Supplementary Materials for Chapter II

Xu Gao

MATH 110 | Introduction to Number Theory | Summer 2023

June 28, 2023

Prerequisites

In order to succeed in this course, it is important to meet the following prerequisites:

(a). familiar with the style of proof-based mathematics;

(b). have a good understanding of proof formats and methods;

(c). have basic knowledge of set theory and combinatorics, which are covered in Math 100;

(d). solid grasp of lower division math courses, such as calculus and linear algebra.

In addition, you will meet some concepts which will be explored in greater depth in later courses. They will be used as terminology, and you should have ability to unpackage the abstract definitions.

What to expect in this document?

Definition important concepts which are not explicitly covered in the lectures. You are expected to be proficient in them.

Convenience conveniences used in this course. You should be able to reconginize them without mention.

Terminology useful terminology which are concepts from other courses. You are expected to be able to translate these terms into your own words, even without an in-depth understanding of the relevant theory.

Exercise non-mandatory exercises for practice and self-assessment. Highly recommended.

Further reading reading materials for further interest.

Problem homework problems and challenge problems.

† contents with † mark may be too deep or too off-topics.

Chapter II
Prime Numbers

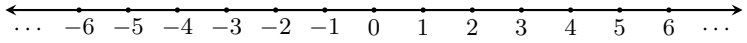
1 Hasse diagram

Terminology 1.1. Given an ordered set $(S, \preccurlyeq)$, we can illustrate the partial order by a *Hasse diagram*:

- the nodes are the elements of S, listed from smaller to larger;
- if two elements a, b are *adjacent*, namely $a \preccurlyeq b$ and there is no other elements c between them ($a \preccurlyeq c$ and $c \preccurlyeq b$), we draw an arrow (omitting the head) from a to b.

We can read out the partial order from the Hasse diagram as follows: $a \preccurlyeq b$ if and only if there is a path from a to b.

Exercise 1.1. Consider the set of integers $\mathbb{Z}$ equipped with the usual order $\leqslant$, show that the Hasse diagram looks as follows:



Exercise 1.2. In the definition of Hasse diagram, we implied assumed that every pair (a, b) with the partial order relation $a \preccurlyeq b$ can be decomposed into a chain of adjacent ones:

$$a = x_0 \preccurlyeq x_1 \preccurlyeq \cdots \preccurlyeq x_n = b.$$

However, this is NOT true in general: show that in $(\mathbb{R}, \leqslant)$, every pair $a \leqslant b$ is NOT adjacent.

Terminology 1.2. A partial order $\preccurlyeq$ on a set S is called a *linear order* if every two elements of S is comparable: namely, either $a \preccurlyeq b$ or $b \preccurlyeq a$. If this is the case, we say $(S, \preccurlyeq)$ is a *linear ordered set*.

Exercise 1.3 (†)**.** If an ordered set $(S, \preccurlyeq)$ is linear ordered set (and if it has a Hasse diagram), then we can assemble its Hasse diagram as a line (for example, exercise 1.1). To see this, show that there is no *branch* in the Hasse diagram, namely for every element $a \in S$, there can be at most one inward edge and one outward edge adjacent to a.

2 Primes

Terminology 2.1. A *unit* in an abelian monoid $(M, *, e)$ is an invertible element.

Example 2.2.
- The only unit in $(\mathbb{Z}_+, \cdot, 1)$ is 1.
- The only unit in $(\mathbb{N}, +, 0)$ is 0.
- In $(\mathbb{Z}, \cdot, 1)$, there are two units: 1 and -1.
- In $(\mathbb{Z}, +, 0)$, every element is a unit.

Terminology 2.3. Let a, b be two elements in an abelian monoid $(M, *, e)$. We say a *divides* b, a is a *divisor* of b, or b is *divided by* a, if there is an element $c \in M$ such that $b = a * c$. We will use $a \mid b$ to denote this. (*Warn*: distinguish this with the divisibility of integers, which is an example of the above notion.)

Exercise 2.1. Show that in $(\mathbb{N}, +, 0)$, we have $a \mid b$ if and only if $a \leqslant b$.

