1 Overview

To begin, Number Theory is the study of properties of the positive integers. From an algebraic point of view, it quickly becomes clear that one should actually study the ring of integers \( \mathbb{Z} \), and then the basic question of Number Theory can be formulated as follows:

Given a polynomial \( f(x_1, \ldots, x_m) \in \mathbb{Z}[x_1, \ldots, x_m] \), do there exist integers \( a_1, \ldots, a_m \) such that \( f(a_1, \ldots, a_m) = 0 \)? How many such integral solutions are there?

This question is very hard, so much of this course will be spent investigating a related but easier question: given \( f \) as above and a positive integer \( n \), does there exist a solution modulo \( n \)? That is, do there exist integers \( a_1, \ldots, a_m \) such that \( f(a_1, \ldots, a_m) \equiv 0 \ (n) \)? Recall that the latter condition means simply that the integer \( f(a_1, \ldots, a_m) \) is divisible by \( n \). We can state our problem in a more sophisticated way in terms of the quotient ring \( \mathbb{Z}/n\mathbb{Z} \):

Given a polynomial \( f(x_1, x_2, \ldots, x_m) \in \mathbb{Z}/n\mathbb{Z}[x_1, x_2, \ldots, x_m] \), does the equation \( f = 0 \) have a solution in \( (\mathbb{Z}/n\mathbb{Z})^m \)? How many solutions are there?
The first part of the course (corresponding to Chapters 1-4 of our text) will lay the groundwork for attacking this problem by studying the algebraic properties of the rings $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$. In particular, we will make a careful study of the phenomenon of unique factorization (in $\mathbb{Z}$ and in some related rings), and we will prove structure theorems for the rings $\mathbb{Z}/n\mathbb{Z}$ and their unit groups $(\mathbb{Z}/n\mathbb{Z})^\times$. Through these analyses it will become clear that the most important case of our question occurs when $n = p$ is a prime number, in which case $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ is a finite field with $p$ elements.

When $f$ is a linear polynomial, we will be able to give a relatively complete answer to our basic question without too much trouble. But already things get interesting when we consider a quadratic polynomial in a single variable. The basic question then becomes

Given a prime number $p$, for which integers $c$ does there exist a solution to the congruence $x^2 \equiv c \pmod{p}$?

As we will see, for a fixed prime $p \neq 2$ the answer is simple: a solution exists if and only if $c^{(p-1)/2} \equiv 1 \pmod{p}$. But we will be much more interested in fixing the integer $c$ and letting the prime number $p$ vary, in which case our question becomes:

Given an integer $c$, for which prime numbers $p$ does there exist a solution to the congruence $x^2 \equiv c \pmod{p}$?

The answer to this question is the famous Law of Quadratic Reciprocity, discovered by Euler and Legendre, but first proved by Gauss in 1796.

The second part of the course (corresponding to Chapters 5-8 of our text) will be devoted to various proofs and consequences of Quadratic Reciprocity. Along the way we will study finite fields and introduce some machinery known as Gauss and Jacobi sums. We will use this machinery to give a complete answer to the following special case of our basic question from above:

If $c_1, \ldots, c_m, b \in \mathbb{F}_p$, how many solutions are there in $\mathbb{F}_p^m$ to the equation $c_1x_1^{e_1} + c_2x_2^{e_2} + \cdots + c_mx_m^{e_m} = b$?

If time remains, we will conclude the course by putting questions such as this one into the context of algebraic geometry over finite fields.
2 Practicalities

2.1 Homework and Exams

There will be regular homework assignments, and selected problems will be carefully graded on the following five point scale:

- 5 = perfect – correct and well-written
- 4 = one minor error
- 3 = one major error or several minor errors
- 2 = several major errors
- 1 = indicative of relevant thought

Remember that the quality and clarity of your writing are important. Take the time to make your solution set neat and legible, and strive to effectively convey your ideas. Homework will count for 70% of your final grade, and absolutely no late homework will be accepted.

We will have a take-home midterm as well as a take-home final exam. Each will count for 15% of your grade for the course.

2.2 Office Hours and Other Details

Please feel free to come by my office, whether you are having difficulty or just want to chat about mathematics. Of course, I may not be in, or I may be otherwise engaged and unable to talk. To ensure that you have my undivided attention, you should come during my office hours, which are listed above. Of course, if these times are impossible for you, you can always make an appointment with me.

In addition to talking with me, I encourage you to speak with each other about the course, and even to work together on the problems if that suits your style of learning. That being said, I expect you to spend some time thinking privately about the problems before collaborating, and each of your writeups should be the result of your own cogitation and exposition. If you like to work together, a good model would be to make a first pass through the problems on your own, then get together with friends to talk about difficulties and share ideas, and finally find a solitary place to write a polished (and unique) solution set. Of course, all of your work for this course is governed by the Lawrence University Honor Code.