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

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

We started with basic properties of congruences. In all four theorems below 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* $x \equiv z \mod n$*.*

Proof. One can prove properties (i)-(iii) using divisibility properties from Lecture 4, but it is more convenient to deduce them directly from the fact that $a \equiv b \mod n \iff b - a = nk$ for some $k \in \mathbb{Z}$.

(i) $x \equiv x \mod n$ since $x - x = 0 = n \cdot 0$.

(ii) Suppose $x \equiv y \mod n$. Then $y - x = nk$ for some $k \in \mathbb{Z}$, so $x - y = -nk = n(-k)$, so $y \equiv x \mod n$

(iii) Suppose $x \equiv y \mod n$ and $y \equiv z \mod n$. Then $y - x = nk$ and $z - y = nl$ for some $k, l \in \mathbb{Z}$, whence $z - x = nk + nl = n(k+l)$, so $x \equiv z \mod n$. □

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* $z \in \mathbb{Z}$

Proof. We are given that $x \equiv y \mod n$, so $y - x = nk$ for some $k \in \mathbb{Z}$. Then $(y+z) - (x+z) = y - x = nk$, so $x + z \equiv y + z \mod n$. Also $yz - xz = (y-x)z = n(kz)$, so $xz \equiv yz \mod n$. □

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* $xz \equiv yw \mod n$*.*

Proof. We can prove this theorem directly from the definition of congruences, just as we did in Theorems 6.1 and 6.2, but it will be more convenient to use the results of the two previous theorems instead.

Since $x \equiv y \mod n$ and $z \equiv w \mod n$, using Theorem 6.2 we get $x+z \equiv y+z \mod n$ (from the first congruence) and $y+z \equiv y+w \mod n$ (from the second congruence). Using transitivity of congruences (Theorem 6.1(iii)), we deduce that $x + z \equiv y + w \mod n$.

The proof of the congruence $xz \equiv yw \mod n$ is analogous. □

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

Proof. "$\Leftarrow$" This direction follows directly from Theorem 6.3.

"$\Rightarrow$" Suppose $ax \equiv ay \mod n$, so $n \mid (ay - ax) = a(y - x)$. Since a and n are coprime, applying the Coprime Lemma (Lemma 5.1), we deduce that $n \mid (y - x)$, so $x \equiv y \mod n$. □

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 proceed with solving two explicit congruences.

Example 1. *Find all $x \in \mathbb{Z}$ such that $12x \equiv 36 \mod 151$.*

Since $36 = 12 \cdot 3$ and $gcd(12, 151) = 1$, by cancellation law this congruence is equivalent to $x \equiv 3 \mod 151$. Thus the general solution is $x = 3 + 151k$ with $k \in \mathbb{Z}$.

Example 2. *Find all $x \in \mathbb{Z}$ such that $9x \equiv 2 \mod 149$.*

Here we cannot apply the cancellation law since 4 is not divisible by 9; so instead we proceed with the definition of a congruence relation.

We have $9x \equiv 2 \mod 149 \iff 2 - 9x = 149m$ for some $m \in \mathbb{Z} \iff 9x + 149m = 2$ for some $m \in \mathbb{Z}$. Rather than find all pairs (x, m) satisfying this equation, we will find one such pair (in fact, we just need the value of x) and then use it to describe all the solutions applying Theorem 6.5 below.

It turns out that x and m as above can be found using the Euclidean algorithm discussed in Lecture 4. First we find $u, v \in \mathbb{Z}$ such that $9u+149v = 1$ (such u and v exist since $gcd(9, 149) = 1$).

We have $149 = 9 \cdot 16 + 5$; $9 = 5 \cdot 1 + 4$; $5 = 4 \cdot 1 + 1$; whence $1 = 5 - 4 \cdot 1 = 5 - (9 - 5) = 5 \cdot 2 - 9 = (149 - 9 \cdot 16) \cdot 2 - 9 = 149 \cdot 2 - 9 \cdot 33$.

So $1 = 9 \cdot (-33) + 149 \cdot 2$. Multiplying both sides by 2, we get $2 = 9 \cdot (-66) + 149 \cdot 4$. Thus, the equation $9x + 149m = 2$ has a particular solution $x = -66$, $m = 4$, so $x = -66$ is a particular solution to the congruence $9x \equiv 2 \mod 149$.

We claim that the general solution to our congruence is $x = -66 + 149k$ with $k \in \mathbb{Z}$. This follows from Theorem 6.5 below.

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. Existence: we proceed as we did in the above example. Since a and n are coprime, by GCD Theorem there exist $u, v \in \mathbb{Z}$ such that $au + nv = 1$. Multiplying both sides by b, we get $a(ub) + n(vb) = b$. If we set $x_0 = ub$, then $b - ax_0 = n(vb)$, so $ax_0 \equiv b$ and x_0 is a particular solution.

Now we prove that if we are given any $x \in \mathbb{Z}$, then x is a solution $\iff$ $x = x_0 + nk$ for some $k \in \mathbb{Z}$. Indeed, we have

$$\begin{aligned} ax \equiv b \mod n &\iff ax \equiv ax_0 \mod n && \text{by transitivity} \\ & && \text{(since we know that } ax_0 \equiv b \mod n\text{)}, \\ ax \equiv ax_0 \mod n &\iff x \equiv x_0 \mod n && \text{by cancellation law,} \end{aligned}$$

and finally $x \equiv x_0 \mod n \iff x = x_0 + nk$ for some $k \in \mathbb{Z}$ as observed at the beginning of the lecture. □

Remark: Note that the general solution can be expressed in the form $x_0 + nk$, $k \in \mathbb{Z}$, for any particular solution x_0. In Example 2 above we initially found -66 to be a particular solution, so the general solution is $-66 + 149k$. Setting $k = 1$, we get that $-66 + 149k = 83$ is also a solution. Thus, we can also say that the general solution has the form $x = 83 + 149k$, $k \in \mathbb{Z}$ (of course, k in the last formula is not the same as k in the formula $x = -66 + 149k$).

We finish 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. □

6.1. **Book references.** This lecture follows [Gilbert, 2.5] quite closely. Pinter's book introduces congruences in Chapter 23; however, it contains almost no discussion of the algorithm for solving congruences.