Chapter 6

Modular Arithmetic

6.1 Congruences

We usually associate arithmetic with the infinite set of integer numbers. However, *modular arithmetic* on finite sets is commonly used in our daily life. As an example, if it is now 1 am and we let 1000 hours pass, what time will it be? We can use the division algorithm to see that $1000 = 41 \times 24 + 16$ and conclude that adding 1000 hours is like adding 16 hours, since the clock returns to the same position every 24 hours. So after 1000 hours it will be 5 pm (17 hours after midnight).

There are many examples in which it is natural and useful to limit our number system to a finite range of integers, such as 0 through $n-1$, for some n. This number system is denoted by $\mathbb{Z}_n$. Days of the week, hours of the day, minutes in an hour are all familiar examples of finite number systems, as are numbers in microprocessor registers, commonly limited to 32 binary digits.

Modular arithmetic allows us to add, subtract, multiply, and sometimes divide numbers while staying within the finite set $\mathbb{Z}_n$. The number n is called the *modulus*. A central notion in modular arithmetic is *congruence*. We say that two integers are congruent modulo n if they leave the same remainder when divided by n. Here is the formal definition:

Definition: Two integers $a, b \in \mathbb{Z}$ are said to be *congruent modulo* n, written as $a \equiv_n b$ or $a \equiv b \pmod{n}$, if and only if they leave the same remainder when divided by n, that is, $a \text{ rem } n = b \text{ rem } n$.

This definition captures our intuition that the day of the week will be the same whether we let 10, 17, or 80 days pass. There is an equivalent definition of congruence that is often useful in proofs:

Lemma 6.1.1. *$a \equiv_n b$ if and only if $n|(a-b)$.*

Proof. If $a \equiv_n b$ then $a \text{ rem } n = b \text{ rem } n$. Put $r = a \text{ rem } n = b \text{ rem } n$. Then there exist two integers q_1 and q_2, such that $a = q_1 n + r$ and $b = q_2 n + r$. Subtracting the second equation from the first, we get $a - b = (q_1 - q_2)n$ and $n|(a-b)$.

On the other hand, if $n|(a-b)$ then there exists an integer d, such that $a - b = nd$. By the division algorithm, there exist integers $q_1, q_2 \in \mathbb{Z}$, and $0 \leq r_1, r_2 < n$, such

that $a = q_1 n + r_1$ and $b = q_2 n + r_2$. Thus $(q_1 - q_2)n + (r_1 - r_2) = nd$, and $r_1 - r_2 = (q_2 - q_1 + d)n$. Thus $n|(r_1 - r_2)$. However, $|r_1 - r_2| < n$, so necessarily $r_1 - r_2 = 0$, which implies that $a \text{ rem } n = b \text{ rem } n$, and $a \equiv_n b$. □

You should use the definition to verify that for any $a, b, c \in \mathbb{Z}$,

- $a \equiv_n a$. (Reflexivity.)
- If $a \equiv_n b$ then $b \equiv_n a$. (Symmetry.)
- If $a \equiv_n b$ and $b \equiv_n c$ then $a \equiv_n c$. (Transitivity.)

The operations of addition, subtraction, and multiplication on $\mathbb{Z}_n$ are defined by first doing the corresponding operation in $\mathbb{Z}$ and then taking the remainder modulo n. That is, if we denote these respective operations by $+_n$, $-_n$, and $\cdot_n$, then

$$\begin{aligned} a +_n b &= (a + b) \text{ rem } n \\ a -_n b &= (a - b) \text{ rem } n \\ a \cdot_n b &= (ab) \text{ rem } n \end{aligned}$$

Exponentiation is defined through repeated multiplication.

