$n = 12$

## Examples of "$+_n$", "$\cdot_n$"

$$3 +_n 5 = (3+5) \bmod n$$
$$= 8 \bmod 12$$
$$= 8$$

$$7 +_n 8 = (7+8) \bmod 12$$
$$= 3$$

$$6 +_n 6 = (6+6) \bmod 12$$
$$= 0$$

$$2 \cdot_n 4 = (2 \cdot 4) \bmod n$$
$$= 8 \bmod 12$$
$$= 8$$

$$3 \cdot_n 4 = (3 \cdot 4) \bmod n$$
$$= 12 \bmod 12$$
$$= 0$$

$$3 \cdot_n 5 = 3$$

on-fly 1

# Theorem 2.4

* $+_n$ commutative

$$a +_n b = (a+b) \bmod n$$
$$= (b+a) \bmod n$$
$$= b +_n a$$

* $\cdot_n$ commutative

$$a \cdot_n b = (a \cdot b) \bmod n$$
$$= (b \cdot a) \bmod n$$
$$= b \cdot_n a$$

* $+_n$ Associative:

$$a +_n (b +_n c) = (a +_n b) +_n c$$

See slide for proof

* $\cdot_n$ associative

$$a \cdot_n (b \cdot_n c) = (a \cdot_n b) \cdot_n c$$

proof: Same as that for $+_n$

* Distributive law

$$(a +_n b) \cdot_n c = a \cdot_n c +_n b \cdot_n c$$

Can you prove this yourself?

# Caesar Cipher Example

* plaintext: SEA $\boxed{18 \quad 4 \quad 0}$

* Encrypt: $(n+13) \bmod 26$

$$\boxed{5 \quad 17 \quad 13}$$

* Decrypt: $(n'-13) \bmod 26$

$$(5-13) \bmod 26 = -8 \bmod 26$$
$$= 18$$

$$(-8 = 26 \cdot (-1) + 18)$$

$$(17-13) \bmod 26 = 4$$

$$(13-13) \bmod 26 = 0$$

Get back $\boxed{18 \quad 4 \quad 0}$

S E A

Encrypt: $f(x) = a \cdot_n x$

Decrypt ?

---

Naive idea :

$$a \cdot_n x = a \cdot x \mod n$$

Define:

$$x \div_n a = x \div n \mod n$$

Decrypt: $g(x') = x' \div_n a$

---

$n = 12, \quad a = 6$

$$x = 3 \xrightarrow{f} 6 \cdot 3 \mod 12 = 6$$

$$x' = 6 \xrightarrow{g} 6 \div 6 \mod 12 = 1$$

Don't get back 3 !

---

$\div_n$ not well defined

$$1 \div_n 6 = 1 \div 6 \mod n$$

$$= 0.166 \mod n$$

Not integer

If exists $b \in \mathbb{Z}_n$, s.t. $\underline{b \cdot_n a = 1}$,

can set:

$$g(x') = b \cdot_n x'$$

---

$$x \xrightarrow{f} a \cdot_n x$$

$$x' = a \cdot_n x \xrightarrow{g} b \cdot_n (a \cdot_n x)$$

$$= (b \cdot_n a) \cdot_n x$$

$$= 1 \cdot_n x$$

$$= x \quad \text{works!}$$

---

b: inverse of a in $\mathbb{Z}_n$

denoted by $a^{-1}$

---

$f^{-1}$ exist? $\quad a^{-1}$ exist?

# Conditions for public-key Crpto system to work

* $S_B(P_B(M)) = M$

* This is not easy

$$P_B,\ P_B(M) \Longrightarrow M;\ P_B \Longrightarrow S_B$$

Example of unsecure system

$P_B$: $\quad X \longrightarrow (X+11) \bmod 26$

$S_B$: $\quad X' \longrightarrow (X'-11) \bmod 26$

unsecure: can recover $X$ from

$P_B$, $\quad P_B(x)$

without knowing $S_B$