Exercise 2.2 (†)**.** Show that, if the monoid $(M, *, e)$ has only one unit, then $\cdot \mid \cdot$ is a partial order on it.

Terminology 2.4. An element p in an abelian monoid $(M, *, e)$ is a *prime* if

- p is not the neutral e,
- p is not a unit, and
- whenever $p = a * b$ with $a, b \in M$, we necessarily have one of a, b being a unit.

Example 2.5.

- Prime elements in $(\mathbb{Z}_+, \cdot, 1)$ are prime numbers.
- Prime elements in $(\mathbb{Z}, \cdot, 1)$ are prime numbers and their negations.
- The only prime elements in $(\mathbb{N}, +, 0)$ is 1.

Terminology 2.6. Let a, b be two elements in an abelian monoid $(M, *, e)$. We say a, b are *associated*, denoted by $a \sim b$, if both $a \mid b$ and $b \mid a$.

Exercise 2.3 (†)**.** Show that, "being associated" is an equivalent relation. Namely,

- (*reflexivity*) for all $a \in M$, $a \sim a$;
- (*symmetry*) for all $a, b \in M$, if $a \sim b$, then $b \sim a$;
- (*transitivity*) for all $a, b, c \in M$, if $a \sim b$ and $b \sim c$, then $a \sim c$.

3 Prime factorization

Convenience 3.1. We will use the following notations for *indexed sum* and *product*:

$$\begin{aligned}
\sum S &:= \text{the sum of elements of } S, \\
\sum_{a \in S} f(a) &:= \text{the sum of values of } f(a) \text{ when } a \text{ is taken over } S, \\
\prod S &:= \text{the product of elements of } S, \\
\prod_{a \in S} f(a) &:= \text{the product of values of } f(a) \text{ when } a \text{ is taken over } S.
\end{aligned}$$

Example 3.2. The prime factorization can be written as $n = \prod_{p \in \mathbb{P}} p^{e_p}$.

Convenience 3.3. When a presentation of a set S is given:

$$S = \{\text{expression} \mid \text{rule}\},$$

we usually write indexed sum and product in a more compact way:

$$\begin{aligned}
\sum_{\text{rule}} f(\text{expression}) &:= \text{the sum of values of } f(\text{expression}) \text{ when the value of expression is specified by rule}, \\
\prod_{\text{rule}} f(\text{expression}) &:= \text{the product of values of } f(\text{expression}) \text{ when the value of expression is specified by rule}.
\end{aligned}$$

Example 3.4. The prime factorization can be written as $n = \prod_{p \text{ is prime}} p^{e_p}$.

Terminology 3.5. It is worth to point out that a *sequence* and a *map* are more or less the same thing.

- A sequence $(a_1, \cdots, a_n)$ is the same as a map from the index set $\{1, \cdots, n\}$ mapping i to a_i.
- Similarly, a sequence $(a_1, \cdots)$ is the same as a map from the index set $\mathbb{Z}_+$ mapping $i \in \mathbb{Z}_+$ to a_i.
- More generally, a sequence $(x_i)_{i \in I}$ is a map from the index set I mapping $i \in I$ to x_i.
- Conversely, a map from a set I to some target set T is the same as a sequence $(x_i)_{i \in I}$ with each $x_i \in T$.

4 Translation between two worlds

The purpose of what follows is to explain the meaning of the above title.

Terminology 4.1. An *ordered monoid* is a monoid $(M, *, e)$ equipped with a partial order $\preccurlyeq$ such that for all $a, b, c \in M$, we have

$$a \preccurlyeq b \implies c * a \preccurlyeq c * b \text{ and } a * c \preccurlyeq b * c.$$

Example 4.2. We have seen the following ordered monoids

(a). $(\mathbb{Z}_+, \cdot, 1, \cdot \mid \cdot)$,

(b). $(\mathbb{N}, +, 0, \leqslant)$, and

(c). $(\mathbb{Z}, +, 0, \leqslant)$.

