recap

Modular Arithmetic Basics

- closely tied with concept of remainder.
- $x \equiv y \pmod m \iff m \mid (x-y)$ ← x, y have the same remainder when divided by m
- no division → use multiplicative inverses instead. x is $y^{-1} \bmod m$ iff $xy \equiv 1 \bmod m$
- $1^{-1} \bmod m = 1$; $(m-1)^{-1} \bmod m = m-1$
- negative numbers (mod m) : "how much higher is it than the last multiple of m"
  $-32 \equiv 4 \pmod{12}$ b/c "last multiple" of 12 below -32 is -36)

if $a \equiv b \pmod m$, $c \equiv d \pmod m$ ...

$a+c \equiv b+d \pmod m$ | $a^k \equiv b^k \pmod m$

$ac \equiv bd \pmod m$ | $a^c \not\equiv a^d \pmod m$

Repeat Squaring

exponent should ~halve each time.

$$(26)^{30} \pmod 7$$

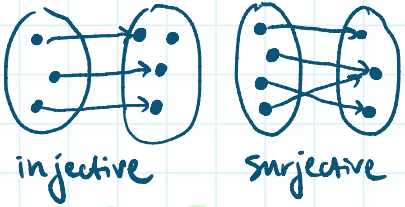
$$5^{30} \equiv (5^2)^{15} \equiv (4)^{15} \equiv 4 \cdot 4^{14} \equiv 4 \cdot (4^2)^7 \equiv 4 \cdot 2^7 \equiv 4 \cdot 2 \cdot 2^6$$

$$4 \cdot 2 \cdot 2^6 \equiv 4 \cdot 2 \cdot (2^2)^3 \equiv 4 \cdot 2 \cdot 4 \cdot 4^2 \equiv \underbrace{4 \cdot 2}_{8} \cdot \underbrace{4 \cdot 2}_{8} \equiv 1 \pmod 7$$

recap

Sets ... can be mapped using functions !

domain set of inputs
codomain set of possible outputs
range set of actual outputs
↳ aka image



$f: X \to Y$ maps each $x \in X$ to some $y \in Y$

injective at most one x mapped to each y
↳ aka one-to-one

surjective at least one x mapped to each y
↳ aka onto

bijection™ exactly one x mapped to each y
↳ f is bijection $\iff$ f has inverse function

to prove a bijection ... need to prove it is
- one-to-one AND onto OR
- one-to-one AND $|X| = |Y|$ OR
- onto AND $|X| = |Y|$

if $\gcd(a, m) = 1$, $f(x) = ax \pmod m$ $a, x \in \{0, \dots m-1\}$

- domain & range are from same set → same cardinality
- WTS injectivity: if $f(x) = f(x')$, $x = x'$. Show $(x \not\equiv x' \Rightarrow ax \not\equiv ax' \bmod m) \to P$
- assume $\neg P$: $x \not\equiv x' \wedge ax \equiv ax' \bmod m$
- $\exists a^{-1} \bmod m$ (b/c $\gcd(a, m) = 1$)

So we know $f(x)$ is injective.

$ax \equiv ax' \bmod p$

$a^{-1}ax \equiv a^{-1}ax' \bmod p$

$x \not\equiv x' \bmod p$. ↯