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 15, 2022.

Contents

§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

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

Conjecture 0.2 (Twin Prime Conjecture)

Twin primes are pairs of primes p, q of the form $q = p + 2$. Examples include $(3, 5), (11, 13), \ldots$. 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^{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...[1]

§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 <u>prime</u> if its only positive divisors are 1 and p.

[1] 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 $\operatorname{ord}_p n$.

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

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 $a(p) = \operatorname{ord}_p n$.

§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 a 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 $r, q \in \mathbb{Z}$. $\square$

Corollary 1.8
$\mathbb{Z}$ is a Euclidean domain, with a Euclidean function given by lemma 1.7.

Definition 1.9 (Euclidean Domain)
Let R be an integral domain. R is a Euclidean domain if there exists a function $\lambda : R \setminus \{0\} \to \mathbb{N}$ 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 λ function given in lemma 1.7.

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

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 $a \in I$, then I is said to be a <u>principal ideal</u>.

R is a <u>principal ideal domain</u> (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 <u>irreducible</u> if $a \mid p \Rightarrow a$ is either a unit or an associate of p.

   $p \in R$ is <u>prime</u> 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 $a, b \in Z$. Then $\operatorname{ord}_p(ab) = \operatorname{ord}_p a + \operatorname{ord}_p b$.

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

$$\alpha = \operatorname{ord}_p a$$
$$\beta = \operatorname{ord}_p b$$

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 $\text{ord}_p(ab) = \alpha + \beta$. □

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 ord_q of both sides. By lemma 1.13, this yields

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

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. □

§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 mroe 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 $\gcd(0, 0) = 0$.

§2 February 3, 2022

§2.1 Arithmetic Functions

We look at arithmetic functions and how they act on prime numbers:

Definition 2.1 (Arithmetic Function)
An arithmetic function is a function $f : \mathbb{Z}_+ \to \mathbb{C}$.

(Typically, these are integer valued.)

Example 2.2
We have some examples of arithmetic functions:

- Euler ϕ function.
- $\tau(n)$, the counting function. It takes a positive integer and counts the number of positive divisors of n.
$$\tau(n) = \sum_{d|n} 1$$
- $\sigma(n)$, the sum of divisors function. It is the sum over all the positive divisors of n.
$$\sigma(n) = \sum_{d|n} d$$

We have some properties of these functions, like *multiplicative*, *completely multiplicative*, *additive*, *completely additive*.

Definition 2.3 (Multiplicativity)
An arithmetic function f is multiplicative if
$$f(mn) = f(m)f(n) \quad \text{whenever } (m, n) = 1$$
f is said to be totally or completely multiplicative if
$$f(mn) = f(m)f(n) \quad \forall m, n \in \mathbb{Z}_+$$
regardless of coprimality.

If f is multiplicative and $n_1, \ldots, n_k$ are positive pairwise coprime integers, then

$$f(n_1 \ldots n_k) = f(n_1)f(n_2)\ldots f(n_k).$$

A particular case that is useful is when we write

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

so that assuming multiplicativity, we have that

$$f(n) = f(p_1^{e_1})f(p_2^{e_2}) \cdots f(p_k^{e_k})$$

A common type of arithmetic function is a summatory function, namely a function f of the form

$$f(n) = \sum_{d|n} g(d), \quad \text{where } g \text{ is some arithmetic function.}$$

Food for thought: how special are summatory functions within the set of all arithmetic functions?

A special property of summatory functions is that they "inherit multiplicativity".

Lemma 2.4

If g is a multiplicative function, and

$$f(n) = \sum_{d|n} g(d) \quad \forall n,$$

then f itself is multiplicative.

Proof. Suppose $m, n \in \mathbb{Z}_+$ are coprime positive integers.

The divisors d of mn are the products $a \cdot b$ where $a \mid m$ and $b \mid n$. Each such pair a, b yields a uniquely determined produce $d = a \cdot b$. Conversely, since $(m, n) = 1$, each divisor d of mn determines a unique divisor $a = \gcd(d, m)$ and $b = \gcd(d, n)$ so that $d = a \cdot b$.

