Chapter 19 - Congruence of Integers

Recall that the Division Theorem states that given $a, b \in \mathbb{Z}$ with $b > 0$ there exist unique integers q, r with

$$a = bq + r \quad \text{and} \quad \underbrace{0 \leq r < b}_{\text{i.e. } r \in \{0, 1, \ldots, b-1\}}.$$

We refer to r as the remainder when a is divided by b.

Def^n: For each $m \in \mathbb{N}$ we define the map $r_m : \mathbb{Z} \longrightarrow \{0, 1, \ldots, m-1\}$ by $a \mapsto r_m(a)$ where $r_m(a)$ is the remainder when a is divided by m.

Def^n: The set $R_m = \{0, 1, \ldots, m-1\}$ is called the set of remainders upon division by m (or the set of residues modulo m). The map $r_m : \mathbb{Z} \to R_m$ is called the remainder map for division by m.

Example: Consider $r_4 : \mathbb{Z} \to \{0,1,2,3\}$.

We have

$$
\begin{array}{ll}
\vdots & \\
r_4(-4) = 0 & r_4(4) = 0 \\
r_4(-3) = 1 & r_4(5) = 1 \\
r_4(-2) = 2 & r_4(6) = 2 \\
r_4(-1) = 3 & r_4(7) = 3 \\
r_4(0) = 0 & r_4(8) = 0 \\
r_4(1) = 1 & r_4(9) = 1 \\
r_4(2) = 2 & r_4(10) = 2 \\
r_4(3) = 3 & r_4(11) = 3 \\
 & \vdots
\end{array}
$$

Def^n: Let $m \in \mathbb{N}$ (usually $m > 1$).

We say that integers a and b are congruent modulo m, written

$$a \equiv b \mod m,$$

When the "mod m" is clear from the context we sometimes just write $a \equiv b$.

if a and b have the same remainder upon division by m, i.e. if $r_m(a) = r_m(b)$.

Usually we work with this definition

Equivalently, we say that $a \equiv b \mod m$ if $a - b$ is an integer multiple of m, i.e. m divides $a - b$.

Examples:

- $6 \equiv 2 \mod 4$, $15 \equiv 7 \equiv 3 \mod 4$
- $6 \equiv 1 \mod 5$, $15 \equiv 0 \mod 5$

The following properties are immediate from the definition.

Proposition: Let $m \in \mathbb{N}$.

(i) Reflexive property: $\forall a \in \mathbb{Z}$, $a \equiv a \bmod m$.

(ii) Symmetric property: $\forall a, b \in \mathbb{Z}$,

$a \equiv b \bmod m \Rightarrow b \equiv a \bmod m$.

(iii) Transitive property: $\forall a, b, c \in \mathbb{Z}$,

$(a \equiv b \bmod m$ and $b \equiv c \bmod m) \Rightarrow a \equiv c \bmod m$.

($r_m(a) = r_m(b)$, $r_m(b) = r_m(c)$, $r_m(a) = r_m(c)$)

Our main aim now is to understand how arithmetic works "modulo m".

Proposition (Modular Arithmetic):
Let $m \in \mathbb{N}$ and $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ s.t.
$a_1 \equiv a_2 \bmod m$ and $b_1 \equiv b_2 \bmod m$.
Then

(i) $a_1 + b_1 \equiv a_2 + b_2 \bmod m$;

(ii) $a_1 - b_1 \equiv a_2 - b_2 \bmod m$;

(iii) $a_1 b_1 \equiv a_2 b_2 \bmod m$.

Proof: Since $a_1 \equiv a_2 \bmod m$ and $b_1 \equiv b_2 \bmod m$, $\exists\, q, q' \in \mathbb{Z}$ s.t. $a_1 = a_2 + qm$ and $b_1 = b_2 + q'm$. Hence

$$a_1 + b_1 = a_2 + b_2 + (q+q')m \equiv a_2 + b_2 \bmod m;$$

$$a_1 - b_1 = a_2 - b_2 + (q-q')m \equiv a_2 - b_2 \bmod m;$$

$$a_1 b_1 = (a_2 + qm)(b_2 + q'm) = a_2 b_2 + (a_2 q' + b_2 q + mqq')m$$
$$\equiv a_2 b_2 \bmod m.$$

□

Corollary: Let $m, n \in \mathbb{N}$, $a, b \in \mathbb{Z}$.
If $a \equiv b \bmod m$, then $a^n \equiv b^n \bmod m$.

