectured and in some cases verified with the analytic properties of this  $L$ -function. In particular, we have one version of the celebrated Birch-Swinnerton-Dyer Conjecture, one of the Millenium Problems

*The order of vanishing of the  $L$ -function at  $s = 1$  is equal to the rank of the elliptic curve.*

I should also say a little about elliptic curves over  $\mathbb{C}$ . Take a lattice  $\Lambda$  over  $\mathbb{C}$ , that is, a discrete, real rank 2 subgroup of  $\mathbb{C}$ . Now take the group  $X = \mathbb{C}/\Lambda$ . The set of meromorphic functions on this space is actually generated by two functions, the *Weirstrass*  $p$ -function and its derivative. These equations also satisfy a cubic equation, that is,  $p(x), p'(x)$  defines a map onto an elliptic curve. It turns out that over  $\mathbb{C}$ , every elliptic curve arises in this way, that is, every elliptic curve is analytically equivalent to a quotient of  $\mathbb{C}$  by some lattice. Now it's possible the same lattice will give us the same elliptic curve. Certainly multiplying our lattice by a constant will give us an isomorphic lattice, so we can scale our lattice and assume that one of the basis vectors is 1 and the other  $\omega$  has positive imaginary part. Therefore, every point on the upper half plane  $\mathbb{H} = \{z \in \mathbb{C} | \text{Im}z > 0\}$  gives us an elliptic curve. But these are still not unique. In particular, we can pick different bases that correspond to the same lattice. Then these two choice of bases will differ by an element of  $SL(2, \mathbb{Z})$  (by linear algebra). Therefore, if we take  $\mathbb{H}/SL(2, \mathbb{Z})$ , every point of this will correspond to a unique (over  $\mathbb{C}$ ) elliptic curve.

Texts: Tate and Silverman's Rational Points on Elliptic Curves is a great introduction-it barely assumes you know Galois theory, and gives some background. After that, Silverman's The Arithmetic of Elliptic Curves is good-it develops the theory much more fully, and again gives you something to do with all that algebraic geometry you've been learning I'm not sure what I'm going to read next-perhaps the other Silverman book.

### 3.7 Cohomology

It's extremely surprising to me how important topology considerations are to number theorists. Then again, I think this was surprising to everyone until about 60 years ago. This comes up in a wide variety of ways, which seem fairly disjoint to me. I'll point some of them out here, and add that to call my knowledge of this area rudimentary would be to pay me too great a compliment.

Algebraic Number Theory-The way to define the bijection in the case of local class field theory turns out to be through the group cohomology of the Galois group. The first time I saw this, I didn't realize it was a topological

construction, but then after I learned some more homological algebra I found the construction more natural.

Algebraic Geometry-I'm told that when considering Spec of a ring, and schemes, their cohomological properties are important. So I'll have to learn more about that. I think this is where étale cohomology comes in. I do know that part of the proof of the Weil conjectures is relating points over finite fields to cohomology of function fields. There are many functors in algebraic geometry that are only left exact or right exact, so we try to compute the cohomology.

Representation Theory-When you make the move from representations of finite groups to representations of compact groups, you suddenly restrict your attention to unitary representations. My understanding is this is largely because you need the extra Hilbert space structure to get any nice theorems about the representations. I believe you care about the topology of something involved here as well; in particular, I think for parts of the Langlands program you look at the cohomology of Lie groups.

Texts: Hatcher still seems to be indispensable for learning about homology and cohomology. I found it easier to read after I already knew what I would be using it for; otherwise it seemed too abstract. Dummit and Foote give you some material on group cohomology, including interpretations of the first two cohomology groups. That might be sufficient, as other texts, such as Hartshorne, give you some more information about cohomology as you need it.