Thus there is a *bijection* between divisors of mn and m, n separately

$$d \mid mn \longleftrightarrow (a \mid m, b \mid n)$$

Thus we have

$$\begin{aligned}
f(m \cdot n) &= \sum_{d|mn} g(d) \\
&= \sum_{a|m} \sum_{b|n} g(ab) \\
&= \sum_{a|m} \sum_{b|n} g(a)g(b) \\
&= \left(\sum_{a|m} g(a) \right) \left(\sum_{b|n} g(b) \right) = f(m) \cdot f(n)
\end{aligned}$$

Thus completes the proof that f is multiplicative. $\square$

Recall: The functions introduced earlier

$$\tau(n) = \sum_{d|n} 1 \qquad \sigma(n) = \sum_{d|n} d$$

So τ is the summatory function of the constant 1 functions, and σ is the summatory function of the identity function. We know that the constant 1 function and the identity function are both completely multiplicative, so σ and τ are multiplicative functions.

The implication of which is that it suffices to apply τ and σ on prime powers and multiply.

Let p be a prime. Then

$$\tau(p^e) = e + 1 \quad (\text{from } p^0 \text{ to } p^e).$$

We also have

$$\sigma(p^e) = 1 + p + p^2 + \cdots + p^e = \frac{p^{e+1} - 1}{p - 1}$$

Therefore, if $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then

$$\tau(n) = \prod_{i=1}^{k} (e_i + 1)$$
$$\sigma(n) = \prod_{i=1}^{k} \left(\frac{p_i^{e_i+1} - 1}{p_i - 1} \right).$$

Remark 2.5. There are higher order divisor functions

$$\sigma_k(n) = \sum_{d|n} d^k$$

so $\sigma_0 = \tau, \sigma_1 = \sigma, \ldots$

§2.2 Review of $\mathbb{Z}/n\mathbb{Z}$ and its units

Definition 2.6 (Modular Congruence)
If $a, b, m \in \mathbb{Z}$, $m \neq 0$, we say that a is congruent to b modulo m if $m \mid b - a$. We write

$$a \equiv b \mod m, \text{ or more simply } a \equiv b \ (m)$$

Congruence mod m is an equivalence relation on $\mathbb{Z}$. If $a \in \mathbb{Z}$, $\overline{a}$ denotes the set of integers congruent to $a \mod m$, i.e. $\overline{a} = \{a + km \mid k \in \mathbb{Z}\}$.

Definition 2.7 ($\mathbb{Z}/m\mathbb{Z}$, Residues mod m)
The set of congruence classes mod m is denoted $\mathbb{Z}/m\mathbb{Z}$. This is a quotient ring of the ring of integers $\mathbb{Z}$.

If $\overline{a}_1, \overline{a}_2, \ldots, \overline{a}_m$ form a complete set of congruence classes mod m, then the set of integers $\{a_1, a_2, \ldots, a_m\}$ is called a complete set of residues mod m.

$\mathbb{Z}/m\mathbb{Z}$ can be endowed with the structure of a commutative ring by setting

$$\overline{a} + \overline{b} = \overline{a+b}$$
$$\text{and } \overline{a} \cdot \overline{b} = \overline{ab},$$

and proving that this is well-defined as ring operations.

Proposition 2.8
The set of units in $\mathbb{Z}/m\mathbb{Z}$ is exactly

$$\{\overline{a} \mid (a, m) = 1\}$$

Proof. Let $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, then

$$\exists \overline{b} \in \mathbb{Z}/m\mathbb{Z} \text{ s.t. } \overline{b} \cdot \overline{a} \equiv 1 \mod m$$
$$\iff \exists b, n \in \mathbb{Z} \text{ s.t. } ba - mn = 1$$

Then by Bézout's identity...

$$\iff (a, m) = 1$$

□

§2.3 The Euler ϕ Function

For $n \in \mathbb{Z}_+$, $\phi(n)$ is defined to be the number of integers $1 \le m \le n$ coprime to n.

Example 2.9
We have some examples of the Euler ϕ functions:

$$\phi(1) = 1$$
$$\phi(p) = p - 1 \text{ for any prime } p$$

Let $e \geq 1$,

$$\phi(p^e) = p^e - p^{e-1} \text{ for prime powers, we exclude multiples of } p$$

Wouldn't be great if ϕ were multiplicative? It is!

