Supplementary Materials for Chapter I

Xu Gao

MATH 110 | Introduction to Number Theory | Summer 2023

June 27, 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 I
Linear Diophantine Equations

1 Divisibility

Definition 1.1. Consider integers x, y, we say that x divides y, denoted $x \mid y$, if there exists an integer u such that $y = xu$.

Unpackage the definition of *divisibility* to solve the following exercises.

Exercise 1.1. Let a, b, c be integers, then show that

(a). $a \mid b$ if and only if $|a| \mid |b|$.

(b). If $a \mid b$ and $b \neq 0$, then $|a| \leqslant |b|$.

(c). If $c \neq 0$, then $a \mid b$ if and only if $ac \mid bc$.

Terminology 1.2. We say a *relation* $\preccurlyeq$ on a set S is a *partial order* if it satisfies:

- (*reflexivity*) for all $a \in S$, $a \preccurlyeq a$;
- (*antisymmetry*) for all $a, b \in S$, if $a \preccurlyeq b$ and $b \preccurlyeq a$, then $a = b$;
- (*transitivity*) for all $a, b, c \in S$, if $a \preccurlyeq b$ and $b \preccurlyeq c$, then $a \preccurlyeq c$.

A set equipped with a partial order is called an *ordered set*.

Exercise 1.2. Show that the divisibility $(\cdot \mid \cdot)$ on $\mathbb{Z}_+$ and on $\mathbb{N}$ are partial orders. However, it is not a partial order on $\mathbb{Z}$.

Terminology 1.3. A *monoid* is a set M together with a binary operation $*$ and a specific element e (called its *neutral elements*) satisfying the following axioms:

- (*associativity*) $(a * b) * c = a * (b * c)$ for all $a, b, c \in M$;
- (*neutrality*) $a * e = e * a = a$ for all $a \in M$.

Exercise 1.3. Determine whether the following triples are monoids:

(a). (endomaps of a set S, composition, id),

(b). $(\mathbb{N}, \text{multiplication}, 1)$,

(c). $(\mathbb{Z}_+, \text{multiplication}, 1)$,

(d). $(\mathbb{Z}, \text{multiplication}, 1)$,

(e). $(\mathbb{Z}_+, \text{division}, 1)$,

(f). $(\mathbb{N}, \text{addition}, 0)$,

(g). $(\mathbb{Z}_+, \text{addition}, 0)$,

(h). $(\mathbb{Z}, \text{addition}, 0)$.

Terminology 1.4. We say a *property* P defined for elements of a monoid $(M, *, e)$ satisfies the *2-out-of-3 principle* if for any $a, b, c \in M$ satisfying the equation $a * b = c$, we have: if any two of $\{a, b, c\}$ satisfy P, then so does the third element.

Exercise 1.4. Determine whether the following properties satisfy the 2-out-of-3 principle.

(a). The monoid is (endomaps of a set S, composition, id) and the property is "being bijective".

(b). The monoid is $(\mathbb{Z}, \text{addition}, 0)$ and the property is "being divided by d", where d is a positive integer.

2 Linear Diophantine equation

Definition 2.1. The terminology *linear Diophantine equation* can be separated into two:

- *Diophantine equation* = equations in multiple unknowns and the interesting solutions are in a given set of numbers (e.g $\mathbb{Z}$).
- *Linear* = the expression only contains linear combinations of unknowns. Namely, no higher terms, no strange functions.

Example 2.2. (a). $x^2 + y^2 = 1$ is Diophantine equation but not a linear one.

(b). $18x - 27y + 39z = 4$ is a linear Diophantine equation with three unknowns.

Terminology 2.3. Given some objects $X, Y, \cdots, Z$, a *linear combination* of them is an *expression* of the form

$$aX + bY + \cdots + cZ,$$

where $a, b, \cdots, c$ are called the *coefficients*. If all the coefficients are contained in a set S, then we say it is an *S-linear combination*.

Sometimes, we also call

$$Xa + Yb + \cdots + Zc$$

a *linear combination* of the objects $X, Y, \cdots, Z$. The two definitions are equivalent as long as we are allowed to interchange the coefficient a and the object X.

Example 2.4. (a). X is a linear combination of X itself, while X^2 is not.