Lemma 6.1.2. *Properties of congruence:*

(a) $(a \text{ rem } n) \text{ rem } n = a \text{ rem } n$

(b) $(a \text{ rem } n) \equiv_n a$

(c) $(ab) \text{ rem } n = (a \text{ rem } n)(b \text{ rem } n) \text{ rem } n$

(d) $(a \text{ rem } n)(b \text{ rem } n) \equiv_n ab$

(e) $\prod_{i=1}^{k} (a_i \text{ rem } n) \equiv_n \prod_{i=1}^{k} a_i$

(f) If $a_1 \equiv_n a_2$ *and* $b_1 \equiv_n b_2$ *then*

$$\begin{aligned} a_1 + b_1 &\equiv_n a_2 + b_2 \\ a_1 - b_1 &\equiv_n a_2 - b_2 \\ a_1 b_1 &\equiv_n a_2 b_2 \end{aligned}$$

Proof. (b) is just a restatement of (a). To prove these we need to show that $n|(a - (a \text{ rem } n))$. Put $r = a \text{ rem } n$. By the division algorithm, there exists $q \in \mathbb{Z}$, such that $a = qn + r$. Thus $a - r = qn$, which implies that $n|a - r$ and concludes the proof.

(d) is a restatement of (c), and (e) can be proved from (d) by induction. To prove (c) we need to show that $n|(ab - (a \text{ rem } n)(b \text{ rem } n))$. Use the division algorithm to represent $a = q_1 n + r_1$ and $b = q_2 n + r_2$. Then

$$ab - (a \text{ rem } n)(b \text{ rem } n) = (q_1 n + r_1)(q_2 n + r_2) - r_1 r_2 = (q_1 q_2 n + r_1 q_2 + q_1 r_2)n,$$

which implies the claim.

We now prove (f). We know that $n|(a_1 - a_2)$ and $n|(b_1 - b_2)$. That is, there exist integers q and s, such that $a_1 - a_2 = qn$ and $b_1 - b_2 = sn$. Adding these equations gives $(a_1 + b_1) - (a_2 + b_2) = (q + s)n$, which yields the first part of the claim. Subtracting similarly gives the second part. Writing $a_1 = a_2 + qn$ and $b_1 = b_2 + sn$ and multiplying the equations gives

$$\begin{aligned} a_1 b_1 &= a_2 b_2 + b_2 qn + a_2 sn + qsn^2 \\ a_1 b_1 - a_2 b_2 &= (b_2 q + a_2 s + qsn)n, \end{aligned}$$

which yields the third part. □

6.2 Modular division

You might have noticed that we defined addition, subtraction, and multiplication, but not division. This might not be surprising, since the division operation is not defined for the integers in general: There is no integer that corresponds to 5 divided by 4, for instance. (In other words, there is no $x \in \mathbb{Z}$, such that $4x = 5$.) This distinguishes $\mathbb{Z}$ from sets like $\mathbb{Q}$ or $\mathbb{R}$ that are *closed under division*.

Division in $\mathbb{Z}_n$ appears even more unruly. For example, in $\mathbb{Z}_6$, the equation $2x = 4$ is satisfied by both $x = 2$ and $x = 5$, while the equation $2x = 3$ has no solutions. So the notion of "b divided by a" can be undefined or even ambiguous in $\mathbb{Z}_n$. In particular, we cannot generally cancel a multiplier from both sides of a congruence, that is, if $ab \equiv_n ac$ we cannot reason that $b \equiv_n c$. To take the above illustration, $2 \cdot 2 \equiv_6 2 \cdot 5$, but $2 \not\equiv_6 5$.

Quite remarkably, however, the division operation is well-defined when n is a prime p. Thus $\mathbb{Z}_p$ is in a sense as well-behaved as the real numbers, despite being a finite set! After a small digression that explores what "well-behaved" actually means here, we will state an even more general result on modular division.

Digression (notions from abstract algebra): There is a way to precisely state what we mean by "well-behaved" above. Jumping the gun, I'll say that $\mathbb{Z}_p$ is a *field*, not just a *ring*. Now let me tell you what this means. The notion of a ring in algebra is meant to abstract our intuition concerning the essential properties of the integers. Given a set S equipped with two operations, $+$ (addition) and $\cdot$ (multiplication), we say that S is a ring if the following all hold for any $a, b, c \in S$:

- $a + b \in S$ and $a \cdot b \in S$.
- $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- $a + b = b + a$ and $a \cdot b = b \cdot a$.
- $a \cdot (b + c) = a \cdot b + a \cdot c$.
- There exists an *additive identity* element $0 \in S$ that satisfies $a + 0 = a$ and a *multiplicative identity* element $1 \in S$ that satisfies $a \cdot 1 = a$ for all $a \in S$.

