Greatest Common Divisor

Def: $\gcd(a,b)$ is the largest positive int. that divides both.

Examples:

1) $\gcd(15,12) = 3$
2) $\gcd(2^3 \cdot 3^7 \cdot 5 \cdot 11,\ 2^2 \cdot 3^{13} \cdot 5 \cdot 13) = 2^2 \cdot 3^7 \cdot 5$
3) $\gcd(n,0) = |n|$

Euclid's Alg: (or Euclidean Algorithm)

Exercise: Prove that for $a,b \in \mathbb{N}$ and $a > b$,

$$\gcd(a,b) = \gcd(a-b,b)$$

Pf: $\gcd(a,b) = d$ $\quad \gcd(a-b,b) = d'$

$d \mid a$ and $d \mid b$ by definition.

so $d \mid a-b$ so $d \leq d'$ by defn of d'.

In the other dir. then $d' \mid a-b$, $d \mid b$,

so $d' \mid (a-b)+b$ (i.e. $d' \mid a$) so $d' \leq d$

so $d = d'$.

This is a solid alg. since it reduces the size of the number involved (as a consequence this alg. always terminates)

Example: $\gcd(35,50) = \gcd(50,35)$

$50 = 1 \cdot 35 + 15$

$35 = 2 \cdot 15 + 5$

$15 = 3 \cdot 5 + 0$

Ex $\gcd(120, 46)$

$120 = 2 \cdot 46 + 28$

$46 = 1 \cdot 28 + 18$

$28 = 1 \cdot 18 + 10$

$18 = 1 \cdot 10 + 8$

$10 = 1 \cdot 8 + 2$

$8 = 4 \cdot 2 + 0$

Diophantine Equations

Are solutions to linear sys. int. coefficients and integer sol.

e.g. $ax + by = 1$ where $a, b \in \mathbb{Z}$.

Solving this eqn gives you a^{-1} mod b and b^{-1} mod a.

The goal, is to use the steps in Euclid's alg to reconstruct x and y.

$a = 50 \qquad b = 35$

recipe card

$$\boxed{\begin{matrix}(c,d)\\ n\end{matrix}} = \{ca + db = n\}$$

Easy Recipe Card: $\boxed{\begin{matrix}(1,0)\\ 50\end{matrix}}$ $\boxed{\begin{matrix}(0,1)\\ 35\end{matrix}}$

$$\boxed{\begin{matrix}(1,0)\\ 50\end{matrix}} = 1 \cdot \boxed{\begin{matrix}(0,1)\\ 35\end{matrix}} + \boxed{\begin{matrix}(1,-1)\\ 15\end{matrix}}$$

$$\boxed{\begin{matrix}(0,1)\\ 35\end{matrix}} = 2 \boxed{\begin{matrix}(1,-1)\\ 15\end{matrix}} + \boxed{\begin{matrix}(-2,3)\\ 5\end{matrix}}$$

$$\boxed{\begin{matrix}(1,-1)\\ 15\end{matrix}} = 3 \boxed{\begin{matrix}(-2,3)\\ 5\end{matrix}} + \boxed{\begin{matrix}(7,-10)\\ 0\end{matrix}}$$

$50 = 1 \cdot 35 + 15$

$35 = 2 \cdot 15 + 5$

$15 = 3 \cdot 5 + 0$

Solve $50 \cdot x + 35y = 15$

Ex $\qquad 46x + 13y = 1$

$$\boxed{\begin{matrix}(1,0)\\ 46\end{matrix}} = 3 \boxed{\begin{matrix}(0,1)\\ 13\end{matrix}} + \boxed{\begin{matrix}(1,-3)\\ 7\end{matrix}}$$

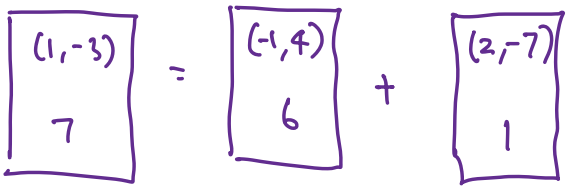
$$\boxed{\begin{matrix}(0,1)\\ 13\end{matrix}} = \boxed{\begin{matrix}(1,-3)\\ 7\end{matrix}} + \boxed{\begin{matrix}(-1,4)\\ 6\end{matrix}}$$

