

# Math 1560: Number Theory *Lecture Notes*

N. Looper

Spring 2022

These are lecture notes for Math 1560: Number Theory taught at BROWN UNIVERSITY by Nicole Looper in the Spring of 2022.

Notes last updated February 1, 2022.

## Contents

|          |   |          |
|----------|---|----------|
| <b>0</b> | <b>January 27, 2022</b>                         | <b>2</b> |
| 0.1      | Course Logistics . . . . .                      | 2        |
| 0.2      | Introduction to Number Theory . . . . .         | 2        |
| 0.2.1    | Examples of Analytic Number Theory . . . . .    | 2        |
| 0.2.2    | Examples of Algebraic Number Theory . . . . .   | 3        |
| <b>1</b> | <b>February 1, 2022</b>                         | <b>4</b> |
| 1.1      | Divisibility and Factorization . . . . .        | 4        |
| 1.2      | Euclidean and Principal Ideal Domains . . . . . | 6        |
| 1.3      | Unique Prime Factorization . . . . .            | 7        |
| 1.4      | Greatest Common Divisors . . . . .              | 8        |

## §0 January 27, 2022

### §0.1 Course Logistics

- Mostly refer to syllabus for any information that you might need.
- Midterm is planned for March 17.
- Final exam schedule can be found on CAB.

### §0.2 Introduction to Number Theory

Number theory can be split into two branches: analytic number theory and algebraic number theory.

*What is number theory?* Number theory is the study of integers and their analogues in algebraic number fields.

Prime numbers are a key focus of number theory, and the study of different properties of primes constitutes different fields of number theory:

- i. The study of their distributional properties, which is analytic number theory.
- ii. As building blocks for algebraic numbers, which is algebraic number theory.

#### §0.2.1 Examples of Analytic Number Theory

Here are some examples of analytic number theory and their statements:

- Prime Number Theorem
- Twin Prime Conjecture
- Goldbach's conjecture

**Theorem 0.1** (Prime Number Theorem)

Let  $\pi(x)$  be the number of primes between 1 and  $x$ , then

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln(x)} = 1.$$

**Conjecture 0.2** (Twin Prime Conjecture)

Twin primes are pairs of primes  $p, q$  of the form  $q = p + 2$ . Examples include  $(3, 5), (11, 13), \dots$ . The conjecture postulates that there are infinitely many twin primes.

**Conjecture 0.3** (Goldbach's conjecture)

Any positive even integer greater than 2 can be written as the sum of 2 primes.

**§0.2.2 Examples of Algebraic Number Theory**

Analyzing the factorization (rings of integers) of number fields is one topic of algebraic number theory.

**Example 0.4**

2 is prime (irreducible) in  $\mathbb{Z}$ .

Yet 2 is not prime in  $\mathbb{Z}[i]$  (the Gaussian integers). This is because

$$2 = \underbrace{(1+i)(1-i)}_{\text{associates}}$$

we have that  $(1+i) = i(1-i)$ . We also note the property that the principal ideals  $(2) = (1+i)^2$  are equal.

In this example, we say that 2 “ramifies” in the ring of integers.

Fermat's Last Theorem is another such example.

*Recall:* that a *Pythagorean triple* is a triple of the form  $a, b, c \in \mathbb{Z}_+$  such that

$$a^2 + b^2 = c^2$$

Are there examples of such numbers with different exponents (say,  $k^{\text{th}}$  powers for  $k \geq 3$ )?

**Theorem 0.5** (Fermat's Last)

There are no positive integers  $a, b, c \in \mathbb{Z}_+$  satisfying

$$a^k + b^k = c^k$$

for  $k \geq 3$ .

The answer is no! (Proved by Andrew Wiles)

**Conjecture 0.6** (*abc Conjecture, informally*)

We say *powerful numbers* are positive integers whose prime factorization contains relatively few distinct primes (appropriately weighted) with an exponent of 1.

**Example**

$2^{10}3^7$  is powerful,  $2^{10}3^75$  is powerful, 1 is powerful.

If  $a, b$  are *very powerful* coprime numbers, then  $a + b$  is predicted to be *not powerful*.

**Example 0.7**

Consider  $2^{10}$  and  $3^{15}$ . We have

$$2^{10} + 3^{15} = 14,349,931 = \underbrace{31 \cdot 462 \cdot 901}_{\text{not powerful}}$$

What about another example, like  $3^{15} + 5$ ? The *abc* conjecture also predicts that this number is not so powerful...<sup>1</sup>

## §1 February 1, 2022

Happy Lunar  
New Year! 🐰

(Thanks Qinan and Andrew for allowing me to shamelessly copy their notes.)