Theorem 2.10

If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.

Proof. By the Chinese Remainder Theorem[2], $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ if $(m, n) = 1$.

Taking the unit groups on both sides, we have

$$(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$$

and the Euler ϕ function is simply measuring the order of said unit groups ($\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$). □

Here is an important fact about the Euler ϕ function:

Proposition 2.11

We have

$$\sum_{d|n} \phi(d) = n.$$

Proof. (1: a cute, snazzy proof) Consider the n rational numbers

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, \frac{n}{n} = 1$$

and reduce all to lowest terms so that the numerator and denominator are coprime.

Q: Given a positive divisor d of n, how many fractions have d as the denominator?

A: We have exactly $\phi(d)$ of them.

Conversely, every denominator d is certainly a divisor of n. So we conclude that $n = \sum_{d|n} \phi(d)$. □

Proof. (2: using what we've learnt) We use the fact that ϕ is multiplicative, and that this function is a summatory function of ϕ, so this function itself is multiplicative. We can decompose this into prime powers. So it suffices to show this for prime powers.

[2]This is an easy way to prove this assuming Math 1530 (Abstract Algebra). There is another way to prove this with one hand tied behind the back, it just takes more mental muscle to do.

Let $n = p^k$. Let

$$f(n) = \sum_{[} d \mid n]\phi(d).$$

Then we have

$$f(p^k) = \sum_{d|p^k} \phi(d) = 1 + (p-1) + (p^2 - p) + \cdots + (p^k - p^{k-1})$$

which is a telescoping sum which leaves

$$= p^k$$

which is as intended. □

§3 February 8, 2022

§3.1 Dirichlet Convolutions

Definition 3.1 (Dirichlet Convolution)

Let f, g be arithmetic functions. Then the Dirichlet convolution/product of g and g it

$$\begin{aligned}(f * g)(n) := &\sum_{d_1 d_2 = n} f(d_1) g(d_2) \\ = &\sum_{d|n} f(d) g(n/d)\end{aligned}$$

We do check that this has properties that we want it to have, like associativity:

$$\begin{aligned}((f * g) * h)(n) &= (f * (g * h))(n) \\ &= \sum_{d_1 d_2 d_3 = n} f(d_1) g(d_2) h(d_3)\end{aligned}$$

It is also clearly commutative.

We also have that this product has a multiplicative identity.

Definition 3.2

Let $I : \mathbb{Z}_+ \to \{0, 1\}$ be given by

$$I(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

Then I is an identity for $*$, in the sense that $f * I = I * f = f$.

Lemma 3.3

If f is an arithmetic function such that $f(1) \neq 0$, then there exists an arithmetic function g such that $f * g = I$.

It is given recursively by

$$\begin{aligned} g(1) &= \frac{1}{f(1)} \\ g(n) &= -\frac{1}{f(1)} \cdot \sum_{d|n, d<n} g(d) f(n/d) \end{aligned}$$

Proof. We want to show that given g and g defined as above, we have that $f * g = I$.

$n = 1$:

$$g(1) \cdot f(1) = \frac{1}{f(1)} f(1) = 1$$

$n > 1$:

$$\begin{aligned} \sum_{d|n} g(d) f(n/d) &= g(n) \cdot f(1) + \sum_{d|n, n<n} g(d) f(n/d) \\ &= -\frac{1}{f(1)} \cdot \sum_{d|n, d<n} g(d) f(n/d) \cdot f(1) + \sum_{d|n, n<n} g(d) f(n/d) \\ &= 0 \end{aligned}$$

So g is indeed an inverse of f since they produce the identity function I. □

§3.2 Möbius Inversion

The motivation of this is: given a summatory function of multiplicative functions, can we recover the multiplicative function?

Definition 3.4 (Möbius μ Function)

We define $\mu : \mathbb{Z}_+ \to \{-1, 0, 1\}$ given by

$$\mu(n) = \begin{cases} (-1)^k & \text{if } n = p_1 p_2 \dots p_k \text{ if } p_i \text{ are pairwise distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

(We note that $\mu(1) = 1$.)

Lemma 3.5

μ is a multiplicative function.

