0.1 Modular Arithmetic

We review basic facts of modular arithmetic.

We are familiar with the concept of integer division with remainder:

For any integer a and positive integer n there are unique integers q and r such that $0 \leq r < n$ and $a = qn + r$. We call $q = \lfloor a/n \rfloor$ the *quotient* of the division and $r = a - \lfloor a/n \rfloor \cdot n$ the *remainder (or residue)* of the division. The remainder plays such an important role that is deserves its own notation. We use $a \mod n$ to denote the remainder of the division of a by n. We have

$$0 \leq a \bmod n < n \quad \text{and} \quad a \bmod n = a - \lfloor a/n \rfloor \cdot n \ .$$

We introduce a shorthand for the fact that two numbers have equal remainder. We write $x \equiv y \pmod{n}$ and call x and y *equivalent* to y, modulo n, iff $x \bmod n = y \bmod n$. For example, $2 \equiv 7 \pmod{5}$. Equivalence modulo n is an equivalence relation. Indeed, for any x, y, and z, we have (1) $x \equiv x \pmod{n}$, (2) $x \equiv y \pmod{n}$ implies $y \equiv x \pmod{n}$, and (3) $x \equiv y \pmod{n}$ and $y \equiv z \pmod{n}$ implies $x \equiv z \pmod{n}$.

We have $x \equiv y \pmod{n}$ iff $(x - y) \equiv 0 \pmod{n}$, see exercise 1. If two numbers are not equivalent, we write $x \not\equiv y \pmod{n}$.

We will frequently need to consider the reminders of all multiples of a number a modulo a number n. For example, if $a = 3$ and $n = 4$, $0 \cdot 3 \bmod 4 = 0$, $1 \cdot 3 \bmod 4 = 3$, $2 \cdot 3 \bmod 4 = 2$, and $3 \cdot 3 \bmod 4 = 1$, i.e., all numbers in $[0 \mathinner{..} n-1]$ occur as a reminder and each number occurs exactly once. This is true whenever a and n are relatively prime as the next lemma shows.

Two numbers a and n are called *relatively prime* if their greatest common divisor is equal to 1, i.e., if there is no prime p which divides both of them.

Lemma 1 *If a and n are non-negative, relatively prime integers, the sequence*

$$0 \cdot a \bmod n, 1 \cdot a \bmod n, 2 \cdot a \bmod n, \ldots, (n-1) \cdot a \bmod n$$

is a permutation of $[0 \mathinner{..} n-1]$.

Proof: The sequence has length n and all numbers in the sequence belong to $[0 \mathinner{..} n-1]$. It therefore suffices to show that the numbers are pairwise distinct. Consider i and j with $0 \leq i \leq j < n$ and assume $ia \bmod n = ja \bmod n$. Then $n | (j-i)a$ and hence $n | (j-i)$. The latter conclusion follows from the fact that n and a are relatively prime (see exercise 2). But $j - i < n$ and hence $j = i$. ∎

The following corrollary is extremely useful.

Lemma 2 a) *If a and n are non-negative, relatively prime integers and $b \in range 0 n - 1$, there is an x such that $ax \equiv b \pmod{n}$.*

b) *If n is a prime, $a \not\equiv 0 \pmod{n}$, and $b \in range 0 n - 1$, there is an x such that $ax \equiv b \pmod{n}$.*

Proof: Since the multiples of a have different remainders (by the preceding lemma), the value b appears among the reminders. This proofs part a). If p is a prime, any number $anot \equiv 0 \pmod{n}$ is relatively prime to n. ∎

For example, the equation $4 \cdot x \equiv 1 \pmod 19$ has the solution $x = 5$.

We will next define an addition and a multiplication operation for the remainders modulo n.

We start by defining residue classes modulo n. For any integer a, the residue class of a modulo n is denoted $[a]_n$ and is defined as

$$[a]_n = \{a + in \; ; i \in Z\} \; .$$

For a residue class $[a]_n$ we call any element $b \in [a]_n$ a *representative* of the residue class.

We collect some simple facts about residue classes.

- $a \in [a]_n$.
- If $b \in [a]_n$ then $[a]_n = [b]_n$. Indeed, we have $b = a + in$ and hence $[b]_n \subseteq [a]_n$. Also, $a = b - in$ and hence $[a]_n \subseteq [b]_n$.
- Two classes $[a]_n$ and $[b]_n$ are either disjoint or equal. Indeed, if $c \in [a]_n \cap [b]_n$ then $[a]_n = [c]_n$ and $[b]_n = [c]_n$ by the preceding item.
- $[a]_n = [b]_n$ iff $a \equiv b \pmod n$. Indeed, if $[a]_n = [b]_n$ then $a \in [b]_n$ and hence $a = b + in$ for some i. Thus $n|(a - b)$ and hence $a \equiv b \pmod n$. Conversely, if $a \equiv b \pmod n$, then $n|(a - b)$ and hence $a = b + in$ for some i. Thus $a \in [b]_n$ and hence $[a]_n = [b]_n$.

The set of all residue classes module n is denoted Z_n,

$$Z_n = \{[a]_n \; ; a \in Z\} \; .$$

We next define addition and multiplication of residue classes.

- $[a]_n + [b]_n = [a + b]_n$.
- $[a]_n + [b]_n = [a + b]_n$.

These definitions look innocent, but they aren't. We need to prove that they make sense. A

Exercises:

1. Prove $x \equiv y \pmod n$ iff $(x - y) \equiv 0 \pmod n$.

   Solution: We have $x \equiv y \pmod n$ iff $x \bmod n = y \bmod n$. Let $r = \bmod n$. Then $x = q_x n + r$ and $y = q_y n + r$ for some integers q_x and q_y and hence $x - y = (q_x - q_y)n$. Thus $x - y \equiv 0 \pmod n$. Conversely, if $x - y \equiv 0 \pmod n$ then $x - y = qn$ for some q and hence $(x \bmod n) - (y \bmod n) = x - \lfloor x/n \rfloor n - (y - \lfloor y/n \rfloor n) = (q - \lfloor x/n \rfloor + \lfloor y/n \rfloor)n$. Thus $(x \bmod n) - (y \bmod n)$ is a multiple of n. On the the other hand $|(x \bmod n) - (y \bmod n)| < n$ and hence $x \bmod n = y \bmod n$.

2. Let a and n be relatively prime integers and let i be an arbitrary integer. Prove: if $n|ia$ then $n|i$.

   Solution: Let $n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}$ be the prime factor decomposition of n. Since there is no prime that divides a and n we conclude that n divides i.