6. Congruences

Definition. Fix an integer $n \geq 2$. Given $a, b \in \mathbb{Z}$, we say that a and b are congruent mod n and write $a \equiv b \mod n$ if $n \mid (b - a)$.

Note that

$$a \equiv b \mod n \iff n \mid (b-a) \iff b = a + nk \text{ for some } k \in \mathbb{Z}.$$

We started by discussing basic properties of congruences. The proofs of the following four theorems are given in Section 2.5 of the book. In all these theorems n is a fixed integer ≥ 2.

Theorem 6.1 (Congruence is an equivalence relation)**.** *The following hold:*

(i) $x \equiv x \mod n$ *for all* $x \in \mathbb{Z}$

(ii) *If* $x \equiv y \mod n$ *for some* $x, y \in \mathbb{Z}$*, then* $y \equiv x \mod n$

(iii) *If* $x \equiv y \mod n$ *and* $y \equiv z \mod n$ *for some* $x, y, z \in \mathbb{Z}$*, then* $x \equiv z \mod n$*.*

Theorem 6.2. *Suppose* $x \equiv y \mod n$ *for some* $x, y \in \mathbb{Z}$*. Then* $x+z \equiv y+z \mod n$ *and* $xz \equiv yz \mod n$ *for all* $z \in \mathbb{Z}$

Theorem 6.3 (Congruences can be added or multiplied)**.** *Suppose* $x \equiv y \mod n$ *and* $z \equiv w \mod n$ *for some* $x, y, z, w \in \mathbb{Z}$*. Then* $x + z \equiv y + w \mod n$ *and* $xz \equiv yw \mod n$*.*

Theorem 6.4 (Cancellation law)**.** *Suppose* a *and* n *are coprime and* $x, y \in \mathbb{Z}$*. Then* $ax \equiv ay \mod n \iff x \equiv y \mod n$*.*

Note that cancellation law is not valid if a and n are not coprime. For instance, $2 \cdot 3 \equiv 2 \cdot 0 \mod 6$ but $3 \not\equiv 0 \mod 6$.

We proceeded with solving two explicit congruences.

Example 1. *Find all* $x \in \mathbb{Z}$ *such that* $6x \equiv 30 \mod 151$*.*

This example can be solved directly by cancellation law since $30 = 6 \cdot 5$ and $gcd(6, 151) = 1$. The general solution is $x = 5 + 151k$ with $k \in \mathbb{Z}$.

Example 2. *Find all* $x \in \mathbb{Z}$ *such that* $6x \equiv 4 \mod 151$*.*

We solved this example using the Euclidean algorithm for representing $gcd(a, b)$ as an integer linear combination of a and b (see Example 2 on page 104 of the book). The general solution here is $x = -100 + 151k$ with $k \in \mathbb{Z}$.

Theorem 6.5. *Let $a, b, n \in \mathbb{Z}$ with $n \geq 2$, and assume that a and n are coprime. Then the congruence $ax \equiv b \mod n$ always has a solution, and if x_0 is a particular solution, then the general solution is $x = x_0 + nk$ with $k \in \mathbb{Z}$.*

Proof. See Theorem 2.26 in Section 2.5 of the book. □

We finished the lecture with an application of congruences (see Lecture 7 for continuation).

Lemma 6.6. *For any $x \in \mathbb{Z}$ we have $x^2 \equiv 0$ or 1 mod 4.*

Proof. Divide x by 4 with remainder: $x = 4q + r$. We claim that $x^2 \equiv r^2 \mod 4$. Indeed, $x^2 = (4q + r)^2 = 16q^2 + 8qr + r^2 = 4(4q^2 + 2qr) + r^2$, so $x^2 \equiv r^2 \mod 4$. Alternatively $x = 4q + r$ implies that $x \equiv r \mod 4$, and squaring this congruence (which we can do by Theorem 6.3), we get $x^2 \equiv r^2 \mod 4$.

Since r can only equal $0, 1, 2$ or 3, there are 4 possible cases:

Case 1: $r = 0$. Then $r^2 = 0$, so $x^2 \equiv 0 \mod 4$, as desired.

Case 2: $r = 1$. Then $r^2 = 1$, so $x^2 \equiv 1 \mod 4$

Case 3: $r = 2$. Then $r^2 = 4$. Since $4 \equiv 0 \mod 4$, using transitivity, we get $x^2 \equiv 0 \mod 4$

Case 4: $r = 3$. Then $r^2 = 9 \equiv 1 \mod 4$, so $x^2 \equiv 1 \mod 4$.

Thus, we showed that in all possible cases $x^2 \equiv 0$ or 1 mod 4. □