Computing GCD of two numbers:

Euclid algorithm:-

Thm: Let a, b are two numbers such that $b > 0$. Then.

$$\gcd(a,b) = \gcd(b, a \bmod b).$$

$b = dK$

$$d = \gcd(a,b) \Rightarrow d \mid a,\ d \mid b$$

$c \mid b,\ c \mid r$

$$a \bmod b = r \Rightarrow r = a - bq$$

$$a - r = bq.$$

$\Rightarrow c \mid b,\ c \mid a - bq$

$d \mid bq$

$\Rightarrow c \mid a \Rightarrow c \mid d.$

$\Rightarrow d \mid a - r,\ d \mid a \Rightarrow d \mid r$

$$\gcd(18, 12)$$

$$= \gcd(12, 6) \quad b_{i+2}$$

$$= \gcd(6, 0) = 6.$$

h

EUCLID Algorithm:-

Input: $a, b \in \mathbb{Z}$ s.t $b > 0$.

$\text{GCD}(a, b)$

- if $b = 0$ return a
- else return $\text{GCD}(b, a \bmod b)$.

Lemma: Consider an execution of GCD(a_0, b_0), where it holds that $a_0 \geq b_0 > 0$; and let a_i, b_i for $i = 1, \ldots, k$. denote the arguments to the ith recursive call of GCD. Then,

$$b_{i+2} \leq b_i/2 \quad \text{for } 0 \leq i \leq k-2.$$

$$b_2 \leq b_0/2$$

$$b_4 \leq b_2/2 \leq b_0/2^2$$

Pf: For $a > b$. $a \bmod b < a/2$.

- Case 1: if $b \leq a/2$ then $a \bmod b < b < a/2$.
- Case 2: if $b > a/2$ then $a \bmod b = a - b < a/2$

$$b_{i+2} = a_{i+1} \bmod b_{i+1} < a_{i+1}/2 = b_i/2$$