MATH 323, Algebra I, Fall 2020

Course notes, Chapter 2, Introductory number theory

Laurence Barker, Bilkent University. Version: 14 November 2020.

These notes, updated as the course progresses, are a record of the prepared text of the lectures, with a little more detail added, but they cannot cover much of the oral component of the lectures.

Summary of contents

We shall be reviewing some preliminary notions from introductory number theory.

Fuller details on the material we shall be summarizing can be found in Judson, primarily Chapter 2. These notes are independent of that text.

The main notions to be reviewed are those of:

• the **greatest common divisor** and **highest common factor** of two non-zero integers.

• a **binary operation**,

• **modular arithmetic**,

• **Euler's totient function**.

We shall also have a little preview concerning abelian groups. A more thorough discussion of abelian groups will appear in the next chapter.

The greatest common divisor and least common multiple: The following result, proved using the theory of the Euclidian algorithm, appears in courses on Abstract Mathematics or Introduction to Number Theory. Recall, the **greatest common divisor** $\gcd(x, y)$ of non-zero integers x and y is defined to be the smallest positive integer that divides both x and y.

Theorem 2.1: (Greatest Common Divisor Theorem.) *Given non-zero integers a and b, then there exist integers x and y such that* $\gcd(a, b) = xa + yb$.

In particular, a and b are coprime if and only if there exist integers x and y such that $xa + yb = 1$.

The least common multiple: The **least common multiple** $\mathrm{lcm}(a, b)$ of two non-zero integers a and b is defined to be the smallest positive integer divisible by both a and b.

Now suppose a and b are positive integers. Consider mutually distinct primes p_1, ..., p_r and natural numbers α_1, ..., α_r and β_1, ..., β_r such that a and b have prime

factorizations

$$a = p_1^{\alpha_1}...p_r^{\alpha_r} \ , \qquad b = p_1^{\beta_1}...p_r^{\beta_r} \ .$$

For each integer $1 \in i \leq r$, let γ_i be the minimum of α_i and β_i. Let δ_i be the maximum of α_i and β_i. Then $\gcd(a,b)$ and $\mathrm{lcm}(a,b)$ have prime factorizations

$$\gcd(a,b) = p_1^{\gamma_1}...p_r^{\gamma_r} \ , \qquad \mathrm{lcm}(a,b) = p_1^{\delta_1}...p_r^{\delta_r} \ .$$

Noting that each $\alpha_i + \beta_i = \gamma_i + \delta_i$, we obtain following result.

Proposition 2.2: *Given positive integers a and b, then $ab = \gcd(a,b)\mathrm{lcm}(a,b)$.*

Binary operations: We define a **binary operation** on a set X to be a function $X \leftarrow X \times X$. For $x, y \in X$, we often write the image of (x,y) under $*$ as $x * y$ instead of $*(x,y)$.

- We call $*$ **commutative** provided $x * y = y * x$ for all $x, y \in X$.
- We call $*$ **associative** provided $x * (y * z) = (x * y) * z$ for all $x, y, z \in X$.

For example, on the set $\mathbb{Z}$ of integers, the addition operation $x + y \leftarrow\!\shortmid (x,y)$ is commutative and associative. Again on $\mathbb{Z}$, the multiplication operation $xy \leftarrow\!\shortmid (x,y)$ is commutative and associative.

As another example, on the set $\mathbb{Z} - \{0\}$ of non-zero integers, the functions $\gcd(x,y) \leftarrow\!\shortmid (x,y)$ and $\mathrm{lcm}(x,y) \leftarrow\!\shortmid (x,y)$ are

The congruence relations on the integers: Let n be a positive integer. On the set $\mathbb{Z}$ of integers, we define a relation $\equiv_n$ such that, given $a, b \in \mathbb{Z}$, then $a \equiv_n b$ provided $a - b$ is divisible by n.

It is easy to check that $\equiv_n$ is an equivalence relation.

The equivalence relation $\equiv_n$ on $\mathbb{Z}$ is called **modulo n congruence**. For $x \in \mathbb{Z}$, the equivalence class of x under $\equiv$, denoted $[x]_n$, is called the **modulo n congruence class** of n. Thus,

$$[x]_n = \{..., x - 2n, x - 2n, x, x + n, x + 2n, ...\} \ .$$

We write the set of modulo n congruence classes as

$$\mathbb{Z}/n = \{[x]_n : x \in \mathbb{Z}\} = \{[0]_n, [1]_n, ..., [n-1]_n\} \ .$$

Modular arithmetic: We shall equip $\mathbb{Z}/n$ with two binary operations, called *addition* and *multiplication*.

We define the **addition operation** on $\mathbb{Z}/n$ to be the binary operation $+$ on $\mathbb{Z}/n$ such that

$$[x]_n + [y]_n = [x + y]_n$$

for $x, y \in \mathbb{Z}$. We call $[x]_n + [y]_n$ the **sum** of $[x]_n$ and $[y]_n$.

Let us show that the addition on $\mathbb{Z}/n$ is well-defined. We are to show that, given $\xi, \eta \in \mathbb{Z}/n$, then the formula for $\xi + \eta$ does not depend on choices. Choose $x, y \in \mathbb{Z}/n$ such that $\xi = [x]_n$ and $\eta = [y]_n$. By the formula, $\xi + \eta = [x + y]_n$. We must show that this evaluation of $\xi + \eta$ is independent of the choices of x and y. Choose some other representatives of the congruence classes, $x', y' \in \mathbb{Z}/n$ such that $\xi = [x']_n$ and $\eta = [y']_n$. By the formula again, $\xi + \eta = [x' + y']_n$. But n divides $x - x'$ and $y - y'$, so n divides $x+y-(x'+y')$, in other words, the two evaluations of $\xi+\eta$ are equal, $[x+y]_n = [x'+y']_n$.

