recap

Extended Euclidean Algorithm

old values: a', b'

new values: $a = b'$

$b = a' - b'\left(\left\lfloor \frac{x}{y} \right\rfloor\right)$

gcd(28, 11)	(1, 2, -5)
gcd(11, 6)	(1, -1, 2)
gcd(6, 5)	(1, 1, -1)
gcd(5, 1)	(1, 0, 1)
gcd(1, 0)	(1, 1, 0)
	d a b

$1 = (1)(6) + (-1)(5)$! :o

$d = ax + by$

gcd(32, 6)	(2, 1, -5)
gcd(6, 2)	(2, 0, 1)
gcd(2, 0)	(2, 1, 0)
	d a b

$2 = (1)(32) + (-5)(6)$ ✓

d will always be the gcd.

Inverses :/

$\gcd(x, y) = ax + by$

inverses iff $\gcd(x, y) = 1$

$1 = ax + by$

$1 \equiv ax + by \pmod{x}$

$1 \equiv by \pmod{x}$

b is $y^{-1} \bmod x$

$1 \equiv ax + by \pmod{y}$

$1 \equiv ax \pmod{y}$

a is $x^{-1} \bmod y$

gcd (28, 11) - (1, 2, -5)
gcd (11, 6) - (1, -1, 2)
gcd (6, 5) - (1, 1, -1)
gcd (5, 1) - (1, 0, 1)
gcd (1, 0) - (1, 1, 0)
d a b

$1 = (2)(28) + (-5)(11)$

$\gcd(x, y) = \gcd(y, x \bmod y)$

$d = ax + by$

old values:
a', b'

new values:

$a = b'$

$b = a' - b'\left(\left\lfloor \frac{x}{y} \right\rfloor\right)$

$1 - 0$

$0 - 1(1)$

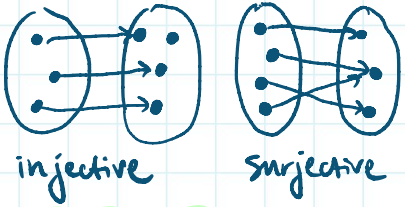
$1 - (-1)(1)$

$-1 - 2(2)$

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.

$ax \equiv ax' \bmod p$

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

$x \not\equiv x' \bmod p$. ↯

recap

Chinese Remainder Theorem

$n_1, n_2 \dots n_k$ coprime $\longrightarrow$ $N = n_1 \cdot n_2 \cdot \dots \cdot n_k$

for the system $x \equiv a_1 \mod n_1$

$\vdots$

$x \equiv a_k \mod n_k$

x is unique mod N and $x = \sum_{i=1}^{k} a_i b_i \mod N$

$$b_i = \frac{N}{n_i} \left(\frac{N}{n_i} \right)^{-1}_{n_i}$$

$\left(\frac{N}{n_i} \right)^{-1}_{n_i}$ ⟶ inverse of $\frac{N}{n_i}$, in mod n_i

recap

CRT Example.

$x \equiv 2 \mod 3$

$x \equiv 3 \mod 5$

$x \equiv 4 \mod 7$

① find x_1 st

70

$x \equiv 1 \mod 3$

✓ $0 \mod 5$

✓ $0 \mod 7$

② x_2 st

21

$x \equiv 0 \mod 3$

$1 \mod 5$

$0 \mod 7$

$21^{-1} \mod 5 = 1$

$x_2 = 21 \cdot 1$

③ x_3 st

15

$x \equiv 0 \mod 3$

$0 \mod 5$

$1 \mod 7$

$15^{-1} \mod 7 = 1$

$x_3 = 15 \cdot 1$

follow these steps to find each x_i

ⓐ first deal w/ the 0s.

x needs to be divisible by 5·7. $x = 35m$

ⓑ now deal with the 1 mod 3.

$\rightarrow 35m \equiv 1 \mod 3$

m is $35^{-1} \mod 3$

$\equiv 2.$

$x = 35 \cdot 2 = 70$

$x \equiv 1 \mod 3$

$0 \mod 5$

$0 \mod 7$

70 meets these constraints

④ $x = 2(x_1) + 3(x_2) + 4(x_3) \pmod{3 \cdot 5 \cdot 7}$ **53**

recap

Basis Vectors

in linear algebra, you can build any vector as a linear combination of basis vectors

$$\begin{bmatrix} x \\ y \\ z \end{bmatrix} = x\underbrace{\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}}_{v_1} + y\underbrace{\begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}}_{v_2} + z\underbrace{\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}}_{v_3}$$

Similarity to CRT

$$k \equiv a_1 \mod n_1$$
$$k \equiv a_2 \mod n_2$$
$$k \equiv a_3 \mod n_3$$

find k.

$(N = n_1 \cdot n_2 \cdot n_3)$

$$v_1 \equiv 1 \mod n_1 \equiv 0 \mod n_2 \equiv 0 \mod n_3$$

$$v_2 \equiv 0 \mod n_1 \equiv 1 \mod n_2 \equiv 0 \mod n_3$$

$$v_3 \equiv 0 \mod n_1 \equiv 0 \mod n_2 \equiv 1 \mod n_3$$

$$k = a_1 v_1 + a_2 v_2 + a_3 v_3 \pmod N$$

CRT

$x \equiv 5 \pmod{17}$

$x \equiv 3 \pmod{11}$

$x \equiv 2 \pmod{9}$

$x_1 = 1089$

$x_2 = 1530$

$x_3 = 187 \cdot 4 = 748$

$x_1 \equiv 1 \pmod{17}$ ←

$0 \pmod{11}$ ←

$0 \pmod{9}$ ←

$x_1 = 99m$ ←

$99m \equiv 1 \pmod{17}$

$m = 11$

$x = 99 \cdot 11 = 990 + 99 = 1089$

$x_2 \equiv 0 \pmod{17}$

$1 \pmod{11}$

$0 \pmod{9}$

$x_2 = 17 \cdot 9 \cdot m = 153m$

$153m \equiv 1 \pmod{11}$

$x_3 \equiv 0 \pmod{17}$

$0 \pmod{11}$

$1 \pmod{9}$ ←

$x_3 = 187m$

$187m \equiv 1 \pmod{9}$

$m = 4$

$$x = 5(1089) + 3(1530) + 2(748) \pmod{1683}$$

recap

Fermat's little Theorem for prime p and $\gcd(a,p)=1$, $a^{p-1} \equiv 1 \pmod p$

Proof: $a \neq 0$.

$S = \{1, 2 \dots p-1\}$ nonzero ints mod p.

$S' = \{1a, 2a \dots (p-1)a\}$ when $\gcd(a,p)=1$, $f(x) = ax \pmod m$ is a bijection.

$f : S \to S'$ is bijection

Take both sets mod p. all elements are $\in \{1 \dots p-1\}$ and $p-1$ elements, so every $i \in \{1 \dots p-1\}$ must be in S'.

$S = S'$

$\prod_{s \in S} s = (p-1)!$ $\prod_{s \in S'} = a^{p-1}(p-1)!$

$(p-1)! = a^{p-1}(p-1)!$

Consider both sizes mod p.

ALL $i \in \{1 \dots p-1\}$ are coprime to so $(p-1)!$ has inverse mod p.

$1 \cdot (p-1)! \equiv a^{p-1}(p-1)! \pmod p$

$a^{p-1} \equiv 1 \pmod p$