### §1.1 Divisibility and Factorization

We start with some commonly used notation:

**Definition 1.1** (Divisibility)

We use  $a \mid b$  to mean “ $a$  divides  $b$ ” and  $a \nmid b$  to mean “ $a$  does not divide  $b$ ”.

Now for a series of definitions:

**Definition 1.2** (Primality)

A positive integer  $p \geq 2$  is said to be prime if its only positive divisors are 1 and  $p$ .

<sup>1</sup>After lecture Jiahua: It's a prime!?

**Definition 1.3 (Positive Integers)**

$\mathbb{Z}_+$  will denote the positive integers.

**Definition 1.4 (Order)**

For a nonzero  $n \in \mathbb{Z}$  and a prime  $p$ , there is a nonnegative integer  $a$  such that  $p^a \mid n$  but  $p^{a+1} \nmid n$ . This number  $a$  is called the order of  $n$  at  $p$ , denoted by  $\text{ord}_p n$ .

For  $n = 0$ , we set  $\text{ord}_p 0 = \infty$ . We also have  $\text{ord}_p n = 0 \Leftrightarrow p \nmid n$ .

We prove a lemma as warm-up:

**Lemma 1.5 (Existence of Factorization)**

Every nonzero integer can be written as a product of primes.

*We make an exception for  $-1$ . The empty product is 1 so 1 is fine.*

*Proof.* Suppose for the sake of contradiction otherwise, that some nonzero integer can be written as a product of primes. Let  $N$  be the smallest integer greater than 2 that cannot be written as a product of primes.

$N$  had better not be a prime number itself (since then it would be a product of itself). Then we can write  $N = a \cdot b$  where  $1 < a, b < N$ .

Since we took  $N$  as the least such number that cannot be written as a product of primes,  $a$  and  $b$  which are less than  $N$  can be written as a product of primes. Then  $N$  is a product of primes since  $a$  and  $b$  individually are. This is a contradiction! Thus it had better be the case that *every* nonzero integer can be written as a product of primes.  $\square$

This is the theorem we will eventually work toward proving:

**Theorem 1.6 (Unique Factorization)**

Every nonzero integer  $n$  yields a *unique* prime factorization

$$n = (-1)^\varepsilon \cdot \prod_p p^{a(p)}, a(p) \geq 0$$

where  $\varepsilon = 0$  or  $1$ , and  $\varepsilon, a(p)$  are uniquely determined by  $n$ . Moreover, we note that  $a(p) = \text{ord}_p n$ .

## §1.2 Euclidean and Principal Ideal Domains

Before this proof, we first recall a conclusion from Math 1530:

### Lemma 1.7 (Division Lemma)

If  $a, b \in \mathbb{Z}$  and  $b > 0$ , then there exists  $q, r \in \mathbb{Z}$  such that

$$a = bq + r$$

with  $0 \leq r < b$ .

*Proof.* Consider the set

$$S = \{a - xb \mid x \in \mathbb{Z}\}$$

We note that  $S$  contains *some* positive elements. Let  $r = a - qb$  be the least nonnegative element of  $S$ .

We claim that  $0 \leq r < b$ . Suppose for the sake of contradiction otherwise, then  $r = a - qb \geq b$  gives  $a - qb - b \leq 0$  and  $a - (q+1)b \leq 0$ . Which is a contradiction since we took  $r$  to be the least nonnegative element in  $S$  and we've found such smaller element  $a - (q+1)b$ .

Then it had better be that  $0 \leq r < b$  for some  $r, q \in \mathbb{Z}$ . □

### Corollary 1.8

$\mathbb{Z}$  is a Euclidean domain, with a Euclidean function given by [lemma 1.7](#).

$R[x]$  for field  $R$  is also a Euclidean domain, with  $\lambda = \deg$ .

### Definition 1.9 (Euclidean Domain)

Let  $R$  be an integral domain.  $R$  is a Euclidean domain if there exists a function  $\lambda : R \setminus \{0\} \rightarrow \mathbb{N}$  such that if  $a, b \in R$  with  $b \neq 0$ , then there exists some  $c, d \in R$  with the property that  $a = cb + d$  with  $d = 0$  or  $\lambda(d) < \lambda(b)$ .

### Example 1.10

$\mathbb{Z}$  is a Euclidean domain with  $\lambda$  function given in [lemma 1.7](#).

