Definition:

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

Conclude:

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

$\Longrightarrow$: 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: <u>Inverse</u>

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

" 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?

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

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

Example: $n=7$

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

? $x=3$

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

? $x=5$

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

So why does it work?

$$x \equiv \frac{2}{3} \pmod 7 \Rightarrow x \equiv 2.\underbrace{3^{-1}}_{\text{inverse of 3 mod 7}} \pmod 7$$

So x is well defined $\in \mathbb{N}$ if 3^{-1} exists mod 7.

$3.5 \equiv 1 \pmod 7$, so $3^{-1} = 5$.

$$x \equiv 2.5 \pmod 7$$

$$x \equiv 3 \pmod 7$$

So $\frac{2}{3}$ "is" $3 \pmod 7$.

$\gcd(a, n) = 1 \iff a$ has an inverse a^{-1} mod 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: $\gcd(a, n) = 1 \implies ax \equiv ay \pmod{n}$

$x < n$

$y < n$

$\implies x = y$

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

$$\underbrace{a^{-1} \cdot a}x \equiv \underbrace{a^{-1} \cdot a}y \pmod{n}$$
$$1 \cdot x \equiv 1 \cdot y \pmod{n}$$
$$x \equiv y \pmod{n}$$

$\implies x = y$ (because $x < n$, $y < n$)

So, if $\underbrace{ax}_{\text{inverse}} \equiv \underbrace{ay}_{\text{inverse}} \equiv 1 \pmod{n}$

and $\gcd(a, n) = 1$ (so a^{-1} exists)

then $x = y$ $(x < n,\ y < n)$

Inverse is unique.

Example: $n=7$

$a=3$

$$\begin{array}{c} 0\quad 1\quad 2\quad 3\quad 4\quad 5\quad 6 \\ \hline \Big\downarrow \times 3 \\ \underbrace{0\quad 3\quad 6\quad 2\quad 5\quad 1\quad 4} \end{array} \qquad \begin{array}{c} x \neq y \\ \Downarrow \\ 3x \neq 3y \end{array}$$

they are all different
(a permutation)

This is not generally true; for instance,

$$2 \cdot 3 \equiv 6 \pmod 8$$
$$2 \cdot 7 \equiv 6 \pmod 8$$

so $\quad 2 \cdot 3 \equiv 2 \cdot 7 \quad$ but $\quad 3 \neq 7$

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: $13 \times 5 = 65$

$$65 = 21 \times 3 + \underbrace{2}_{\text{Remainder}} \quad \checkmark$$