Proof. Let $m, n \in \mathbb{Z}_+$ such that $(m, n) = 1$. We write

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
$$n = q_1^{f_1} q_2^{f_2} \cdots q_l^{f_l}$$

Case 1 Some exponent e_i or $f_i \geq 2$. Then we have that

$$\mu(mn) = \mu(m)\mu(n) = 0$$

Case 2 We have that

$$m = p_1 p_2 \cdots p_k$$
$$n = q_1 q_2 \cdots q_l$$

where p_i and q_i are all pairwise distinct. Then $\mu(m) = (-1)^k$ and $\mu(n) = (-1)^l$, so $\mu(m) = \mu(n) = (-1)^{k+l}$.

Since these are coprime $(m, n) = 1$, then we have that $\mu(mn) = (-1)^{k+l}$.

Which is as intended, giving that μ is a multiplicative function. $\square$

Lemma 3.6

We have the property:

$$\sum_{d|n} \mu(d) = 0 \qquad \forall n \geq 2.$$

Which tells us that the summatory function of μ is I.

Proof. We define

$$f(n) := \sum_{d|n} \mu(d) \qquad \text{is multiplicative}$$

We check this on prime powers, for prime p and $e \geq 1$:

$$\begin{aligned} f(p^e) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) \\ &= 1 - 1 + 0 + \cdots + 0 = 0 \end{aligned}$$

so we're done since f is multiplicative and is 0 for all power of primes. $\square$

Lemma 3.7

Let $i : \mathbb{Z}_+ \to \{1\}$ be the constant 1 function.

$$i * \mu = \mu * i = I$$

Proof. In the case of $n = 1$, we have $i(1)\mu(1) = 1$.

For $n > 1$, we have $(i * \mu)(n) = \sum_{d|n} \mu(d) = 0$ from above. □

We see here that summatory functions can be seen as Dirichlet products: the summatory function F of f is $F = f * i$. What we said about summatory functions being multiplicative boils down to Dirichlet convolutions preserving multiplicativity.

Recall: that summatory functions inherit multiplicativity. In fact, this holds for Dirichlet products as well. If f, g are multiplicative, then so is $f * g$.

The proof is parallel to the proof for summatory functions, for lemma 2.4.

Theorem 3.8 (Möbius Inversion)

Let

$$F(n) = \sum_{d|n} f(d)$$

Then we have

$$f(n) = \sum_{d|n} \mu(d) \cdot F(n/d) = \mu * F.$$

Proof. $F = f * i$, then

$$F * \mu = (f * i) * \mu = f * (i * \mu) = f * I = f.$$

which was simpler than I expected... □

Corollary 3.9

If F is the summatory function of f, and F is multiplicative, then f is also multiplicative, as $f = \mu * F$ and μ is multiplicative and convolutions with multiplicative functions are multiplicative.

Corollary 3.10

Corollary 3.9 gives another proof that ϕ is multiplicative, as

$$\sum_{d|n} \phi(d) = \phi * i = \mathrm{id}.$$

§3.3 Applications of Möbius Inversion

§3.3.1 Cyclotomic Polynomials

Recall: the n^{th} cyclotomic polynomial $\Phi_n(x)$ is the unique irreducible polynomial in $\mathbb{Z}[x]$ dividing $x^n - 1$ but no $x^k - 1$ for $k < n$.

Thus

$$\Phi_n(x) = \prod_{\substack{1 \le k < n \\ (k,n)=1}} \left(x - e^{2\pi i k/n}\right)$$

as the roots of this polynomial are exactly the primitive n^{th} roots of unity. We have that

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

By Möbius inversion, if

$$G(n) = \prod_{d|n} g(d),$$

then we have that

$$g(n) = \prod_{d|n} G(d)^{\mu(n/d)}$$

In particular, taking $G(n) = x^n - 1$ (with particular $x \in \mathbb{C}$) as an arithmetic function, we have

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} \qquad (x \in \mathbb{C})$$

Applying this identity for enough $x \in \mathbb{C}$ yields this as an identity of polynomials.

§3.3.2 Dynatomic Polynomials

The roots of cyclatomic polynomials are roots of unity. Dynatomic polynomials have as roots the periodic points (of certain periods) of a polynomial.