### Proposition 1.11

If  $R$  is a Euclidean domain, then  $R$  is a principal ideal domain. That is, if  $I \subseteq R$  is an ideal, then  $\exists a \in R$  such that  $I = Ra = \{ra \mid r \in R\}$ .

*Proof.* Assume WLOG that  $I$  is not the trivial ideal  $I \neq (0)$ . Let  $0 \neq a \in I$  such that  $\lambda(a) \leq \lambda(b) \forall b \in I, b \neq 0$ .

We claim that  $I = (a) = Ra$ .

We know that  $Ra \subseteq I$  since  $I$  is an ideal. Let  $b \in I$ . Then  $\exists c, d \in R$  such that  $b = ca + d$  where  $d = 0$  or  $\lambda(d) < \lambda(a)$ . Now we have  $d = b - ca \in I$ , so we can't have  $\lambda(d) < \lambda(a)$ . Thus  $d = 0$ , so  $b = ca \in Ra$ .

Hence we have  $I \subseteq Ra$ . Together, we conclude that  $I = Ra$ . □

### Definition 1.12 (Principal Ideals, PIDs)

If  $I = (a)$  for some  $a \in R$ , then  $I$  is said to be a principal ideal.

$R$  is a principal ideal domain (PID) if every ideal of  $R$  is principal.

Here are some important properties of PIDs:

1. Nonunit irreducible elements are exactly the prime elements in  $R$ .

*Recall:*  $p \in R$  is irreducible if  $a \mid p \Rightarrow a$  is either a unit or an associate of  $p$ .

$p \in R$  is prime if  $p \mid ab \Rightarrow p \mid a$  or  $p \mid b$  and  $p$  is a nonzero, nonunit of  $R$ .

2. GCDs always exist in PIDs.

## §1.3 Unique Prime Factorization

We're nearly ready to prove unique factorization, after a lemma:

### Lemma 1.13

Suppose  $p$  is a prime, and  $a, b \in \mathbb{Z}$ . Then  $\text{ord}_p(ab) = \text{ord}_p a + \text{ord}_p b$ .

*Proof.* WLOG, assume  $a, b \neq 0$ . We let

$$\alpha = \text{ord}_p a$$

$$\beta = \text{ord}_p b$$

Then we have

$$a = p^\alpha \cdot c \text{ where } p \nmid c$$

$$b = p^\beta \cdot d \text{ where } p \nmid d$$

Thus,  $ab = p^{\alpha+\beta} \cdot cd$ . We have that  $p \nmid cd$  since  $p \nmid c$  and  $p \nmid d$  (we rely on the fact that if  $p$  is irreducible,  $p$  is prime). Thus we have that  $\text{ord}_p(ab) = \alpha + \beta$ .  $\square$

*Proof.* (of [theorem 1.6](#), that  $\mathbb{Z}$  is a UFD). Recall that for a nonzero  $n \in \mathbb{Z}$ , we write

$$n = (-1)^\varepsilon \prod_p p^{a(p)}, \text{ where } \varepsilon = 0 \text{ or } 1 \text{ and } a(p) \geq 0$$

Given a positive prime  $q$ , we take  $\text{ord}_q$  of both sides. By [lemma 1.13](#), this yields

$$\text{ord}_q n = \varepsilon \cdot \text{ord}_q(-1) + \sum_p a(p) \text{ord}_q(p)$$

Since we have that  $\text{ord}_q(-1) = 0$  and  $\text{ord}_q(p) = 0, \forall p \neq q$ , we've uniquely determined  $a(q)$  since  $\text{ord}_q(n) = a(q)$ . That is,  $a(q)$  is *uniquely determined* for all primes  $q$ . So  $n$  has a *unique* prime factorization.  $\square$

## §1.4 Greatest Common Divisors

### Definition 1.14

Let  $R$  be an integral domain. Then  $d \in R$  is said to be a gcd of two elements  $a, b$  if

- i)  $d \mid a$  and  $d \mid b$ ,
- ii) if  $d' \mid a$  and  $d' \mid b$ , then  $d' \mid d$ .

**Remark.** An aside for ring theory enthusiasts: gcd domains are a class of rings more general than PIDs or UFDs.

We will denote  $(a, b)$  as the gcd of  $a$  and  $b$ .

**Caution, however!** gcd's are only unique up to units.

### Example

$-5$  and  $5$  are both gcds of  $-5$  and  $10$  since  $-1$  is a unit.

We will make the convention that the gcd of 2 integers is the positive gcd, that is,  $(-5, 10) = 5$ .

An edge case is that  $\text{gcd}(0, 0) = 0$ .