Terminology 4.3. You may have heard the notion *homomorphism*, that is a structure-preserving map between two algebraic structures of the same type (e.g. monoids, groups, $\mathbb{Z}$-modules, ordered sets, etc.). For example, a homomorphism between ordered monoids $f \colon (M, *, e, \preccurlyeq) \to (N, *, e, \preccurlyeq)$ is a map from M to N such that:

(a). (preserving the operation) $\forall a, b \in M : f(a * b) = f(a) * f(b)$;

(b). (preserving the neutral) $f(e) = e$;

(c). (preserving the order) $\forall a, b \in M : a \preccurlyeq b \implies f(a) \preccurlyeq f(b)$.

If a homomorphism $f \colon M \to N$ has two-side inverses (i.e. there are homomorphisms $g, h \colon N \to M$ such that $g \circ f = \mathrm{id}_M$ and $g \circ h = \mathrm{id}_N$), then it is called an *isomorphism*.

Exercise 4.1. Show that for each prime p, the function v_p gives a homomorphism between ordered monoids

$$v_p \colon (\mathbb{Z}_+, \cdot, 1, \cdot \mid \cdot) \longrightarrow (\mathbb{N}, +, 0, \leqslant)$$

Moreover, show that it is surjective but not injective. Hence, none of v_p is an isomorphism.

However, we can combine all the homomorphisms v_p. To do this, we need to first organize the (infinitely many) copies of $(\mathbb{N}, +, 0, \leqslant)$ into a single ordered monoid. The underlying set is

$$\mathbb{N}_{\mathbb{P}} := \{(e_p)_{p\in\mathbb{P}} \mid e_p \in \mathbb{N} \text{ and only finitely many of } e_p \text{ are nonzero}\}.$$

The operation is the componentwise addition:

$$(e_p)_{p\in\mathbb{P}} + (f_p)_{p\in\mathbb{P}} := (e_p + f_p)_{p\in\mathbb{P}},$$

the neutral is the zero sequence $(0)_{p\in\mathbb{P}}$, and the order is the componentwise order

$$(e_p)_{p\in\mathbb{P}} \preccurlyeq (f_p)_{p\in\mathbb{P}} \qquad \text{defined as:} \qquad \forall p \in \mathbb{P}, e_p \leqslant f_p$$

Exercise 4.2 (†)**.** Show that the above is an ordered monoid and the map

$$\mathbf{v}\colon \mathbb{Z}_+ \to \mathbb{N}_{\mathbb{P}}\colon n \mapsto (v_p(n))_{p\in\mathbb{P}}$$

is an isomorphism of ordered monoid. (Hint: use the unique prime factorization and Theorem 5.6 in the lecture.)

5 Distribution of primes

There are many ways to prove *Euclid's theorem on infiniteness of prime numbers*. If you are interested in, you can start from Wikipedia or Proof Wiki. It is worth mentioning that one method is to show the series $\sum_{p \text{ is prime}} \frac{1}{p}$ of reciprocals of prime numbers *diverges*.

The method people used to attack the *twin prime conjecture* as well as many other questions on distribution of primes is called the *Sieve theory*, a central method in *analytic number theory*.

6 Arithemtic functions

Substitution in indexed sum and product

In the lecture, we used the substitution

$$\sum_{(a,b)\in\mathscr{D}(m)\times\mathscr{D}(n)} (ab)^k = \sum_{c\in\mathscr{D}(mn)} c^k.$$

Let me explain further how substitution works in general.

In general, suppose you have an indexed sum $\sum_{a\in S} f(a)$ and you want to substitute in, say $a = g(b)$ $(b \in T)$. What you actually doing is:

(a). change the expression from $\sum_{a\in S} f(a)$ to $\sum_{b\in T} f(g(b))$;

(b). the new expression gives the same value as the old one: 1, since $g\colon T \to S$ is bijective, the summations have the same number of terms; 2, for each pair of terms $f(a)$ and $f(g(b))$ corresponding through $a = g(b)$, we know that they give the same value.

