Last time: Congruences

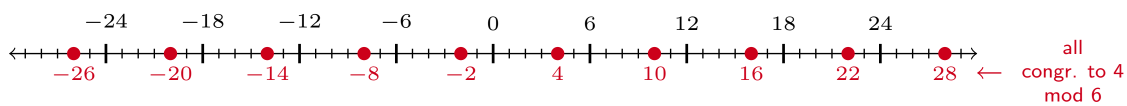
For integers a, b, we say a is congruent to b modulo (mod) n, written

$$a \equiv b \pmod{n} \quad \text{or} \quad a \equiv_n b,$$

if a and b have the same remainders when divided by n.

Equivalently: $a \equiv b \pmod{n}$ if and only if n divides $a - b$.

Example: The numbers that are equivalent to 4 modulo 6 are



Some properties: Fix $n \geqslant 1$.

1. "Congruent" is an equivalence relation. The least residue of a modulo n is the remainder when a is divided by n. (This is the *favorite representative* of all numbers that are congruent to a mod n.)
2. If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then
   (a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and
   (b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Arithmetic

If $a_1 \equiv b_1 \pmod{n}$ and $a_2 \equiv b_2 \pmod{n}$, then

(a) $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, and

(b) $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Division. In the integers, suppose you want to solve

$$ax = b, \qquad a, b \in \mathbb{Z}.$$

Either $b/a \in \mathbb{Z}$, or there is no solution.

In modular arithmetic, there are three possibilities:
The equation $ax \equiv b \pmod{n}$ either

1. has no solutions;
2. has one solution (up to congruence);
3. has multiple solutions (up to congruence).

Here, up to congruence means that we consider two solutions $x_1 \neq x_2$ to be the "same" if $x_1 \equiv x_2 \pmod{n}$.
For example, $x = 2$ is a solution to $3x \equiv 6 \pmod{10}$. But so are

$$12,\ 22,\ 31,\ \ldots, \quad \text{as well as} \quad -8,\ -18,\ -28,\ \ldots.$$

Division

On the homework, you prove that if $\gcd(c, n) = 1$, then

$$ac \equiv bc \pmod{n} \quad \text{implies} \quad a \equiv b \pmod{n}.$$

This turns out to be an if and only if:

Claim: if $\gcd(c, n) \neq 1$, then there are a and b such that

$$ac \equiv bc \pmod{n} \quad \text{but} \quad a \not\equiv b \pmod{n}.$$

Proof: Letting $\gcd(n, c) = g > 1$, there are $2 \leqslant k < n$ and $2 \leqslant \ell < c$ such that $kg = n$ and $\ell g = c$. So $ck = \ell gk = \ell n$. Therefore

$$ck \equiv_n 0 \equiv_n c \cdot 0.$$

But since $2 \leqslant k < n$, $k \not\equiv 0 \pmod{0}$.

Solving congruences

Solving congruences: If $a + x \equiv b \pmod{n}$, then

$$x \equiv_n a + x - a \equiv_n b - a.$$

Again, solving equations with multiplication is trickier!

Example: $4x = 8 \pmod{7}$.
Since $\gcd(4, 7) = 1$, and $8 \equiv_7 4 \cdot 2$, we have $x = 2 \pmod{7}$.

Example: $4x = 8 \pmod{10}$.
Since $\gcd(4, 10) = 2$, we end up having several solutions...

Again: If $a = qn + r$ with $0 \leqslant r < n$, then we call r the least residue of a mod n. And if x is a solution to a congruence, then so are $x + nk$ for all $k \in \mathbb{Z}$ (homework). So we only really care about the least residue solutions.

---

x	0	1	$\boxed{2}$	3	4	5	6	$\boxed{7}$	8	9
$4x$	0	4	8	12	16	20	24	28	32	36
least residue	0	4	$\boxed{8}$	2	6	0	4	$\boxed{8}$	2	6

Division

Example: Solve $4x \equiv 3 \pmod{19}$.
"Dividing by 4" becomes "multiply by m s.t. $4m \equiv 1 \pmod{19}$.

If $\gcd(a,n) = 1$, then there are $k, \ell \in \mathbb{Z}$ satisfying

$$ka + \ell n = 1. \quad \text{So } 1 - ka = \ell n, \quad \text{implying } ka \equiv_n 1.$$

Therefore

$$\text{if } ax \equiv b \pmod{n}, \quad \text{then} \quad x \equiv_n kax \equiv kb.$$

In our example above, $5 \cdot 4 = 20 \equiv 1 \pmod{19}$. So

$$x \equiv_{19} 5 \cdot 4 \cdot x \equiv_{19} 5 \cdot 3 \equiv_{19} 15.$$

If $\gcd(a,n) = 1$ and $ax \equiv b \pmod{n}$, then

1. compute $1 \leqslant k < n$ such that $ka \equiv 1 \pmod{n}$, so that
2. $x \equiv kb \pmod{n}$.

You try: Compute x such that

(1) $3x \equiv 7 \pmod{10}$ (2) $5x \equiv 2 \pmod{9}$

and check your answer.

Division

Example: Solve $4x \equiv 3 \pmod 6$.
This is equivalent to

$$6|(4x-3). \qquad \text{This is not possible!}$$

Note that

$$ax \equiv b \pmod n \quad \text{iff} \quad n|(ax-b), \quad \text{i.e. } ax-b=nk,$$

for some $k \in \mathbb{Z}$. Therefore

$$ax \equiv b \pmod n \quad \text{if and only if} \quad b = ax - nk.$$

Now, suppose $\gcd(a,n) = d > 1$. Then $d|a$ and $d|n$ imply $d|b$.
Therefore,
if $\gcd(a,n) \nmid b$, then there is no solution to $ax \equiv b \pmod n$.

Division

Example: Solve $4x \equiv 2 \pmod 6$.

x	0	1	$\boxed{2}$	3	4	$\boxed{5}$
$4x$	0	4	8	12	16	20
least residue	0	4	$\boxed{2}$	0	4	$\boxed{2}$

Suppose $\gcd(a,n) = d > 1$. Then
if $\gcd(a,n) \nmid b$, then there is no solution to $ax \equiv b \pmod n$.
Otherwise, $d|b$. So $b = dk$ for some $k \in \mathbb{Z}$. Let $u, v \in \mathbb{Z}$ satisfy

$$d = ua + vn. \quad \text{Then } b = dk = (ku)a + (kv)n.$$

Therefore $a(ku) \equiv b \pmod n$. (So $x = uk = u(b/d)$ is a solution.)

Recall all solutions to $u'a + v'n = d$ are of the form

$$u' = u + \ell(n/d) \quad \text{and} \quad v' = v - \ell(a/d).$$

All solutions: Find one solution $u, v \in \mathbb{Z}$ to $d = ua + vn$. If $d|b$, then the solutions to $ax \equiv b \pmod n$ are given by

$$x = u(b/d) + \ell(n/d), \qquad \text{for} \quad \ell = 0, 1, \ldots, d-1.$$

Nonlinear congruences

Theorem (Polynomial Roots Mod p Theorem)

Let p be prime in $\mathbb{Z}_{>0}$, and let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x],$$

with $n \geqslant 1$ and $p \nmid a_n$. Then the congruence

$$f(x) \equiv 0 \pmod{n}$$

has at most d incongruent solutions.