Definition 3.11

Let K be a field, and let $f \in K[x]$ of degree $d \geq 2$. Let

$$f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}$$

then $P \in \overline{K}$[a] is said to be periodic under f if

$$f^n(P) = P \qquad \text{for some } n \geq 1$$

[a] Algebraic numbers in field K, the field you get by adjoining all roots of polynomials in $K[x]$.

Example 3.12

Let $f(x) = x^2 - 1$. 0 is a period point under f:

$$0 \longmapsto -1 \longmapsto 0$$

and its period is 2.

> **Remark.** If n is the smallest positive integer such that $f^n(p) = p$ (p periodic), then we call n the exact period of p under f.

Definition 3.13

The n^{th} dynatomic polynomial of f is

$$\Phi_{f,n}(x) := \prod_{d|n} \left(f^d(x) - x\right)^{\mu(n/d)}$$

We hope that $\Phi_{f,n}(x)$ has as its roots the points of exact period n... This hope is dashed...

Example 3.14

$f(x) = x^2 - \frac{3}{4}$.

$$f^2(x) - x = \left(x - \frac{3}{2}\right)\left(1 - \frac{1}{2}\right)^3$$
$$f(x) - x = \left(x - \frac{3}{2}\right)\left(x + \frac{1}{2}\right)$$

Thus

$$\frac{f^2(x) - x}{f(x) - x} = \left(x + \frac{1}{2}\right)^2$$

But $x = -\frac{1}{2}$ is fixed under f.

§4 February 10, 2022

§4.1 Congruences *continued*

Recall: that for $m \in \mathbb{Z}_+$, $a, b \in \mathbb{Z}$, the linear congruence

$$ax \equiv b \mod m$$

has a solution if and only if $(a, m) \mid b$. Unwinding this gives Bezout's identity.

Q: How do we actually find a solution?

A: Either guess and check; or apply the following algorithm:

1) Divide all terms in the congruence by $d = (a, m)$.

2) If step 1 yields
$$a'x \equiv b' \mod m'$$
with $(a', m') = 1$, then $d := (a', b')$ is a unit mod m', so we can divide both sides by d'.
$$a'd'^{-1}x \equiv b'd'^{-1} \mod m'$$

3) Let $a''x \equiv b'' \mod m$ be the result so far. We replace b'' by some $b'' + km'$[3] such that $(a'', b'' + km') > 1$ allows us to repeat step 2. This results in some a''' such that $|a'''| < |a''|$.

   Given that we repeat this process, this must eventually terminate, since the absolute values of the a terms are strictly decreasing each time.

Example 4.1
Let $10x \equiv 6 \mod 14$.

1) $(a, m) = (10, 14) = 2$ so we divide through by 2.
$$5x \equiv 3 \mod 7$$

2) Irrelevant since $(5, 3)$ are coprime.

3) Consider integers of form $3 + 7k$, and see which are divisible by 5. We can take $k = 1$. We

[3] Since made a' and m' coprime, we have $(a', m') = 1$ so we can indeed solve congruence $a''q \equiv b'' + km'$ gives noncoprime pairs.

get

$$5x \equiv 10 \mod 7$$

2) Divide by $(5, 10) = 5$ so we have $x \equiv 2 \mod 7$.

§4.2 Simultaneous Linear Congruences

Recall: the CRT/Sun-tzu's theorem.

Theorem 4.2 (Sun-tzu's Theorem / Chinese Remainder Theorem)
Suppose that $m = m_1 m_2 \cdots m_t$ with $(m_i, m_j) = 1 \forall i \neq j$.

Let $b_1, b_2 \ldots, b_t$ be integers, and consider the system of congruences

$$\begin{aligned} x_1 &\equiv b_1 \mod m_1 \\ x_2 &\equiv b_2 \mod m_2 \\ &\vdots \\ x_t &\equiv b_t \mod m_t \end{aligned} \tag{*}$$

Then this system has a unique solution modulo m[a].

[a]That is, we have at least one solution, and we can shift it by *any* multiple of m.

