

INTRODUCTION TO MODERN NUMBER THEORY

COURSE OVERVIEW

AARON POLLACK
JANUARY 4, 2026

CONTENTS

1. Introduction	1
2. Tentative lecture schedule	3
3. Assessment	4

1. INTRODUCTION

The point of this course is to introduce you to some of the big ideas in number theory. I will do this by focusing on some simple-minded problems, whose solutions introduce and/or connect to present day research themes. Here are the problems.

1.1. Quadratic reciprocity. The first problem we will consider is the following:

Problem 1.1. *Fix an integer a , and consider the polynomial $x^2 - a \in \mathbf{Z}[x]$. For which prime numbers p does $x^2 - a$ factor modulo p ? In other words, for which primes p can we write a as a square modulo p ?*

Somewhat remarkably, the question has a simple answer: Whether or not $x^2 - a$ factors modulo p only depends on p modulo $4a$. The solution to this question goes back to Gauss, and goes by the name of **Quadratic Reciprocity**.

Let $\zeta_p = e^{2\pi i/p}$. We will answer Problem 1.1 by doing computations in the subring $\mathbf{Z}[\zeta_p]$ of the complex numbers.

1.2. Primes in arithmetic progression. It goes back to Euclid that there are infinitely many prime numbers p : If there were only finitely many, $p_1, \dots, p_N$, then one sets $M = p_1 \cdots p_N + 1$. But then no p_i could divide M , a contradiction. But what about if we impose a simple condition on the primes? The next problem we will consider is:

Problem 1.2. *Fix a positive integer m , and an integer a relatively prime to m . Are there infinitely many prime numbers p with $p \equiv a \pmod{m}$? In other words, does the arithmetic progression $a, a + m, a + 2m, \dots$ contain infinitely many prime numbers?*

The answer is yes; this was proved by Dirichlet. Beyond being an interesting result, the proof by Dirichlet introduced one of the most important objects of modern number theory, called **L -functions**.

Let s denote a variable in the complex plane; in the context of L -functions, it is standard to use s as a variable name instead of x, y or z . An L -function is a function of s of the form

$\sum_{n \geq 1} a_n n^{-s}$ for certain complex numbers a_n , that satisfies additional properties. Rather than spell them out now, here are some examples:

- (1) Let $a_n = 1$ for all n . Then $\sum_{n \geq 1} n^{-s}$ is called the Riemann zeta function, denoted $\zeta(s)$. This is the simplest example of an L -function.
- (2) Define

$$\chi_4(n) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4} \\ -1 & \text{if } n \equiv -1 \pmod{4} \\ 0 & \text{if } n \equiv 0, 2 \pmod{4}. \end{cases}$$

Then $L(\chi_4, s) = \sum_{n \geq 1} \chi_4(n) n^{-s}$ is an example of an L -function.

By understanding properties of the functions $\zeta(s)$ and $L(\chi_4, s)$, we will prove that there are infinitely many primes that are 1 modulo 4, and infinitely many primes that are 3 modulo 4. I.e., we will answer Problem 1.2 for $m = 4$. We will handle the general case by studying other L -functions.

1.3. Modular forms and counting with quadratic constraints. Fix a positive integer k . The next type of question we will answer is how to count the number of $v = (v_1, v_2, \dots, v_k) \in \mathbf{Z}^k$ with a fixed distance to the origin.

For a positive integer k and a non-negative integer n , define

$$r_k(n) = \#\{(v_1, \dots, v_k) \in \mathbf{Z}^k : \sum_{i=1}^k v_i^2 = n\}.$$

This is the number of ways of writing n as the sum of k squares of integers. For example, when $k = 2$, we ask how many ways can one write n as the sum of two squares.

Problem 1.3. *Fix the positive integer k . Is there any discernible pattern for the $r_k(n)$ as the n vary? In other words, can one say something non-trivial about the generating function $\sum_{n \geq 0} r_k(n) q^n$ as a power series in the variable q ?*

It is perhaps extremely hard to guess in general, but the answer turns out to be remarkably beautiful. For example, here is a theorem when $k = 4$.

Define

$$\sigma^*(n) = \sum_{d|n, 4 \nmid d} d,$$

the sum of the divisors of n not divisible by 4.

Theorem 1.4 (Jacobi). *One has $r_4(n) = 8\sigma^*(n)$ for all n .*

It follows immediately from the Theorem that $r_4(n) \geq 1$ for all n , i.e., every non-negative integer can be written as the sum of 4 squares. This result had eluded Euler but was later proven by Lagrange.

In order to prove Jacobi's theorem, we will develop some basic properties of **modular forms**. Let

$$\mathfrak{h} = \{z \in \mathbf{C} : \operatorname{Im}(z) > 0\}$$

denote the complex upper half-plane. Let $\operatorname{SL}_2(\mathbf{R})$ denote the 2×2 matrices with determinant 1, and let $\operatorname{SL}_2(\mathbf{Z}) \subseteq \operatorname{SL}_2(\mathbf{R})$ denote the subgroup of matrices with integer entries.

The group $\mathrm{SL}_2(\mathbf{R})$ acts on $\mathfrak{h}$ via fractional linear transformations: If $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{R})$ and $z \in \mathfrak{h}$, we set $g \cdot z = \frac{az+b}{cz+d}$. This gives a (transitive) group action of $\mathrm{SL}_2(\mathbf{R})$ on $\mathfrak{h}$.