Example:

- Find the remainder when $97^3 + 144^2$ is divided by 5.

$$\begin{cases} 97 \equiv 2 \bmod 5 \\ 97^3 \equiv 2^3 \equiv 8 \equiv 3 \bmod 5 \\ 144 \equiv 4 \bmod 5 \\ 144^2 \equiv 4^2 \equiv 16 \equiv 1 \bmod 5 \end{cases}$$

$$\rightarrow 97^3 + 144^2 \equiv 3 + 1 \equiv 4 \bmod 5$$

↳ i.e. $r_5(97^3 + 144^2) = 4$

Proposition:
Let $k \in \mathbb{Z}$, then $r_4(k^2)$ is 0 or 1.

Proof: Note that $r_4(k) \in \{0, 1, 2, 3\}$. So we have four cases to consider.

Case 1: If $k \equiv 0 \bmod 4$ then

$$k^2 \equiv 0^2 \equiv 0 \bmod 4.$$

Case 2: If $k \equiv 1 \bmod 4$ then

$$k^2 \equiv 1^2 \equiv 1 \bmod 4.$$

Case 3: If $k \equiv 2 \bmod 4$ then

$$k^2 \equiv 2^2 \equiv 4 \equiv 0 \bmod 4.$$

Case 4: If $k \equiv 3 \bmod 4$ then

$$k^2 \equiv 3^2 \equiv 9 \equiv 1 \bmod 4.$$

In any case $r_4(k^2)$ is 0 or 1. □

Example: Prove that $m^2+n^2 = 1234567$ has no integer solutions.

Proof: For $m,n \in \mathbb{Z}$, $r_4(m^2+n^2)$ is 0, 1 or 2. But

0 or 1 plus 0 or 1 → 0, 1 or 2.

since $r_4(m^2) = 0$ or 1 & $r_4(n^2) = 0$ or 1

$$1234567 = 12345 \times 100 + 67 \equiv 3 \bmod 4.$$

($100 = 25 \times 4$)

□

Proposition: Let $a, m \in \mathbb{N}$. Then, for any $b_1, b_2 \in \mathbb{Z}$,

$$ab_1 \equiv ab_2 \bmod am \iff b_1 \equiv b_2 \bmod m.$$

Proof: By the definition of congruence

$$ab_1 \equiv ab_2 \bmod am \iff \exists q \in \mathbb{Z} \text{ s.t. } ab_1 - ab_2 = qam$$
$$\iff \exists q \in \mathbb{Z} \text{ s.t. } b_1 - b_2 = qm$$

$\iff b_1 \equiv b_2 \bmod m.$ □

Example: For $x \in \mathbb{Z}$,

(i) $4x \equiv 12 \bmod 16 \iff x \equiv 3 \bmod 4$;

(ii) $4x \equiv 12 \bmod 14 \iff 2x \equiv 6 \bmod 7.$

Proposition 19.3.2: Let $m \in \mathbb{N}$, and $a \in \mathbb{Z}$ with $\gcd(a,m) = 1$. Then, for any $b_1, b_2 \in \mathbb{Z}$,

$ab_1 \equiv ab_2 \bmod m \iff b_1 \equiv b_2 \bmod m.$

Proof: Let $b_1, b_2 \in \mathbb{Z}$.

Forward implication: Suppose $ab_1 \equiv ab_2 \bmod m$.

Then m divides $ab_1 - ab_2 = a(b_1 - b_2)$.

But then, since $\gcd(a,m) = 1$, m divides $b_1 - b_2$. That is, $b_1 \equiv b_2 \bmod m$.

Reverse implication: Suppose m divides $b_1 - b_2$.

Then m divides $a(b_1 - b_2) = ab_1 - ab_2$.

So $ab_1 \equiv ab_2 \bmod m$. □

Example: For $x \in \mathbb{Z}$,

$2x \equiv 6 \bmod 7 \iff x \equiv 3 \bmod 7.$

Putting these two propositions together:

Example: For $x \in \mathbb{Z}$,

$$6x \equiv 15 \bmod 21 \iff 2x \equiv 5 \bmod 7$$
$$\iff 2x \equiv 12 \bmod 7 \quad (+7)$$
$$\iff x \equiv 6 \bmod 7.$$