Proof. Let $n_i = m_1 m_2 \cdots \cancel{m_i} \cdots m_t = \frac{m}{m_i}$ for each i. Since m_i is coprime to m_j, $\forall j \neq i$, we have $(n_i, m_i) = 1 \forall i$. Then, there exists solutions $r_i, s_i \in \mathbb{Z}$ such that

$$r_i m_i + s_i n_i = 1$$

Let $e_i = s_i n_i$. Then for each i,

$$e_i \equiv 1 \mod m_i$$

and $e_i \equiv 0 \mod m_j$, $\forall j \neq i$.

Our goal is to ultimately show

$$\mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_t\mathbb{Z}$$

with each e_i generating the "$\mathbb{Z}/m_i\mathbb{Z}$ piece".

Set

$$x_0 = \sum_{i=1}^{t} b_i e_i$$

so that $x_0 \equiv b_i \pmod{m_i} \forall i$, so x_0 is a solution to eq. (*).

Suppose x_1 is another solution. Then we have

$$x_1 - x_0 \equiv 0 \mod m_i \ \forall i, 1 \leq i \leq t$$

Since the m_i are pairwise coprime, we get $m \mid x_1 - x_0$. $\square$

§4.3 Structure of Unit Groups

Recall: in Math 1530, we learned Lagrange's theorem

Theorem 4.3 (Lagrange's Theorem)
If G is a finite group, then for every subgroup H of G, we have $|H| \mid |G|$.

Corollary 4.4
If G is a finite group of order n, and $a \in G$, then $a^n = e$, where e is the identity of the group.

We've seen that $|U(m)| = \phi(m)$.[4] Applying Lagrange's theorem, we have Euler's theorem:

Theorem 4.5 (Euler's Theorem)
For any $a \in \mathbb{Z}$ with $(a, m) = 1$, we have $a^{\phi(m)} \equiv 1 \mod m$.

Definition 4.6
A subset R of $\mathbb{Z}$ is said to be a reduced set of residues mod m if R contains exactly one element from each of the $\phi(m)$ congruence classes that are units mod m.

Alternate proof of theorem 4.5. Let $R = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ be a reduced set of residues mod m. If $(a, m) = 1$, then aR is also a reduced set of residues mod m. Thus, if $x_1, x_2, \ldots, x_{\phi(m)} \in aR$ (pairwise distinct), then

$$\begin{aligned} x_1 x_2 \cdots x_{\phi(m)} &\equiv r_1 r_2 \cdots r_{\phi(m)} \mod m \\ (ar_1)(ar_2) \cdots (ar_{\phi(m)}) &\equiv r_1 r_2 \cdots r_{\phi(m)} \mod m \\ a^{\phi(m)}(r_1 r_2 \cdots r_{\phi(m)}) &\equiv r_1 r_2 \cdots r_{\phi(m)} \mod m \end{aligned}$$

since all the r_i are units mod m, we divide through

$$a^{\phi(m)} \equiv 1 \mod m$$

Which is as desired. $\square$

[4] For notation, we use $U(m) := (\mathbb{Z}/m\mathbb{Z})^\times$.

We'll be studying roots of polynomials over $\mathbb{Z}/m\mathbb{Z}$, especially polynomials of the form $x^d - a$.

By Sun-tzu's theorem, the case of m being a prime power is especially important. This turns out to have a lot to do with the case that $m = p$ is a prime itself.

First something further *afield*:

Proposition 4.7

If p is a prime and $p \nmid d$ for $d \in \mathbb{Z}_+$, then the polynomial

$$x^d - a \in (\mathbb{Z}/p\mathbb{Z})[x], \qquad a \not\equiv 0 \mod p$$

has exactly d roots in some extension of $\mathbb{F}_p$.

Conversely, if $p \mid d$, then there are fewer than d roots in any extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

The proof uses the following proposition:

Proposition

A nonzero polynomial $f \in K[x]$ is separable if and only if it is relatively prime to its derivative f'. (A separable polynomial whose roots in its algebraic closure $\overline{K}$ whose roots are all distinct).

Proof.

$\Rightarrow$ **Right Direction:** Suppose f is separable and α be any root of f. Then $f(x) = (x - \alpha)h(x)$, where $h(\alpha) \neq 0$ since α is a non-repeated root.

We have $f'(\alpha) = h(\alpha) \neq 0$, so α is not a root of f'. Thus f and f' have no common roots, so they are coprime.