This should be fairly clear. However, it may not be obvious in practice. One thing may cause confusion is that we may want to keep the index simple and save the use of letters.

Usually a letter appears both in the expression and the rule of a set's presentation $\{\text{expression} \mid \text{rule}\}$ is a *local notation*, namely it will be released and free to serve in other usage outside this context. The same rule applies to indexed sum and product.

Example 6.1. In the following equalities, the letter a in the left and right sides are NOT the same variable:

$$\sum_{a\in\mathscr{D}(n)} f(a) = \sum_{a\in\mathscr{D}(n)} f(\frac{n}{a}),$$
$$\sum_{a\mid n} f(a) = \sum_{a\mid n} f(\frac{n}{a}).$$

Exercise 6.1. Give a bijection from $\mathscr{D}(n)$ to itself and use this bijection to justify the equalities in above example.

Another situation is when the index set consists of tuples and therefore the function $f(\cdot)$ is multi-variable. This usually comes with the previous issue.

Exercise 6.2. Give bijections between the sets

$$\{(a,b)\in\mathbb{Z}_+^2 \mid a\mid n, b\mid a\}, \left\{(a,b)\in\mathbb{Z}_+^2 \,\middle|\, a\mid n, b\mid \frac{n}{a}\right\}, \{(a,b,c)\in\mathbb{Z}_+^3 \mid abc=n\}.$$

Then use them to justify the substitutions:

$$\sum_{a\mid n, b\mid a} f(b, \frac{a}{b}, \frac{n}{a}) = \sum_{abc=n} f(a,b,c) = \sum_{a\mid n, b\mid \frac{n}{a}} f(a,b,\frac{n}{ab}).$$

Problems

Problem II.1. Let a, b and n be positive integers. `Prove` that

(a) $\gcd(a^n,b^n)=\gcd(a,b)^n$ and $\operatorname{lcm}(a^n,b^n)=\operatorname{lcm}(a,b)^n$;
(b) $\gcd(a\cdot n, b\cdot n)=\gcd(a,b)\cdot n$ and $\operatorname{lcm}(a\cdot n, b\cdot n)=\operatorname{lcm}(a,b)\cdot n$;

Problem II.2. Let a, b and n be three positive integers. If $a^n \mid b^n$, show that $a\mid b$.

Problem II.3. Write the prime factorization of $N=13!$ and then count the divisors of N (give the number, you do not need to list all of them in order to count).

Remark. Recall that for any positive integer n, we denote by $n!$ (read n **factorial**) the product of all the integers between 1 and n.

Problem II.4. Let n be any positive integer. `Prove` that there exists a positive integer k (depending on n) such that the following list of n consecutive integers:

$$k, k+1, \cdots, k+n-1$$

contains *no* prime number at all.

Hint. Use the factorial (but $k=n!$ is NOT the correct answer, start from this and try to see what are missing). You also need the *2-out-of-3* property of division.

Remark. From the problem, we can see that the gaps between consecutive prime numbers can be arbitrarily large.

Problem II.5. As in class, consider the collection of complex numbers of the form

$$\mathscr{O} := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}.$$

(a) `Prove` that the set $\mathscr{O}$ equipped with the addition and multiplication of complex numbers satisfies the following properties:

(i) $\mathscr{O}$ is closed under addition: for any $\alpha, \beta \in \mathscr{O}$, we have $\alpha + \beta \in \mathscr{O}$.

(ii) $\mathscr{O}$ is closed under negation: for any $\alpha \in \mathscr{O}$, we have $-\alpha \in \mathscr{O}$.

(iii) $\mathscr{O}$ is closed under multiplication: for any $\alpha, \beta \in \mathscr{O}$, we have $\alpha\beta \in \mathscr{O}$.

Remark. In the terms of Algebra, $\mathscr{O}$ is a *subring* of the ring $\mathbb{C}$ of complex numbers.

(b) Consider the integer-valued function N defined on $\mathscr{O}$:

$$N(a + b\sqrt{-5}) := a^2 + 5b^2.$$

`Prove` that

$$N(\alpha\beta) = N(\alpha)N(\beta)$$

for any two elements α and β in $\mathscr{O}$.