We define a binary operation on $\mathbb{Z}/n$ called **multiplication** and written multiplicatively, by $[x]_n[y]_n = [xy]_n$. Again, well-definedness is easy to check.

Units in modular arithmetic: Recall, two integers x and y are said to be **coprime** provided x and y have no common prime factor, in other words, the greatest common divisor of x and y is 1.

The next remark is obvious.

Remark: *Let n be a positive integer and $\xi \in \mathbb{Z}/n$. Then the following two conditions are equivalent:*
(a) *For some $x \in \mathbb{Z}$ such that $\xi = [x]_n$, the integers x and n are coprime.*
(b) *For all $x \in \mathbb{Z}$ such that $\xi = [x]_n$, the integers x and n are coprime.*

When the equivalent conditions in the remark hold, we call ξ a **unit** of $\mathbb{Z}/n$. We write $(\mathbb{Z}/n)^\times$ for the set of units of $\mathbb{Z}/n$.

Notation: the textbook Judson writes $(\mathbb{Z}/n)^\times$ more simply as $U(n)$. But the notation $(\mathbb{Z}/n)^\times$ is standard whereas, in the literature, $U(n)$ conventionally denotes an infinite group called the *unitary group of degree n*.

As examples,

$$(\mathbb{Z}/7)^\times = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\} ,$$
$$(\mathbb{Z}/8)^\times = \{[1]_8, [3]_8, [5]_8, [7]_8\} .$$

Proposition 2.2: *Let n be a positive integer and $\xi \in \mathbb{Z}/n$. Then $\xi \in (\mathbb{Z}/n)^\times$ if and only if there exists $\eta \in (\mathbb{Z}/n)^\times$ such that $\xi\eta = [1]_n$.*

Proof: Let $x \in \mathbb{Z}$ such that $\xi = [x]_n$. Suppose such η exists. Let $y \in \mathbb{Z}$ such that $\eta = [y]_n$. Then $xy \equiv_n 1$. That is to say, there exists $k \in \mathbb{Z}$ such that $xy - 1 = kn$. Plainly, no prime factor of n can divide x. So x and n are coprime. We have deduced that $\xi \in (\mathbb{Z}/n)^\times$.

Conversely, suppose x and n are coprime. Then the greatest common divisor of x and n is $1 = xy + nz$ for some $y, z \in \mathbb{Z}$. Putting $\eta = [y]_n$, then $\xi\eta = [1]_n$. □

Remark: *Given $\xi, \eta \in (\mathbb{Z}/n)^\times$, then $\xi\eta \in (\mathbb{Z}/n)^\times$.*

Proof: Write $\xi = [x]_n$ and $\eta = [y]_n$. Then $\xi\eta = [xy]_n$ and xy is coprime to n. So $\xi\eta \in (\mathbb{Z}/n)^\times$. □

The multiplication operation on $\mathbb{Z}/n$ restricts to a binary operation on $(\mathbb{Z}/n)^\times$.

The Euler totient function: Recall, one definition of Euler's totient function $\phi : \mathbb{N} - \{0\} \leftarrow \mathbb{N} - \{0\}$ is by the formula

$$\phi(n) = |(\mathbb{Z}/n)^\times| \ .$$

In courses on Abstract Mathematics or Number Theory, it is shown that

$$\phi(n) = n \prod_p (1 - 1/p)$$

where p runs over the prime divisors of n. Of course, that formula can also be taken as the definition.

As an example, since the prime factors of $360 = 2^3.3^2.5$ are 2, 3, 5, we have

$$\phi(60) = (1 - 1/2)(1 - 1/3)(1 - 1/5)360 = (2^3 - 2^2)(3^2 - 3)(5 - 1) = 4.6.4 = 96 \ .$$

A philosophical question, to be answered later in the course

Examples of the kinds of addition and multiplication tables that we are about to discuss can be found in Judson Examples 3.9 and 3.11.

Observe that $|\mathbb{Z}/6| = 6 = |(\mathbb{Z}/7)^\times|$. Write out the addition table for $\mathbb{Z}/6$ and the multiplication table for $(\mathbb{Z}/7)^\times$. You may notice that in some sense, the two tables have the same structure.

We also have $|\mathbb{Z}/4| = 4 = (\mathbb{Z}/8)^\times$. Write out the addition table for $\mathbb{Z}/4$ and the multiplication table for $(\mathbb{Z}/8)^\times$. You may notice that, this time, the tables are different from each other.

Question 2.A: Given a positive integer m, is there some way of describing the multiplication table of $(\mathbb{Z}/m)^\times$ in terms of the addition tables of $\mathbb{Z}/n$ for some positive integers n?

Let us give an indication of how we shall eventually answer that question. The set $\mathbb{Z}/n$, equipped with addition, is just about the easiest kind of example of a finite abelian group. In fact, up to a kind of equivalence called isomorphism, the groups $\mathbb{Z}/n$ are precisely the finite cyclic groups. These are the easiest kind of finite abelian group.

The groups $(\mathbb{Z}/m)^\times$ are also examples of abelian groups, but some of their features are a little more mysterious. Thus, the question becomes: can we describe the finite abelian groups $(\mathbb{Z}/m)^\times$ in terms of the finite cyclic groups?

It turns out that, for a natural number a, the group $(\mathbb{Z}/2^a)^\times$ is cyclic only when $a \leq 2$. However, for $a \geq 3$, the group $(\mathbb{Z}/2^a)^\times$ is still, in a certain sense, very close to being a cyclic group. This fact is employed in one straightforward algorithm for generating psuedo-random numbers.