$\Leftarrow$ **Left Direction:** Prove by contrapositive. Suppose f is not separable. i.e. it has some repeated root which we call α.

Then $f(x) = (x - \alpha)^2 g(x)$, so $f'(x) = (x - \alpha)^2 g'(x) + 2(x - \alpha)g(x)$. We see that $x - \alpha$ divides both f and f' so $(f, f') \neq 1$.

Which concludes the bidirectional. $\square$

Proof of proposition 4.7. We have $f(x) = x^d - a$, $a \not\equiv 0 \pmod p$ has d distinct solutions in some extension of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, because

$$f'(x) = dx^{d-1} \pmod p$$

and with 0 as its only root but 0 is not a root of f. By above we have that f is separable.

Conversely, if $p \mid d$, then

$$f'(x) \equiv 0 \pmod p,$$

so $(f, f') \neq 1$, meaning that f is not separable. □

Proposition 4.8 (4.1.2 of text)
If p is a prime and if $d \mid p-1$, then the polynomial

$$x^{d-1} \in (\mathbb{Z}/p\mathbb{Z})[x]$$

has exactly d roots in the base field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proof. We know this is true in the case of $d = p-1$ because of Fermat's Little Theorem (also Euler's Theorem).

We also note that $(x^d - 1) \mid (x^{p-1} - 1)$. Since $x^{p-1} - 1$ has all roots in the base field by FLT, $x^d - 1$ had better also retain its roots in the base field $\mathbb{F}_p$ by contradiction. □

§5 February 15, 2022

§5.1 Cyclicity of Groups

§5.1.1 mod odd p

Recall: from last class, we had proposition 4.8:

Proposition
If p is a prime and if $d \mid p-1$, then the polynomial

$$x^{d-1} \in (\mathbb{Z}/p\mathbb{Z})[x]$$

has exactly d roots in the base field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Corollary 5.1
$G := (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.

Proof. For $d \mid (p-1)$, we write $\psi(d)$ for the number of elements of G having order d.

Proposition 2 implies that[5]

$$\sum_{c|d} \psi(c) = d \qquad (\psi * i = \text{id}, \psi = \text{id} * \mu)$$

Möbius inversion gives

$$\psi(d) = \sum_{c|d} \mu(c) \frac{d}{c}.$$

On the other hand, we have $\text{id} = \phi * i \Rightarrow \phi = \mu * \text{id}$. Thus $\psi(d) = \phi(d)$ for all $d \mid (p-1)$. So in particular, $\psi(p-1) = \phi(p-1) \geq 1$ for any prime p. $\square$

§5.1.2 mod odd power p^e

Theorem 5.2

Let $p \in \mathbb{Z}_+$ be an odd prime, and let $e \geq 1$. Then $U(p^e)$ is cyclic.

Proof overview:

1. Pick a primitive root mod p. We call it g (for generator).

2. Show that either g or $g + p$ is a primitive root mod p^2.

3. Show that if h is any primitive root mod p^2, then h is a primitive root mod p^e $\forall e \geq 2$.

Proof of theorem 5.2.

Step 1. Let g be a primitive root modulo p given by corollary 5.1.

Step 2. Let d be the order of g mod p^2. Since $\phi(p^2) = p(p-1)$, we have that

$$d \mid p(p-1) \qquad \text{by Lagange.}$$

By definition of d,

$$g^d \equiv 1 \mod p^2$$

so we also have

$$g^d \equiv 1 \mod p$$

Thus $(p-1) \mid d$ since g has order $p-1$ mod p. Altogether, d is either $p-1$ or $p(p-1)$. If $d = p(p-1)$, then we are done with step 2. So we assume the former that $d = p-1$.

Let $h = g + p$. We know that h is a primitive root mod p, so we do the same [yoga] as above and conclude that the order of h mod p^2 is either $p-1$ or $p(p-1)$.

[5] We throw in Lagrange's theorem, and essentially count the number of solutions to $x^d \equiv 1$.