$46 = 3 \cdot 13 + 7$

$13 = 1 \cdot 7 + 6$

$7 = 1 \cdot 6 + 1$

$6 = 6 \cdot 1 + 0$



$x \equiv 2 \mod 6$

What is: $x \mod 2 \longrightarrow x \equiv 0 \mod 2$

$x \mod 3 \longrightarrow x \equiv 2 \mod 3$

$x \mod 5$

if $x = 2$ $\quad x \equiv 2 \mod 5$

$x = 8$ $\quad x = 3 \mod 5$

$x = 14$ $\quad x = 4 \mod 5$

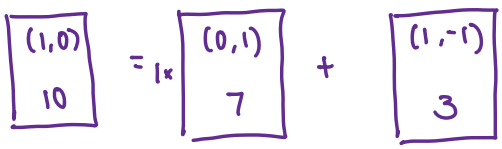
$x = 20$ $\quad x = 0 \mod 5$

$x = 26$ $\quad x = 1 \mod 5$

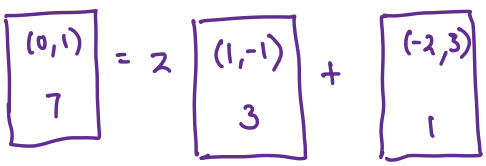
Warm-up: Find mult. inv. of 7 mod 10.

Sol: $7x + 10y = 1$ is an equiv. problem.

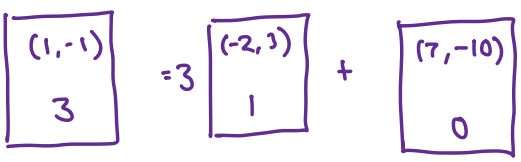
Next step: Find gcd of 7 and 10.



$10 = 1 \cdot 7 + 3$



$7 = 2 \cdot 3 + 1$



$3 = 3 \times 1 + 0$

⇓

$-2 \cdot 10 + 3 \cdot 7 = 1$

⇓

so mult. inv of 7 is 3.

$$x = \begin{cases} a \pmod 3 \\ b \pmod 5 \end{cases}$$

Chinese Remainder Theorem (Sun Zi)

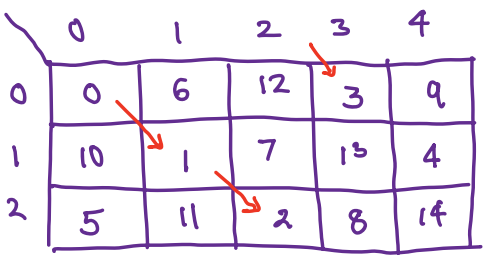
Suppose $\gcd(m,n) = 1$ and $a, b \in \mathbb{Z}$

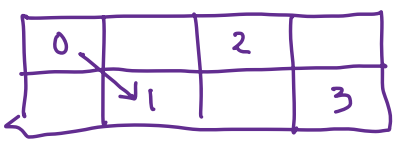
then

$$x \equiv a \pmod m$$

$$x \equiv b \pmod n$$

has exactly one solution mod mn.





"Real" proof: Let $\gcd(m,n) = 1$

$$\mathbb{Z}/_{mn\mathbb{Z}} \longrightarrow \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$

We want a bijective map.

$$\left| \mathbb{Z}/_{mn\mathbb{Z}} \right| = mn$$

$$\left| \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}} \right| = mn$$

Pf: Consider $c \in \mathbb{Z}/mn\mathbb{Z} \longrightarrow (c \bmod m, c \bmod n)$

For finite sets, you only have to check injectivity.

Contradiction: Assume not injective

$$x_1 \not\equiv x_2 \pmod{mn}$$

but

$$x_1 \equiv x_2 \pmod{m}$$
$$x_1 \equiv x_2 \pmod{n}$$

This $m \mid x_1 - x_2$

$n \mid x_1 - x_2$

This implies since $\gcd(m,n) = 1$,

$mn \mid x_1 - x_2$ which is contrary to the assumption that

$$x_1 \not\equiv x_2 \pmod{mn}.$$

Now consider a system

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

We can use Euclid's alg to find $s, t \in \mathbb{Z}$,

$$ns + mt = 1$$

Observe that $ns \equiv 1 \pmod{m}$ and $mt \equiv 1 \pmod{n}$

Take $x = ans + bmt$

and observe that

$$x \equiv ans \equiv a(1) \equiv a \pmod{m}$$
$$x \equiv bmt \equiv b \pmod{n}$$

Example (re-written ☺):

Solve $x \equiv 5 \pmod{11}$

$x \equiv 2 \pmod{7}$

Sol: By Euclid's,

$11s + 7t = 1$

for $s = 2,\ t = -3$

Let $x = ans + bmt$

$= 2 \cdot 11 \cdot s + 5 \cdot 7 \cdot t$

$= 2 \cdot 11 \cdot 2 + 5 \cdot 7 \cdot (-3)$

$= -61$

$\equiv 16 \pmod{77}$