(b). $\frac{1}{2}X$ is not a $\mathbb{Z}$-linear combination of X since $\frac{1}{2}$ is not an integer.

(c). $(+2) \cdot 133 + (-3) \cdot 85$ is a $\mathbb{Z}$-linear combination of 133 and 85.

Remark. Distinguish an *expression* and a *value*. The equation

$$(+2) \cdot 133 + (-3) \cdot 85 = 11$$

should be read as the *value* of the linear combination $(+2) \cdot 133 + (-3) \cdot 85$ is 11, or the integer 11 *can be expressed* as the linear combination $(+2) \cdot 133 + (-3) \cdot 85$. It *shouldn't* read as "11 *is* the linear combination $(+2) \cdot 133 + (-3) \cdot 85$".

Convenience 2.5. When elements of a set are obtained as outputs of operations, we often use a shorthand notations to denote this set.

- Let A, B be two sets. Then $A + B$ denotes the set of elements $a + b$, where $a \in A$, $b \in B$. Similarly, $AB := \{ab \mid a \in A, b \in B\}$.
- Let A be a set and x be an object (e.g. a number, an unknown, etc.). Then $A + x := \{a + x \mid a \in A\}$. Similarly, $Ax := \{ax \mid a \in A\}$.
- Given objects $x, y, \cdots, z$ and a set S, what does the notation $Sx + Sy + \cdots + Sz$ mean?

3 Euclidean Algorithm

Exercise 3.1. Let a, b be two integers. Show that

(a). $\gcd(a, b) = \gcd(|a|, |b|)$;

(b). $\gcd(a, 0) = |a|$;

(c). if $a \mid b$, then $\gcd(a, b) = |a|$;

Exercise 3.2 (substitution of $\mathbb{Z}$-linear combinations)**.** If an integer n can be expressed as a $\mathbb{Z}$-linear combination of the integers a and b, while the integer b can be expressed as a $\mathbb{Z}$-linear combination of the integers c and d, then n can be expressed as a $\mathbb{Z}$-linear combination of the integers a, c, and d.

The analogy and difference between *solving linear equations* (in Linear Algebra) and *solving linear Diophantine equations* (in Number Theory) worth thinking. Here we provide another approach to Theorem 3.3 in the lecture.

Exercise 3.3. Show that the solution set $S = \left\{(x, y) \in \mathbb{Z}^2 \,\middle|\, a \cdot x + b \cdot y = 0\right\}$ has the following properties:

(a). $(0, 0) \in S$;

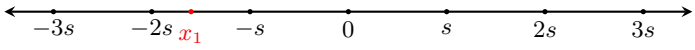
(b). if both $(x_1, y_1) \in S$ and $(x_2, y_2) \in S$, then $(x_1 + x_2, y_1 + y_2) \in S$;

(c). if $(x, y) \in S$ and $m \in \mathbb{Z}$, then $(mx, my) \in S$.

In the language of linear algebra, S is a $\mathbb{Z}$-submodule of $\mathbb{Z}^2$.

Exercise 3.4. Define a map $S \to \mathbb{N}$ as follows: $(x, y) \mapsto |x|$. Suppose $s \in \mathbb{Z}_+$ is the smallest positive integer in the image of the map and $(x_0, y_0) \in S$ is a preimage of s. Show that $S = \mathbb{Z}(x_0, y_0)$ as follows:

(a). Suppose there is $(x_1, y_1) \in S$ which is not a multiple of (x_0, y_0). Show that there is an integer n such that $ns < |x_1| < (n + 1)s$.



(b). Show that $(x_1 - nx_0, y_1 - ny_0) \in S$ but $|x_1 - nx_0| < s$.

(c). Conclude that this is a contradiction and hence $S = \mathbb{Z}(x_0, y_0)$.

Terminology 3.1. A *group* is a monoid $(M, *, e)$ satisfying

- (*invertibility*) for any element $a \in M$, there is an element $a^{-1} \in M$ such that $a*a^{-1} = a^{-1} * a = e$.

A monoid $(M, *, e)$ is *abelian* if it satisfies

- (*commutativity*) $a * b = b * a$ for all $a, b \in M$.

An *abelian group* is an abelian monoid which is a group.