By our new hypothesis,

$$g^{p-1} \equiv 1 \pmod{p^2}$$

so modulo p^2, we have

$$h^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \cdots + p^{p-1}$$

Modulo p^2, the only terms that survive are (expand and all p^2 terms die):

$$\equiv 1 - pg^{p-2} \pmod{p^2}$$

But $p \nmid g$, so $pg^{p-2} \not\equiv 0 \mod p$, and hence $h^{p-1} \not\equiv 1 \mod p^2$. Thus the order of h mod p^2 is $p(p-1)$, so h generates $U(p^2)$.

So we are done with step 2. If g is a primitive root mod p, then either g or $g+p$ is a primitive root mod p^2.

Step 3. We wish to show that a primitive root mod p^2 is also a primitive root mod p^e $\forall e \geq 2$. We induct on e.

Let h be a primitive root mod p^e for some fixed $e \geq 2$. Let d be the order of h mod p^{e+1}. By Lagange, we have that $d \mid \phi(p^{e+1}) = p^e(p-1)$, and from step 2,

$$\phi(p^e) = p^{e-1}(p-1) \mid d$$

Hence $d = p^e(p-1)$ or $p^{e-1}(p-1)$. If it's the former then we are done, so we assume latter.

We want to show that

$$h^{p^{e-1}(p-1)} \not\equiv 1 \mod p^{e+1}$$

implying that $d = p^e(p-1)$ after all.

Since h has order $\phi(p^e) = p^{e-1}(p-1)$ in $U(p^e)$, we have

$$h^{p^{e-2}(p-1)} \not\equiv 1 \mod p^e \tag{$\star$}$$

However,

$$h^{p^{e-2}(p-1)} \equiv 1 \mod p^{e-1} \tag{$\star\star$}$$

Combining eq. ($\star$) and eq. ($\star\star$) yields

$$h^{p^{e-2}(p-1)} = 1 + kp^{e-1}$$

where $p \nmid k$. Therefore, we have

$$\begin{aligned} h^{p^{e-1}(p-1)} &= (1+kp^{e-1})^p \\ &= 1 + pkp^{e-1} + \binom{p}{2}k^2p^{2e-2} + \cdots \end{aligned}$$

Subsequent terms are all divisible by $p^{3e-3} = (p^{e-1})^3$, and hence divisible by p^{e+1} as $e(e-1) \geq 2+1$ $\forall e \geq 2$. Thus

$$h^{p^{e-1}(p-1)} = 1 + kp^e + \frac{1}{2}k^2p^{2e-1}(p-1) \mod p^e + 1$$

p is odd, so
$$\frac{1}{2}k^2p^{2e-1}(p-1)$$
is divisible by p^{e+1}, since $2e-1 \geq e+1$. Thus
$$h^{p^{e-1}(p-1)} \equiv 1 + kp^e \mod p^e + 1$$
Since $p \nmid k$, we get that $kp^e \not\equiv 0$ so
$$h^{p^{e-1}(p-1)} \not\equiv 1 \mod p^e + 1$$
This proves that $d = p^e(p-1)$, which is to say that h is a primitive root mod p^{e+1}.

Altogether, we have that $U(p^e)$ is cyclic. □

§5.1.3 mod powers of 2

Theorem 5.3
$U(2^e)$ is cyclic iff $e = 1$ or $e = 2$.

Proof. Clearly $U(2)$ and $U(4)$ are cyclic[6].

We show that $U(2^e)$ is *not* cyclic for all $e \geq 3$. Notice: it suffices to show that $U(8)$ is not cyclic, since we can find group homomorphisms down powers of 2.
$$U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$
and $\overline{1}^2 = \overline{3}^2 = \overline{5}^2 = \overline{7}^2 \mod 8$. □

§5.2 Classification of all cyclic unit groups

Corollary 5.4
$U(m)$ is cyclic if and only if $m = 1, 2, 4, p^e$ or $2p^e$ for some odd prime p.

Proof. Recall that a product G of finite cyclic groups G_1 and G_2 is cyclic iff $(|G_1|, |G_2|) = 1$.[7] On the other hand, $\phi(m)$ is even $\forall m \geq 3$. So only one of G_1 and G_2 needs odd power.

Combined with our structure theorems on $U(p^e)$ for primes p, this proves the corollary since these are the only possibilities. □

[6] We don't have much choice since there is only one trivial group and one group of order 2, both cyclic.
[7] Secretly, Chinese Remainder Theorem.