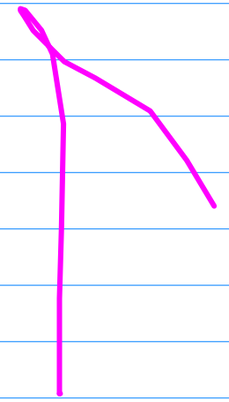
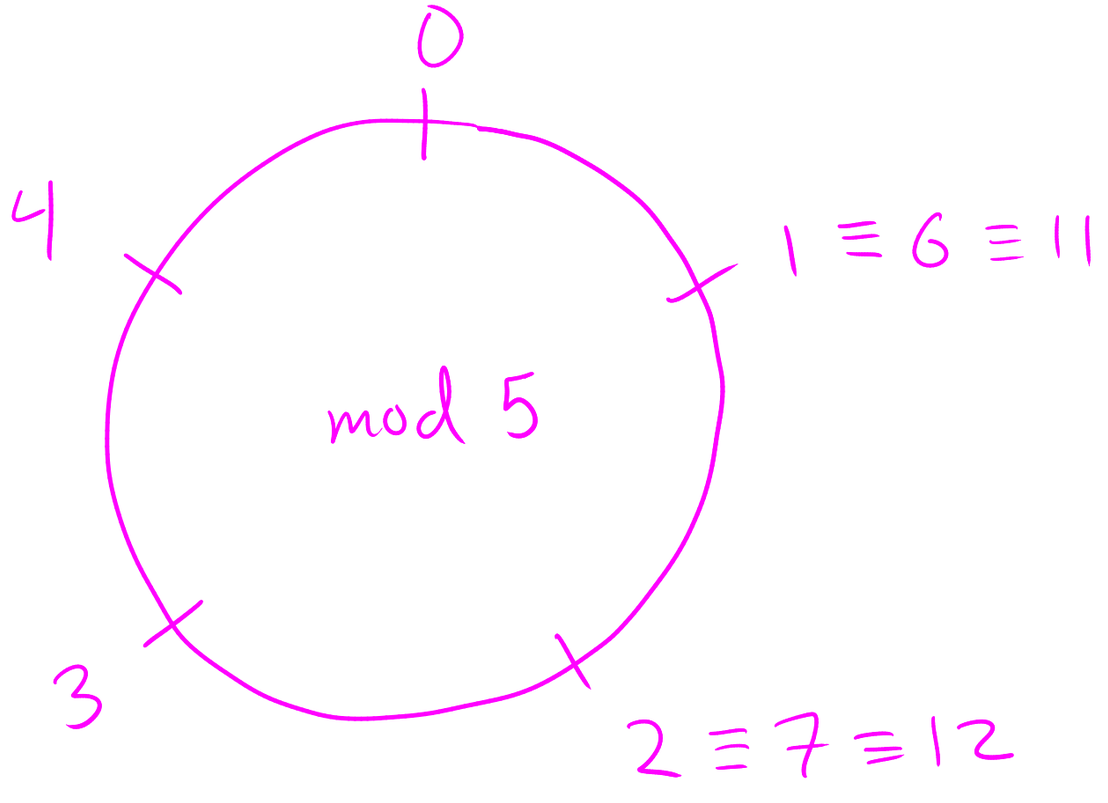


Modular Arithmetic



set of residues:

$$\mathbb{Z}/5\mathbb{Z} := \{0,1,2,3,4\}$$

Every integer is equivalent to exactly one element of $\mathbb{Z}/n\mathbb{Z}$ mod n.

Def^n Let $a, b, n \in \mathbb{Z}$, $n > 0$. We say that $a \equiv b \pmod{n}$ whenever $a = b + nk$ for some integer k.

Equivalently, • a & b differ by a mult. of n
• a & b have same remainder when we divide by n.

Write $\mathbb{Z}/n\mathbb{Z} := \{0, 1, \ldots, n-1\}$ "residues mod n"

Eg. $16 \equiv 1 \pmod 5$
$-1 \equiv 4 \pmod 5$

Addition & Multiplication

Theorem. If $a_1 \equiv a_2 \pmod n$
and $b_1 \equiv b_2 \pmod n$
then $a_1 + b_1 \equiv a_2 + b_2 \pmod n$
$a_1 b_1 \equiv a_2 b_2 \pmod n$

Example

$16 \equiv 1 \pmod 5$
$-3 \equiv 2 \pmod 5$

then $16 + (-3) \equiv 1 + 2 \pmod 5$

Check: 13 vs. 3 ✓

then $16 \cdot (-3) \equiv 1 \cdot 2 \pmod 5$

check: -48 vs. 2 ✓

Moral: You can reduce as you go.

Eg. $13^5 \cdot 701 \equiv (-1)^5 \cdot 1 \equiv (-1) \cdot 1 \equiv 6 \cdot 1 \equiv 6 \pmod 7$

Warning. What's wrong with this comp'n mod 7:

$6^{10} \equiv 6^{2} \cdot 6 \equiv 36 \cdot 6 \equiv 1 \cdot 6 \equiv 6$

(10 ≡ 3, via ×)

$6^{10} \equiv (-1)^{10} \equiv 1$

Moral: You can't reduce exponents mod n as you go.

Example. Alphabet A B C ⋯ Z
00 01 02 ⋯ 25
can be thought of as $\mathbb{Z}/26\mathbb{Z}$.

Caesar cipher: Key: shift $s \in \mathbb{Z}/26\mathbb{Z}$

Encrypt: $m \longmapsto m + s \pmod{26}$ m = message

Decrypt: $c \longmapsto c - s \pmod{26}$. c = ciphertext.