Exercise 3.5. Determine whether the following monoids are groups/abelian groups:

(a). (endomaps of a set S, composition, id),

(b). ($\mathbb{N}$, multiplication, 1),

(c). ($\mathbb{Z}$, multiplication, 1),

(d). ($\mathbb{N}$, addition, 0),

(e). ($\mathbb{Z}$, addition, 0).

Terminology 3.2. A $\mathbb{Z}$-*module* is an abelian group $(M, +, e)$ together with an action of integers $\rho\colon \mathbb{Z} \times M \to M$ satisfying

- (*associativity*) $\rho(mn, a) = \rho(m, \rho(n, a))$ for all $m, n \in \mathbb{Z}$ and $a \in M$;
- (*neutrality*) $\rho(m, e) = e$ for all $m \in \mathbb{Z}$.

Exercise 3.6 (†)**.** Show that any abelian group is automatically a $\mathbb{Z}$-module. (Hint: how to define the action ρ?)

We usually write $m.e$ or me instead of $\rho(m, e)$ for simplicity.

Exercise 3.7. Fix a positive integer n and let $(M, +, 0, \rho)$ be a $\mathbb{Z}$-module. Show that the following tuple gives a $\mathbb{Z}$-module:

- the set is $M^n := \{(a_1, \cdots, a_n) \mid a_1, \cdots, a_n \in M\}$;
- the operation is componentwise addition:

$$(a_1, \cdots, a_n) + (b_1, \cdots, b_n) := (a_1 + b_1, \cdots, a_n + b_n);$$

- the neutral element is $(0, \cdots, 0)$;
- the action is componentwise multiplication:

$$\rho(m, (a_1, \cdots, a_n)) = (ma_1, \cdots, ma_n).$$

In particular, we have $\mathbb{Z}$-module structures on $\mathbb{Z}^n$, $\mathbb{R}^n$, etc.

Terminology 3.3. A subset N of a monoid $(M, *, e)$ is a *submonoid* if $e \in N$ and N is closed under the operation: $\forall a, b \in M : a, b \in N \implies a * b \in N$.

A subset N of a group $(M, *, e)$ is a *subgroup* if it is a submonoid and is closed under taking inverse: $\forall a \in M : a \in N \implies a^{-1} \in N$.

A subset N of a $\mathbb{Z}$-module $(M, +, 0, \rho)$ is a *submodule* if it is a subgroup and is closed under the action:

$$\forall a \in M, m \in \mathbb{Z}\colon a \in N \implies ma \in N.$$

Exercise 3.8 (†)**.** Show that a subset N of a $\mathbb{Z}$-module $(M, +, 0, \rho)$ is a submodule if it is a submonoid and is closed under the action.

Terminology 3.4. A $\mathbb{Z}$-module M is *free of rank one* if there is an element $x_0 \in M$ such that $M = \mathbb{Z}x_0$. Namely, any element of M is a multiple of x_0.

More generally, fix a natural number n, a $\mathbb{Z}$-module M is *free of rank* n if there are elements $x_1, \cdots, x_n \in M$ such that any element of M can be *uniquely* expressed as a $\mathbb{Z}$-linear combination of $x_1, \cdots, x_n$.

Example 3.5.

- The $\mathbb{Z}$-module $\mathbb{Z}^n$ is free of rank n.
- Exercise 3.4 shows that the solution set S of $a \cdot x + b \cdot y = 0$ is free of rank one.

Problems

Problem I.1. This problem is a 3-varibales analogy of the material covered in lectures.

(a) Prove that there exists no integer solution (x, y, z) to the equation

$$18x - 27y + 39z = 4.$$

(b) Find **an** integer solution (x, y, z) to the equation $18x - 27y + 39z = 6$.

(c) Find **all** the integer solutions (x, y, z) to the equation $18x - 27y + 39z = 6$. Your answer should give explicit formulae for x, y, z in terms of two free independent integer parameters m and n.

Remark. Can you work out a general algorithm?

Problem I.2. Let a, b, c be three integers, and let $g = \gcd(a, \gcd(b, c))$.

(a) Prove that g satisfies the following properties:

(i) g is a common divisor of a, b and c, in other words, we have $g \mid a$, $g \mid b$ and $g \mid c$.

(ii) If d is any common divisor of a, b and c, then $d \mid g$.

