Chapter 27 Modular Arithmetic

Def Let $n \in \mathbb{Z}$ such that $n > 1$, and let $x, y \in \mathbb{Z}$.
We say x is congruent to y modulo n if
$n \mid (y - x)$. Notation: $x \equiv y \pmod{n}$.

Remark notice $x \equiv y \pmod{n}$ means $\exists\ k \in \mathbb{Z}$ such that $nk = y - x \iff y = nk + x$
$\iff x = n\ell + y$ where $\ell = -k$.

So x can be decomposed as a sum of (1) a multiple of n and (2) y, and vice versa.

Example Find 5 different solutions to the following:

(a) find $x \in \mathbb{Z}$ such that $5 \equiv x \pmod{12}$

(b) find $x \in \mathbb{Z}$ and $x > 1$ such that $-3 \equiv 39 \pmod{x}$.

(a) $\{\ldots, -19, -7, 5, 17, 29, \ldots\}$ (these are values of x such that $x - 5$ is a multiple of 12)

(b) $\{2, 3, 6, 7, 14, 21, 42\}$ (these are values of x which divide $39 - (-3) = 42$)

Theorem Let $n \in \mathbb{Z}$ with $n > 1$. The relation on $\mathbb{Z}$ given by $x \sim y$ if and only if $x \equiv y \pmod{n}$ is an equivalence relation (called congruence modulo n).

Example Let $m \in \mathbb{Z}$. The equivalence class of m under congruence modulo n is denoted

$$[m]_n = \{ x \in \mathbb{Z} : m \equiv x \pmod{n} \}.$$

Find $[0]_4$, $[1]_4$, $[2]_4$, $[3]_4$, $[4]_4$, $[5]_4$.

$[0]_4 = \{ \ldots, -8, -4, 0, 4, 8, 12, \ldots \}$

$[1]_4 = \{ \ldots, -7, -3, 1, 5, 9, 13, \ldots \}$

$[2]_4 = \{ \ldots, -6, -2, 2, 6, 10, 14, \ldots \}$

$[3]_4 = \{ \ldots, -5, -1, 3, 7, 11, 15, \ldots \}$

$[4]_4 = [0]_4 = \{ \ldots, -8, -4, 0, 4, 8, 12, \ldots \}$

$[5]_4 = [1]_4 = \{ \ldots, -7, -3, 1, 5, 9, 13, \ldots \}$

Def The set of all equivalence classes under congruence modulo n is called the integers modulo n and is denote $\mathbb{Z}_n$. (This forms a partition on $\mathbb{Z}$).

Example $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$.

Modular arithmetic is the algebraic study (eg. addition, multiplication, equation solving) of $\mathbb{Z}_n$.

Theorem (Division Algorithm) For every $m, n \in \mathbb{Z}$ with $n \neq 0$, there exists unique $q, r \in \mathbb{Z}$ such that $m = nq + r$ and $0 \leq r < |n|$.

Proof Let $m, n \in \mathbb{Z}$ with $n \neq 0$. We consider the case when $n > 0$.

$$A = \{m - nx : x \in \mathbb{Z},\ m - nx \geq 0\}.$$

We claim A is non-empty. If $m \geq 0$, then $m \in A$ since $m = m - n \cdot 0 \in A$. Suppose $m < 0$. Since $n \geq 1$, for $x = m$, $m - nx \geq m - 1 \cdot m = 0$. Thus our claim holds.

Since $A \subseteq \mathbb{N}$ is non-empty, by the Well-Ordering Principle of $\mathbb{N}$, A has a minimum, $r = \min A$.

We claim $0 \le r < n$. Since $r \in A$, $r \ge 0$. Suppose $r \ge n$.

Then since $r \in A$, there exists $q \in \mathbb{Z}$ such that

$r = m - nq \ge n$. This implies $m - n(q+1) \ge 0$.

But since $m - n(q+1) < m - nq = r$, this contradicts

r was the smallest element of A. Thus we

have shown there exists $q, r \in \mathbb{Z}$ such that

$$m = nq + r \quad \text{with} \quad 0 \le r < n.$$

To show uniqueness, suppose $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ such

that $m = nq_1 + r_1 \quad 0 \le r_1 < n$

and $m = nq_2 + r_2 \quad 0 \le r_2 < n$.

Therefore $nq_1 + r_1 = nq_2 + r_2$, which implies

$n \mid (r_1 - r_2)$ since $n(q_2 - q_1) = r_1 - r_2$. Since $0 \le r_1 < n$

and $0 \le r_2 < n$, $0 \le |r_1 - r_2| < n$. The only way for

$|r_1 - r_2|$ to be a multiple of n and $0 \le |r_1 - r_2| < n$

is if $|r_1 - r_2| = 0$, ie. $r_1 = r_2$. Therefore since

$nq_1 + r_1 = nq_2 + r_2$, this implies $nq_1 = nq_2$ and so $q_1 = q_2$

since $n \neq 0$. Thus q and r are unique.