Modular forms are certain functions $f : \mathfrak{h} \rightarrow \mathbf{C}$ that

- (1) satisfy a nice differential equation;
- (2) have nice transformation properties with respect to the action of $\mathrm{SL}_2(\mathbf{Z})$.

We will make this precise later in the course. If $z \in \mathfrak{h}$ and we set $q = e^{2\pi iz}$, the generating function $\sum_{n \geq 0} r_k(n)q^n$ will turn out to be a modular form.

1.4. Galois representations and factoring polynomials. The last problem we consider is like Problem 1.1, but harder and more interesting. For reasons of time and scope, we will only consider it briefly.

Problem 1.5. Suppose $f(x) \in \mathbf{Z}[x]$ is monic and of degree n , with n -distinct complex roots $\alpha_1, \dots, \alpha_n$. For each prime number p , we can consider $f(x)$ modulo p in $\mathbb{F}_p[x]$. Let $r_p(f)$ denote the number of roots of f in $\mathbb{F}_p[x]$, so $0 \leq r_p(f) \leq n$. Is there any regularity to the $r_p(f)$ as p -varies?

If f is cubic, this question has a known, beautiful answer. (The problem is believed—but not at this point known—to have a beautiful answer in the general case.) When f is cubic and not all roots of f are real, the answer will again be related to modular forms. I will show you some numerical data to convince you of this; it is beyond the scope of this course to prove it.

More generally though, we will place Problem 1.5 in the context of **Galois representations**. Suppose $f \in \mathbf{Q}[x]$ is a polynomial, with roots $\alpha_1, \dots, \alpha_n \in \mathbf{C}$. Let $K = \mathbf{Q}(\alpha_1, \dots, \alpha_n)$ denote the subfield of $\mathbf{C}$ generated by the α_i . Let $\mathrm{Aut}(K)$ denote the automorphisms of the field K . If $\sigma \in \mathrm{Aut}(K)$, then σ permutes the α_i and is determined by its action on them. Consequently, $\mathrm{Aut}(K)$ can be realized as a subgroup of the symmetric group S_n .

In this context, a *Galois representation* is just a group homomorphism $\rho : \mathrm{Aut}(K) \rightarrow \mathrm{GL}_N(\mathbf{C})$ for some positive integer N . We will see that Problem 1.1, Problem 1.2, and Problem 1.5 can all be understood in terms of such ρ . And then *solving* these problems involves finding a (non-obvious) description of the relevant ρ .

2. TENTATIVE LECTURE SCHEDULE

Here is the *tentative* lecture schedule. The notation IR §A.B means Chapter A, section B of the textbook Ireland-Rosen. For topics that do not have a corresponding section in Ireland-Rosen, I will provide written notes or an alternate source. Also, we may discuss the topics for slightly longer than allotted on the schedule below; the *overflow* days are time to catch up.

- (1) Overview of class, the problems we'll consider
- (2) Euclidean algorithm, unique prime factorization. (IR §1.1)
- (3) Congruences (IR §3.2, §3.4); basics of quadratic residues (IR §5.1).
- (4) Cyclotomic fields (IR §6.1)
- (5) Proof of Quadratic Reciprocity (IR §6.3)
- (6) Quadratic number rings (IR §13.1)
- (7) **Monday 19 January 2026: No class (MLK day)**
- (8) Unique factorization of ideals in quadratic number rings (IR §12.2)

- (9) Statement of Dirichlet's Theorem, Dirichlet density. Infinitely many primes 1, 3 modulo 4. (IR §16.1, §16.2)
- (10) Dirichlet L -functions; overview of proof of Dirichlet's theorem, characters of finite abelian groups (IR §16.3)
- (11) Properties of $L(\chi, s)$ for quadratic χ . (*Replacing* IR §16.5, Theorem 2, with a different argument.)
- (12) Primer 1 on complex analysis
- (13) Primer 2 on complex analysis
- (14) Primer on Fourier analysis
- (15) Poisson summation. Analytic continuation and functional equation of $\zeta(s)$.
- (16) **Monday 9 February 2026: Midterm Exam**
- (17) Non-vanishing of $L(\chi, 1)$. Completion of proof of Dirichlet's theorem. (IR §16.4.)
- (18) *Overflow day*
- (19) **Monday 16 February 2026: No class (Presidents Day)**
- (20) Action of $\mathrm{SL}_2(\mathbf{R})$ on $\mathfrak{h}$; definition of modular forms; Eisenstein series as examples
- (21) Fourier expansion of modular forms
- (22) Proof of Sturm bound for modular forms, part 1
- (23) Proof of Sturm bound for modular forms, part 2
- (24) Theta functions are modular via Poisson summation
- (25) Fourier expansion of Eisenstein series: sketch of proof
- (26) Jacobi's theorem
- (27) *Overflow day*
- (28) Factoring cubic polynomials, examples and data
- (29) Decomposition groups, Frobenius, Galois representations
- (30) Examples of Galois representations

3. ASSESSMENT

Because the course will prove substantial theorems over several weeks, I can't exactly test you on lecture material. Instead, Exams will cover material that is an almost exact subset of the homework problems and discussion section problems. That is, every exam question will be a homework question or a discussion section question from a prior week, or very similar to such¹. The homework and discussion section problems will frequently be of the following sort:

- (1) Simple applications of the results/techniques in class, to get you basic familiarity with the concepts;
- (2) Extensions of topics from lecture to prove new/different results, related to what we are discussing.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA SAN DIEGO, LA JOLLA, CA USA
Email address: `apollack@ucsd.edu`

¹However, *hints* given for the homework or discussion section question may be omitted from the exam.