MATH453 Elementary Number Theory

Lecture 7: Congruence

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

7.1 Congruence

Definition 7.1. a is congruent to b modulo m for $m \in \mathbb{Z}^+$ iff

$$m \mid (a - b)$$

and we write $a \equiv b \mod m$.

For example, $3 \equiv 7 \mod 2$ because $3 - 7 = -4$ and $2 \mid -4$.

Remark. Note that despite that congruence is denoted by $\equiv$, some properties of equality does not hold. Importantly, $ca \equiv cb \mod m$ DOES NOT imply $a \equiv b \mod m$. For a simple counterexample, consider $4 \equiv 6 \mod 2$ but $2 \not\equiv 3 \mod 2$.

7.1.1 Properties of Congruence Relation

$$\begin{aligned}
&a \equiv a \mod m && \text{reflexive} \\
&a \equiv b \mod m \iff b \equiv a \mod m && \text{symmetric} \\
&a \equiv b \mod m \land b \equiv c \mod m \implies a \equiv c \mod m && \text{transitive}
\end{aligned}$$

The reflexive and symmetric properties are obvious. We will provide a short proof for the transitive property.

Proof. By definition of congruence, $a \equiv b \mod m$ means $m \mid (a - b)$. And $b \equiv c \mod m$ means $m \mid (b - c)$. It follows by property of divisibility that $m \mid (a - b + b - c)$. Then, $m \mid (a - c)$, which by definition means $a \equiv c \mod m$. ■

Because of these three properties, we say that congruence defines an **equivalence relation**. Hence, equivalence relation of congruence divides integers into **equivalence classes**, known as the **congruence classes** or **residue classes**.

7.1.2 Congruence Classes

Definition 7.2 (Congruence Classes)**.** The congruence class of a modulo m, denoted $[a]_m$, is the set of all integers that are congruent to a modulo m

$$\{z \in \mathbb{Z} \mid m \mid (a - z)\}$$

Example. Let $m = 7$. Then,

$$[0]_7 = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$$
$$[1]_7 = \{\ldots, -13, -6, 1, 8, 15, \ldots\}$$
$$[2]_7 = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$$
$$[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$$

Definition 7.3 (Complete Residue System)**.** A complete residue system modulo m is a set S of integers such that every $n \in \mathbb{Z}$ is congruent to one and only one member of S.

Example. $\{0, 1, 2, 3, 4, 5, 6\}$ is a complete residue system modulo 7.
Although less obvious, $\{14, 57, -12, 1060, -24, -2, 76\}$ is also a complete residue system modulo 7.

Proposition 7.1. $S = \{0, 1, \ldots, m-1\}$ is a complete residue system modulo m.

Proof. Let $a \in \mathbb{Z}$. Apply the division algorithm to a with respect to m, so we have

$$a = mq + r \qquad 0 \le r \le m-1$$

By definition of divisibility, $m \mid (a - r)$, and by definition of congruence, $a \equiv r \mod m$. This shows that every integer is congruent to a member r of $\{0, 1, \ldots, m-1\}$.

We also need to show that a is congruent to only one member of $\{0, 1, \ldots, m-1\}$. We proceed by contradiction. Assume $a \equiv r_1 \mod m$ and $a \equiv r_2 \mod m$ for some $r_1, r_2 \in \{0, 1, \ldots, m-1\}$. By transitivity, $r_1 \equiv r_2 \mod m$, which by definition means $m \mid (r_1 - r_2)$. Since both r_1 and r_2 are between 0 and $m-1$, $0 \le r_1 - r_2 \le m-1$. Then, $0 \le r_1 - r_2 \le m-1$ and $m \mid (r_1 - r_2)$ imply that $r_1 - r_2 = 0$ because otherwise m cannot divide any non-zero integers less than itself. This shows that $r_1 = r_2$ and thus uniqueness. ■

Proposition 7.2. Let $a, b, c, d \in \mathbb{Z}$. If $a \equiv b \mod m$ and $c \equiv d \mod m$, then

$$a + c \equiv b + d \mod m \tag{7.1}$$

$$ac \equiv bd \mod m \tag{7.2}$$

Proof. of Equation (7.1)

By definition of congruence, $m \mid (a - b)$ and $m \mid (c - d)$. By property of divisibility, $m \mid (a - b + c - d)$. This is equivalence to $m \mid [(a + c) - (b + d)]$, which by definition means $a + c \equiv b + d \mod m$. ■

Proof. of Equation (7.2)

By definition, $m \mid (a - b)$ and $m \mid (c - d)$. Trivially, it follows that $m \mid c(a - b)$. Similarly, $m \mid b(c - d)$. By property of divisibility, $m \mid (ca - cb + bc - bd)$ so $m \mid (ac - bd)$. This by definition means $ac \equiv bd \mod m$. ■