- $\gcd(30,24) = 6$

  $\gcd(7,5) = 1$

  $\gcd(9,0) = 9$

  $\gcd(0,0) \stackrel{\Delta}{=} 0$

- d is a divisor of m : $d \mid m$

  $$\left.\begin{array}{l} d \mid m \\ d \mid n \end{array}\right| \Rightarrow \begin{array}{l} d \mid (m+n) \\ d \mid (m-n) \end{array}$$

- in general

  $$\left.\begin{array}{l} d \mid m \\ d \mid n \end{array}\right| \Rightarrow d \mid (mx+ny)$$

  $$\forall x, y \in \mathbb{N}$$

- GCD recursion

$$\gcd(m,n) = \gcd(n, m \bmod n)$$

Def $m \bmod n = m - \left\lfloor \frac{m}{n} \right\rfloor n$

Plan

1. $\gcd(m,n) \mid \gcd(n, m \bmod n)$
2. $\gcd(n, m \bmod n) \mid \gcd(m,n)$

(1) Show that $\gcd(m,n) \mid \gcd(n, m \bmod n)$

$d = \gcd(m,n) \Rightarrow d \mid m$

$d \mid n$

but $(m \bmod n)$ – is a linear combination of m & n

$$\left.\begin{array}{l} d \mid (m \bmod n) \\ d \mid n \end{array}\right\} \Rightarrow d \mid \gcd(n, m \bmod n)$$

$$\Rightarrow \gcd(m, n) \mid \gcd(n, m \bmod n)$$

(2) show that $\gcd(n, m \bmod n) \mid \gcd(m, n)$

$$d \mid \gcd(n, m \bmod n) \Rightarrow \begin{array}{l} d \mid n \\ d \mid (m \bmod n) \end{array}$$

$$m = \left\lfloor \frac{m}{n} \right\rfloor n + (m \bmod n)$$

is a linear comb. of n & $(m \bmod n)$

$$\left.\begin{array}{l} d \mid m \\ d \mid n \end{array}\right\} \Rightarrow d \mid \gcd(m, n)$$

$$\Rightarrow \gcd(n, m \bmod n) \mid \gcd(m, n)$$

1 , 2 $\Rightarrow \gcd(m, n) = \gcd(n, m \bmod n)$

Recursive version of Euclid's alg

```
ALGORITHM Euclid(m, n)
if n = 0
    then return m
    else return Euclid(n, m mod n)
```