- For every $a \in S$ there exists an *additive inverse* $-a \in S$ for which $a + (-a) = 0$.

All the number systems we have encountered so far are rings, including $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{Z}_n$. However, some of them possess additional structure that allows the division operation. Namely, a ring is said to be a *field* if, in addition to the above, the following holds

- For every $a \in S$, such that $a \neq 0$, there exists a *multiplicative inverse* $a^{-1} \in S$ for which $a \cdot a^{-1} = 1$.

The number systems $\mathbb{R}$ and $\mathbb{Q}$, as well as $\mathbb{Z}_p$ when p is prime, are fields. In fields the division operation is well-defined, and $b/a = b \cdot a^{-1}$, as can be verified by plugging $x = b \cdot a^{-1}$ into the equation $ax = b$. A field with a finite number of elements is called a *Galois field*, after the French mathematician Evariste Galois. (A feisty young man who died in a duel at the age of 20, *after* making significant enough contributions to mathematics to have a whole field (sic) named in his honor!) Anyway, now that we know what fields are, let's see why $\mathbb{Z}_p$ is one. In fact, we prove something more general:

Theorem 6.2.1. *If a and n are coprime then there exists exactly one $x \in \mathbb{Z}_n$ for which $ax \equiv_n b$, for any $b \in \mathbb{Z}$.*

Proof. We need to prove existence and uniqueness of x as described in the theorem. $ax \equiv_n b$ if and only if there exists $q \in \mathbb{Z}$, such that $ax - b = nq$, or $ax - nq = b$. Now, since $\gcd(a, n) = 1$, any integer, including b, is a linear combination of a and n. This proves existence.

To prove uniqueness, assume that for $x, y \in \mathbb{Z}_n$ it holds that $ax \equiv_n b$ and $ay \equiv_n b$. Thus $ax - ay \equiv_n 0$, or $n|a(x-y)$. As you proved in one of the homework assignments, since n and a are coprime, this implies that $n|(x-y)$, and therefore that $x - y \equiv_n 0$. Thus $x \equiv_n y$, which proves uniqueness. □

Corollary 6.2.2. *For a prime p and any $a, b \in \mathbb{Z}$, such that $a \not\equiv_p 0$, there exists exactly one $x \in \mathbb{Z}_p$ for which $ax \equiv_p b$.*

The fact that division is well-defined in $\mathbb{Z}_p$ when p is prime also means that cancelations become valid. Thus if $a \not\equiv_p 0$ and $ab \equiv_p ac$ we can safely conclude that $b \equiv_p c$.

We now know that b/a is well-defined in $\mathbb{Z}_p$, but how do we find it? That is, how do we find $x \in \mathbb{Z}_p$, for which $ax \equiv_p b$. This question is particularly important when p is large and it takes too long to simply enumerate all the elements of $\mathbb{Z}_p$. Fortunately, the following result, known as *Fermat's Little Theorem*, can help us:

Theorem 6.2.3. *For a prime p and any $a \not\equiv_p 0$,*

$$a^{p-1} \equiv_p 1.$$

Proof. Consider the set S, defined as $1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a$. None of these $p - 1$ integers are congruent modulo p, since we have seen that if $ia \equiv_p ja$ then $i \equiv_p j$.

However, each element of S is congruent to some element of $\mathbb{Z}_p$. Since there are $p-1$ elements in S and $p-1$ nonzero elements in $\mathbb{Z}_p$, the elements of S must be congruent to each of $1, 2, \ldots, (p-1)$ in some order. Therefore,

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv_p 1a \cdot 2a \cdot \cdots \cdot (p-1)a,$$

or

$$1 \cdot 2 \cdot \cdots \cdot (p-1) \equiv_p 1 \cdot 2 \cdot \cdots \cdot (p-1) \cdot a^{p-1}.$$

We can cancel each of $1, 2, \ldots, (p-1)$ from both sides of the congruence, obtaining $a^{p-1} \equiv_p 1$. □

Fermat's Little Theorem allows us to quickly perform division in $\mathbb{Z}_p$. The element $x \in \mathbb{Z}_p$ for which $ax \equiv_p b$ is simply $(a^{p-2}b \text{ rem } p)$.