Number Theory II
Spring 2010 Notes

Kimball Martin

February 16, 2010

Exercise 0.1. *Read the introduction. It's a roadmap for the course. In fact, you may want to reread it several times throughout the course to remember where we've been and where we're going.*

Introduction

Last semester, we saw some of the power of Algebraic Number Theory. The basic idea was the following. If for example, we wanted to determine

$$\text{Which numbers are of the form } x^2+ny^2? \tag{1}$$

Brahmagupta's composition law tells us that the product of two numbers of this form is again of this form, and therefore it make sense to first ask

$$\text{Which primes } p \text{ are of the form } x^2+ny^2=p? \tag{2}$$

The idea of Algebraic Number Theory is to work with the ring $\mathbb{Z}[\sqrt{-n}]$ so any p such that $p=x^2+ny^2=(x+y\sqrt{-n})(x-y\sqrt{-n})$ factors over $\mathbb{Z}[\sqrt{-n}]$. At this point one would like to use the Prime Divisor Property (or equivalently, Unique Factorization) to say that this means p is not prime in $\mathbb{Z}[\sqrt{-n}]$. Unfortunately this does not always hold in $\mathbb{Z}[\sqrt{-n}]$, and there were two things we did to overcome this obstacle. The first was to work with $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ which is sometimes larger than $\mathbb{Z}[\sqrt{-n}]$, and may have unique factorization when $\mathbb{Z}[\sqrt{-n}]$ does not (we saw this for the case $n=3$—it happens for other values of n also, but still only finitely many times when $n>0$).

Otherwise, we should use Dedekind's ideal theory. The main idea here is we have the Prime Divisor Property and Unique Factorization at the level of ideas. Hence if $p=x^2+ny^2$, the ideal $(p)=p\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ in $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ is not a prime ideal and factors into two principal prime ideals (not necessarily distinct) $(p)=\mathfrak{p}_1\mathfrak{p}_2$, each of norm p. Further, $\mathfrak{p}_1=(x+y\sqrt{-n})$ and $\mathfrak{p}_2=(x-y\sqrt{-n})$. In fact, with some slight modifications, the converse is also true. To understand this, we first need to understand the more basic question

$$\text{When is } p\mathcal{O}_{\mathbb{Q}(\sqrt{-n})} \text{ a prime ideal, and when does it factor?} \tag{3}$$

Once we know for which primes $p\in\mathbb{N}$, (p) is not prime in $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$ (in which case we say p *splits* in $\mathbb{Q}(\sqrt{-n})$), we need to know

$$\text{What is the class group of } \mathbb{Q}(\sqrt{-n})? \tag{4}$$

to determine when (p) is a product of two principal ideals in $\mathcal{O}_{\mathbb{Q}(\sqrt{-n})}$. The first part of the semester will be motivated by these questions, though we shall spend a lot of our time pursuing related questions and topics along the way. In other words, our goal is not so much to seek a definitive answer to the question (2) (see [Cox]), but rather to use it as a guide to understand and pursue some important topics in number theory. Consequently, we will see how these ideas are related to (i) Dirichlet's class number formula, (ii) Dirichlet's theorem that any arithmetic progression with gcd 1 contains infinitely many primes and (iii) Kummer's approach to Fermat's Last Theorem. References for this part of the course are [Cohn], [Stewart–Tall], [Borevich–Shafarevich], and [Cox]. See also any book on Algebraic Number Theory.

Even knowing an answer to (2), we still won't have a complete answer to (1), since the converse to Brahmagupta's composition law is not true. For example $6 = x^2 + 5y^2$ for $x = y = 1$, but neither 2 nor 3 are of the form $x^2 + 5y^2$. However, we can explain this via Gauss's theory of quadratic forms, which in this case says the product of any two numbers of the form $2x^2 + 2xy + 3y^2$ is of the form $x^2 + 5y^2$. Hence the question of which numbers are of the form $x^2 + 5y^2$ doesn't quite reduce to just determining which primes are of this form. In the second part of the course we will use Gauss's theory to determine which numbers are of the form $x^2 + 5y^2$ by studying the two forms $x^2 + 5y^2$ and $2x^2 + 2xy + 3y^2$ in tandem (as well as understanding where the second form came from). In fact, we will see there is another approach to this question via *Dirichlet's mass formula*, which in this case tells us the number of solutions to $x^2 + 5y^2 = n$ and $2x^2 + 2xy + 3y^2 = n$. I will conclude this section on binary quadratic forms by presenting illustrating how these forms can be used to quantitatively study the failure of unique factorization in $\mathcal{O}_{\mathbb{Q}(\sqrt{-5})}$, a very interesting but largely neglectic topic. References for this section are [Cohn], [Cox], [Borevich–Shafarevich], [Landau], [Hurwitz], [Dirichlet] and [Narkiewicz]. See also any book on quadratic forms.

