Example:

	300	18	12	6	0
x	1	0	1	-1	3
y	0	1	-16	17	-50

$$\gcd(300, 18) = 6 = 300(-1) + 18(17)$$

Remember: Not unique!

Idea: $ar + bs = a(r+b) + b(s-a)$

That's why we can always find

$$\gcd(a,b) = ar - bs \quad \text{where } r, s \geq 0$$

Example: $300(-1) + 18(17) = 300(-1+18) + 18(17-300)$

$= 300(17) - 18(283)$

Definition:

a and b are coprime $\iff \gcd(a,b) = 1$

Conclude:

a and b are coprime $\iff \exists\, r, s \in \mathbb{Z},\ ar - bs = 1$

$\Longrightarrow$: from Euclidean Alg.

$\Longleftarrow$: $\left.\begin{array}{l} ar - bs = 1 \\ d \mid a \wedge d \mid b \end{array}\right| \Longrightarrow \underbrace{md}_{a}\, r - \underbrace{nd}_{b}\, s = 1$

$$\Rightarrow d\,(mr - ns) = 1. \Rightarrow d = 1.$$

$$\Rightarrow \gcd(a, b) = 1.$$

Important feature of coprimes: **Inverse**

$$ar - bs = 1$$
$$ar = bs + 1$$

" The remainder of the division ar/b is 1 "

$$ar \equiv 1 \pmod{b}$$

like saying: " if we multiply a by r, we get 1 "

$\equiv$: congruence.

r acts like the inverse of a, call it a^{-1}.

<u>Definition</u> : $a \equiv b \pmod{n} \iff$ • $n \mid a-b$

• a & b have same remainder in division by n

$\equiv$ "behaves" like equality, it's an $\underbrace{\text{"equivalence relation"}}_{\text{later.}}$

$$\frac{\begin{array}{c} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array}}{a+c \equiv b+d \pmod{n}}$$

(same with subtraction)

$$\frac{\begin{array}{c} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{array}}{a \times c \equiv b \times d \pmod{n}}$$

(move from side to side)

$$\frac{\begin{array}{c} a \equiv b \pmod{n} \\ b \equiv b \pmod{n} \end{array}}{a-b \equiv 0 \pmod{n}}$$

What about division?

$$\begin{array}{l} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \\ \hline \frac{a}{c} \equiv \frac{b}{d} \pmod{n} \end{array}$$

? Well, is $\frac{a}{c}$ even an integer?

Example: $n = 7$

$\frac{2}{3} \equiv x \pmod{7}$ $\qquad$ $2 \equiv 3x \pmod{7}$

?

$x = 3$

$\frac{3}{2} \equiv x \pmod{7}$

$x = 5$

$$\frac{2}{3} \times \frac{3}{2} \equiv 3 \times 5 \equiv 15 \equiv 1 \pmod{7}$$

$\gcd(a, n) = 1 \iff a$ has an inverse $a^{-1} \bmod n$.

$$ar - ns = 1$$
$$ar = ns + 1$$
$$ar \equiv 1 \pmod{n}$$

r acts like the inverse of a

simply find r modulo n (bring it to $< n$)

inverse is UNIQUE ! why? (see below)

Interesting fact: $\gcd(a,n) = 1 \implies$

$$\left.\begin{array}{l} ax \equiv ay \pmod{n} \\ x < n \\ y < n \end{array}\right\} \implies x = y$$

(mult. both sides by a^{-1})

$$\underbrace{a^{-1} \cdot a}x \equiv \underbrace{a^{-1} \cdot a}y \pmod{n}$$
$$1 \cdot x \equiv 1 \cdot y \pmod{n}$$
$$x \equiv y \pmod{n} \implies x = y \text{ (because } x < n,\ y < n)$$

Example: $n=7$

$a=3$

$$\begin{array}{r|ccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \times 3 & 0 & 3 & 6 & 2 & 5 & 1 & 4 \end{array}$$

$$\underbrace{0 \quad 3 \quad 6 \quad 2 \quad 5 \quad 1 \quad 4}$$

they are all different

(a permutation)

Application: Solving with modular arithmetics.

$13x \equiv 2 \pmod{21}$ Find x.

$\underbrace{13^{-1} \cdot 13}\, x \equiv 13^{-1} \cdot 2 \pmod{21}$

$1 \cdot x \equiv 13^{-1} \cdot 2 \pmod{21}$

$x \equiv 13^{-1} \cdot 2 \pmod{21}$ Find inverse of 13 mod 21.

Inverse of 13 means: $13 \cdot r \equiv 1 \pmod{21}$

$13 \cdot r = 21 \cdot s + 1$

$13 \cdot r - 21 s = 1$ (do Euclidean alg.)

a	21	13	8	5	3	2	1	0
x	1	0	1	−1	2	−3	5	
y	0	1	−1	2	3	5	−8	

$21(5) + 13(\underset{r}{-8}) = 1$

$-8 \equiv 13 \pmod{21}$

$$x \equiv 13.2 \equiv 26 \equiv 5 \pmod{21}$$

Try: $13 \times 5 = 65$

$$65 = 21 \times 3 + \underbrace{1}_{\text{Remainder}}$$

Primes

A prime number p is a positive integer that has exactly 2 divisors, 1 and p.

Facts about primes:

- Every $n \in \mathbb{N}$ is the product of primes.
- Prime factorization is UNIQUE. (proof: read chap. 7).
  [Fundamental Theorem of arithmetics]
- $p \mid ab \Rightarrow p \mid a \vee p \mid b$

Proof: $p \mid ab \Rightarrow ab = mp$

If we factor a and b into primes, p must show up by uniqueness of prime factorization.

$\Rightarrow p \mid a \vee p \mid b$

- $p \mid b \wedge p \nmid a \Longrightarrow p \mid \frac{b}{a} \quad \left(\frac{b}{a} = k \in \mathbb{N}\right)$

$$\frac{b}{a} = k \Rightarrow p \mid ak \Rightarrow \underbrace{p \mid a}_{\text{false}} \vee p \mid k \Rightarrow p \mid k.$$

- some other properties can be found in chp. 7.