Remark. Say that an element $\alpha \in \mathscr{O}$ **divides** another element $\beta \in \mathscr{O}$, denoted by $\alpha \mid \beta$ if there is an element $\gamma \in \mathscr{O}$ such that $\beta = \alpha\gamma$. Hence, problem II.5.(b) shows that

$$\alpha \mid \beta \implies N(\alpha) \mid N(\beta).$$

(c) Say that an element $\varepsilon \in \mathscr{O}$ is a **unit** if ε divides 1. `Prove` that all the units in $\mathscr{O}$ are 1 and -1.

Hint. Assume $\varepsilon \in \mathscr{O}$ is a unit other than ± 1, then use problem II.5.(b).

(d) Say that an element $\alpha \in \mathscr{O}$ is a **prime element** if

(i) α is nonzero and not a unit;

(ii) whenever $\alpha = \gamma\delta$ with $\gamma, \delta \in \mathscr{O}$, we necessarily have one of γ, δ being a unit.

`Prove` that the following four elements are prime elements: 2, 3, $1+\sqrt{-5}$, and $1-\sqrt{-5}$.

Hint. Proceed by way of contradiction, then use problem II.5.(b).

(e) Say that two elements $\alpha, \beta \in \mathscr{O}$ are **associated** if both $\alpha \mid \beta$ and $\beta \mid \alpha$. `Prove` that none pair of the four elements 2, 3, $1 + \sqrt{-5}$, and $1 - \sqrt{-5}$ are associated.

Hint. Use the definition of *division* and problem II.5.(c).

Remark. A **prime factorization** of a nonzero element $\alpha \in \mathscr{O}$ is a representation

$$\alpha = \varepsilon p_1 \cdots p_n,$$

where $\varepsilon \in \mathscr{O}$ is a unit and $p_1, \cdots, p_n \in \mathscr{O}$ are prime elements in $\mathscr{O}$. Say that α has a **unique** prime factorization if whenever there is another prime factorization

$$\alpha = \varepsilon' p'_1 \cdots p'_m,$$

we necessarily have $m = n$ and there is a bijection $\phi\colon \{1, \cdots, n\} \to \{1, \cdots, m\}$ such that each p_i $(1 \leqslant i \leqslant n)$ is *associated* to $p'_{\phi(i)}$.

Say that the **unique prime factorization property** holds in $\mathscr{O}$ if any nonzero element $\alpha \in \mathscr{O}$ has a *unique prime factorization*.

Then problem II.5 shows that the prime factorization property **fails** in $\mathscr{O}$ due to the following counterexample

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5}).$$

Problem II.6. For this problem, you may want to review one-variable Calculus

(a) Recall the definition (In this course, $\log = \log_e$ denotes the *natural logarithm*)

$$\mathrm{Li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t} \qquad (x > 2).$$

Question: What is the $\frac{\mathrm{d}}{\mathrm{d}x}\mathrm{Li}(x)$ of $\mathrm{Li}(x)$?

(b) Two real functions $f(x)$ and $g(x)$ are *asymptotically equal* if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Prove that: $\mathrm{Li}(x)$ and $\frac{x}{\log x}$ are asymptotically equal.

Problem II.7. Prove that if n is a positive integer, and $\sigma_0(n)$ is prime then n is a power of a prime number.

Problem II.8 (Mersenne, 1644)**.** Describe all circumstances under which $\sigma_1(n)$ is odd.

Problem II.9. Prove that if n is a perfect square, then n is not a perfect number.

Problem II.10. Let p be a prime number and k, l be two natural numbers. **Show that**

$$\sum_{i=0}^{k} \sigma_i(p^l) = \sum_{i=0}^{l} \sigma_i(p^k).$$

Problem II.11. Let n be a positive integer and k a natural number. **Show that**

$$\sigma_k(n) = \sigma_{-k}(n)n^k.$$

Conclude that n is *perfect* if and only if $\sigma_{-1}(n) = 2$.