The third and final part of the course is motivated by the theory of quadratic forms in n variables. Some of the theory of binary quadratic forms carries over to the case of more variables, but some crucial elements do not. We will not be attempting to develop a theory of quadratic forms in n variables, but rather introduce one of the key elements in this theory, the Hasse-Minkowski principle. Roughly, this principle says the following: an equation *should* have a solution in $\mathbb{Z}$ if and only if it has a solution in $\mathbb{Z}/p^k\mathbb{Z}$ for every prime power p^k. This statement is not true in general, but is in special cases. To understand this principle, we'll talk about valuations and p-adic numbers. The Hasse-Minkowski principle can then be used to prove Gauss's famous theorem about which numbers are the sum of three squares. We will follow [Serre] for this. Another important use of p-adic numbers is the modern formulation of higher reciprocity (higher than quadratic) laws. These higher reciprocity laws are given by *class field theory*, which is typically considered the crowning achievement in Algebraic Number Theory, most cleanly stated in the modern language of adèles. Time permitting, we will conclude with a brief discussion of adèles, class field theory and higher reciprocity laws. Some references this are [Ramakrishnan–Valenza], [Ono], [Kato–Kurokawa–Saito], [Cohn2], [Cohn3]. See also any book on Class Field Theory.

This may sound like a rather ambitious plan, and it is. Number Theory is a very rich subject, and one cannot learn even all the central topics of Algebraic Number Theory in a year long course. Any of these three parts could easily form a one semester long course by themselves (though perhaps the first or third more so than the second), and class field theory itself should be a year-long course. Consequently, we will not pursue many topics as deeply as they may deserve (such as Dirichlet's Units Theorem), but I will mention important results and ideas throughout the text, which will hopefully provide at least a good survey of the subject.

This course is not a standard course in number theory, which is the reason we are not following a text. Part of this is due to the fact that the first semester was a mix of elementary and algebraic number theory, whereas they are usually treated separately. But the main reason is my desire to treat the theory of binary quadratic forms (Questions (1) and (2) as well as the second part of the course), which is a very beautiful subject (and one of my interests, though not my primary research focus), but largely neglected in most modern treatments of Algebraic Number Theory (e.g., [Neukirch], [Marcus], [Janusz], [Lang], [Stewart–Tall], [Murty–Esmonde]). Notable exceptions are [Borevich–Shafarevich], [Cohn] and of course [Cox]. However [Borevich–Shafarevich] does not seem appropriate as a text for this class, [Cohn] virtually only treats quadratic fields, and [Cox] already assumes a fair amount of knowledge of algebraic number theory (he reviews it, but omits many proofs). Additionally, [Cohn] and [Cox] say nothing about p-adic numbers. Conversely most books on quadratic forms do not seem to contain much algebraic number theory, and have a different focus than I intend for the course.

Furthermore, while the bulk of the first and third part of the course *are* part of a standard course in Algebraic Number Theory (usually without adèles), most Algebraic Number Theory courses in my experience focus on building up general theory for a long time, often requiring sizable tangents to develop the tools to prove theorems, before being able to get to many applications. While we will treat general number fields throughout the course (and see places where we need them for applications), we will in several places restrict our development of the theory to the case of quadratic fields (though not to the extent of [Cohn]), such as with Minkowski's theory or the class number formula. One critique of this approach might be that one loses much depth this way, however I believe we will gain at least as much as we lose, by being able to go that much deeper into the study of quadratic fields and quadratic forms, thus gaining a more complete and global understanding of the "quadratic" theory, and hopefully a better appreciation of the subject. And in the future, if you need to understand some aspects of the general theory, it would be good to first understand what happens in the simplest setting, that of quadratic fields.

In fact, it is with future aims in mind, that I want to spend a considerable amount of time at the end of the semester on p-adic numbers and adèles. Specifically, they are (i) crucial to understanding modern number theory, (ii) something you need to know about if you end up working with Alan Roche, Ralf Schmidt or myself, and (iii) something that comes up often in the representation theory seminar. During the last week of the course, I will plan on giving survey lectures about class field theory, higher reciprocity laws, and how this leads into the *Langlands Program*, which is the general framework for most of the number theory research going on at OU and OSU.

Finally, since we will be using primarily my notes and not a text, please let me know of any possible errors or unclear portions you may find in the notes so I can address them.