3.15: Three complete residue systems mod 4

Canonical: $\{0, 1, 2, 3\}$

Div. Alg.

Any $a \in \mathbb{Z}$, $a = 4q + r$, where $0 \le r \le 3$

$\rightarrow a - r = 4q$

$\rightarrow a \equiv r \pmod 4$

Another, containing negatives: $\{0, -1, -2, -3\}$

Complete residue system: Each $a \in \mathbb{Z}$ is congruent to exactly one of these numbers.

- a is a multiple of 4 $\Rightarrow a \equiv 0 \pmod 4$
- $a \equiv 1 \pmod 4 \Rightarrow a \equiv 1 - 0 \pmod 4$

  $\equiv 1 - 4 \pmod 4$

  $\equiv -3$
- $a \equiv 2 \pmod 4 \Rightarrow a \equiv 2 - 4 \pmod 4$

  $\equiv -2 \pmod 4$
- $a \equiv 3 \pmod 4 \Rightarrow a \equiv 3 - 4 \pmod 4$

  $\equiv -1 \pmod 4$

Another one, containing no 2 consecutive numbers

$\{0, 5, 2, 7\}$

Linear congruences

Goal: Given integers a and b, find all integers x satisfy

$$ax \equiv b \pmod{n}.$$

"Is it OK to divide both sides by a? What would that even mean?"

Finding all integer solutions x is overkill. Just find the ones in the CCRS.

(Reason: If x is a solution, then so is $x + kn$)

Ex: Find all solutions in the CCRS to

$$3x \equiv 25 \pmod{4}$$

$x = 3$

CCRS $= \{0, 1, 2, 3\}$

Brute force:
- $3(0) \equiv 0 \pmod{4}$
  $25 \equiv 1 \pmod{4}$ ✗
- $3(1) \equiv 3 \pmod{4}$ ✗
- $3(2) = 6 \equiv 2 \pmod{4}$ ✗
- $3(3) \equiv 9 \equiv 1 \pmod{4}$ ✓

Next HW: 3.18–3.20, 3.22

$24x \equiv 123 \pmod{213}$

Key idea: Solving $ax \equiv b \pmod{n}$

is "the same" as solving the equation

$ax + ny = b$. (Exam 2 #3)