Problem II.12. We say that a positive integer n is **square-free** if n is not divisible by p^2 for any prime number p. (E.g. 15 and 37 are square-free, but 24 and 49 are not.) Consider the arithmetic function μ (named after A.F. Möbius, popularly known for his strip) as follows:

$$\mu(n) := \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n \text{ is NOT sqaure-free,} \\ (-1)^t & \text{if } n \text{ is sqaure-free and has exactly } t \text{ prime divisors.} \end{cases}$$

(a) **Compute** $\mu(n)$ for $n = 1, \cdots, 15$.

(b) **Prove that** μ is *multiplicative*. That is, $\mu(ab) = \mu(a)\mu(b)$ whenever a, b are *coprime*.

Hint. Proceed by cases, taking cue from the definition of μ.

Let $f(n)$ and $g(n)$ be two arithmetic functions. Define $(f \star g)(n)$ by the formula

$$(f \star g)(n) := \sum_{d|n} f(d)g(\frac{n}{d}),$$

where the summation is taken over the set $\mathscr{D}(n) := \{d \mid d \text{ is a divisor of } n\}$. The new function $f \star g$ is called the **convolution** of f and g. The idea originates from Fourier analysis.

(c) Let id denote the function mapping each positive integer n to itself. **Compute** the values of $(\mathrm{id} \star \mu)(n)$ for $n = 1, \cdots, 12$.

(d) Let δ_1 be the function defined as follows:

$$\delta_1(n) := \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if otherwise.} \end{cases}$$

Prove that $\delta_1 \star f = f \star \delta_1 = f$ for any arithmetic function f. (In other words, δ_1 is the *identity* for the binary operation $\star$.)

(e) Let $\mathbf{1}$ be the constant function mapping any positive integer to 1. **Show that** $\mu \star \mathbf{1} = \delta_1$. (In other words, μ is a *unit* for the binary operation $\star$.)

(f) Show that $f \star g = g \star f$ for any arithmetic functions f and g. (In other words, the binary operation $\star$ is *commutative*.)

Hint. Show that $d \mapsto \frac{n}{d}$ is a bijection from $\mathscr{D}(n)$ to itself.

(g) Show that $(f \star g) \star h = f \star (g \star h)$ for any arithmetic functions f, g, and h. (In other words, the binary operation $\star$ is *associative*.)

Hint. Define $f \star g \star h$ as follows:

$$(f \star g \star h)(n) := \sum_{abc=n} f(a)g(b)h(c),$$

where the summation is taken over the set $\mathscr{D}_3(n) := \big\{(a, b, c) \in \mathscr{D}(n)^3 \,\big|\, abc = n\big\}$. Show that each of $(f \star g) \star h$ and $f \star (g \star h)$ is equal to $f \star g \star h$ using a bijective map from its summation index set to $\mathscr{D}_3(n)$.

(At this stage, we see that the set of arithmetic functions equipped with the binary operation $\star$ and the element δ_1 forms a *commutative monoid*.)

(h) Suppose f and g are two multiplicative functions. **Prove that** $f \star g$ is a multiplicative function.

Hint. For any copirme pairs (m, n), use the bijection $\Phi \colon \mathscr{D}(m) \times \mathscr{D}(n) \to \mathscr{D}(mn)$.

(Hence, the subset of *multiplicative* functions forms a *submonoid*.)

(i) Say an arithmetic function f is invertible under the operation $\star$ if there is another arithmetic function g such that $f \star g = \delta_1$. **Prove that** f is invertible under the operation $\star$ if and only if $f(1) \neq 0$.

Hint. Spell out the equality $(f \star g)(n) = \delta_1(n)$ and solve out $f(n)$.

(j) The *Möbius transformation* of an arithmetic function f is the function $\widehat{f}$ defined by the formula

$$\widehat{f}(n) := \sum_{d|n} f(d).$$

Prove the *Möbius inversion formula*:

$$f(n) = \sum_{d|n} \mu(d) \widehat{f}(\frac{n}{d}).$$

Hint. Using II.12.(e).