(b) Prove that g is the unique natural number satisfying both (i) and (ii).

Optional. During your proof, try to only use the following facts: 1, the *definition* of $\gcd(\cdot, \cdot)$, 2, the *transitivity* $\cdot \mid \cdot$, and 3, the *reflexivity* of $\cdot \mid \cdot$.

Hint. Compare this problem with the fact that $\max\{a, b, c\} = \max\{a, \max\{b, c\}\}$.

The properties (i) and (ii) together are called the *defining property* of the notion of the *greatest common divisor of a, b and c.*

We will use $\gcd(a, b, c)$ to denote the greatest common divisor of a, b and c. Then problem I.2.(a) says that $\gcd(a, \gcd(b, c))$ gives an *implementation* of $\gcd(a, b, c)$. Namely, it gives a way to compute the $\gcd(a, b, c)$ from the given integers a, b, c: first compute $\gcd(b, c)$, and then plug it in $\gcd(a, \gcd(b, c))$, the final result would be the answer.

Problem I.3. Treat $\gcd(\,\cdot\,, \cdot\,)$ as a binary operation on $\mathbb{Z}$. Show that it is *associative*:

$$\forall a, b, c \in \mathbb{Z}\colon\ \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c).$$

Remark. By symmetry, the same results as in problems I.2 and I.3 holds for $\mathrm{lcm}(\,\cdot\,, \cdot\,)$.

Problem I.4. Let $a_1, \cdots, a_n$ be n integers.

(a) Mimicking problem I.2, give the *defining properties* of the notion of the *greatest common divisor of* $a_1, \cdots, a_n$. (In other words, give a reasonable *definition* of this notion involving two properties mimicking (i) and (ii) in problem I.2.(a))
Then give an *implementation* of such a notion in terms of $\gcd(\,\cdot\,,\,\cdot\,)$. (In other words, give a way to compute the greatest common divisor of $a_1, \cdots, a_n$ using only the two variable version $\gcd(\,\cdot\,,\,\cdot\,)$.)

Remark. We will use the notation $\gcd(a_1, \cdots, a_n)$ or $\gcd\limits_{1 \leqslant i \leqslant n} a_i$ to denote this notion.

(b) Give the *defining properties* of the notion of the *least common multiple of* $a_1, \cdots, a_n$. Then give an *implementation* of such a notion in terms of $\mathrm{lcm}(\,\cdot\,,\,\cdot\,)$.

Remark. We will use the notation $\mathrm{lcm}(a_1, \cdots, a_n)$ or $\mathrm{lcm}\limits_{1 \leqslant i \leqslant n} a_i$ to denote this notion.

(c) Mimicking the proof of the attached proposition, show that:

For any matrix $(a_{ij})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m}$ of integers, we have

$$\mathrm{lcm}_{1 \leqslant i \leqslant n} \gcd_{1 \leqslant j \leqslant m} a_{ij} \mid \gcd_{1 \leqslant j \leqslant m} \mathrm{lcm}_{1 \leqslant i \leqslant n} a_{ij}.$$

Hint. What facts are used in the proof?

Proposition. *Let $(x_{ij})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m}$ be a matrix of real numbers, then we have*

$$\max_{1 \leqslant i \leqslant n} \min_{1 \leqslant j \leqslant m} x_{ij} \leqslant \min_{1 \leqslant j \leqslant m} \max_{1 \leqslant i \leqslant n} x_{ij}.$$

Proof. Define $f(i)$ $(1 \leqslant i \leqslant n)$ to be $\min\limits_{1 \leqslant j \leqslant m} x_{ij}$. Then we have

$$f(i) \leqslant x_{ij} \qquad \text{for all} \qquad 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant m.$$

Therefore, we have

$$\max_{1 \leqslant i \leqslant n} f(i) \leqslant \max_{1 \leqslant i \leqslant n} x_{ij} \qquad \text{for all} \qquad 1 \leqslant j \leqslant m.$$

In particular, we have

$$\max_{1 \leqslant i \leqslant n} f(i) \leqslant \min_{1 \leqslant j \leqslant m} \max_{1 \leqslant i \leqslant n} x_{ij}$$

as desired. □

Problem I.5. Let a, b and n be positive integers. `Prove` that

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