Recall:

- $d = GCD(a,b) = (a,b)$
  iff
  (i) $d|a \wedge d|b$
  (ii) $e|a \wedge e|d \rightarrow e \leq d$

- $m = LCM(a,b) = [a,b]$
  iff
  (i) $a|m \wedge b|m$
  (ii) $a|k \wedge b|k \longrightarrow m \leq k$

Theorem:

$$a \cdot b = (a,b) \cdot [a,b]$$

Theorem

for any $m, n, d \in \mathbb{Z}^+$

$$m \mid nd \longrightarrow \frac{m}{(m,d)} \mid n$$

Proof

Assume $m \mid nd$. Then

$nd = km$ for some $k \in \mathbb{Z}$

$\therefore$ km is a common mult. of m, d

$\therefore$ $[m,d] \mid km$

$\therefore$ $km = k' \cdot [m,d]$ for some $k' \in \mathbb{Z}$.

$\therefore$ $k' = k \cdot \frac{m}{[m,d]} = k \cdot \frac{(m,d)}{d}$ (by Prev. Thm)

$\therefore$ $k'd = k(m,d)$

$\therefore$ $k'md = km(m,d)$

$$\therefore \quad k'md = nd(m,d)$$

$$\therefore \quad k'm = n(m,d)$$

$$\therefore \quad n = k' \cdot \frac{m}{(m,d)}$$

$$\therefore \quad \frac{m}{(m,d)} \mid n$$ ∎

Corollary

Let $a, b, d \in \mathbb{Z}$, $m \in \mathbb{Z}^+$. Then

$$ad \equiv bd \pmod{m} \rightarrow a \equiv b \pmod{\frac{m}{(m,d)}}$$

Proof

Assume $ad \equiv bd \pmod{m}$. Then

$$m \mid ad - bd$$

$$\therefore \quad m \mid (a-b)d$$

$\therefore \frac{m}{(m,d)} \mid (a-b)$ { P-ev. thm with $n = a-b$

$\therefore a \equiv b \pmod{\frac{m}{(m,d)}}$

Corollary

If $(m,d) = 1$, then

$ad \equiv bd \pmod{m} \rightarrow a \equiv b \pmod{m}$

Proof

follows from Prev. Cor. since

$(m,d) = 1$. ▨

Ex.

Find the remainder of 7^{2023} upon division by 5.

Note: $a \equiv b \pmod m \rightarrow a^2 \equiv b^2 \pmod m$

$\rightarrow a^3 \equiv b^3 \pmod m$

$\vdots$

$\rightarrow a^n \equiv b^n \pmod m$

So $7 \equiv 2 \pmod 5 \rightarrow 7^{2023} \equiv 2^{2023} \pmod 5$

2^{2023} still to big!

$$7^{2023} = 7^{2022+1} = 7^{2 \cdot 1011 + 1}$$

$$= (7^2)^{1011} \cdot 7 = (49)^{1011} \cdot 7$$

Also $49 \equiv 4 \pmod 5$

$4 \equiv -1 \pmod 5$

$\Big\} \; 49 \equiv -1 \pmod 5$

$$\therefore 7^{2023} \equiv 49^{1011} \cdot 7 \pmod 5$$

$$\equiv (-1)^{1011} \cdot 2 \pmod 5$$

$$\equiv (-1) \cdot 2 \pmod 5$$

$$\equiv -2 \pmod 5$$

$$\equiv 3 \pmod 5$$

7^{2023} mod 5 = $\boxed{3}$.

Euclidean Algorithm

Ex. $GCD(198, 84) = 6$

$$198 = 84 \cdot 2 + 30$$
$$84 = 30 \cdot 2 + 24$$
$$30 = 24 \cdot 1 + \boxed{6} \leftarrow \text{gcd}$$
$$24 = 6 \cdot 4 + 0 \leftarrow \text{stop}$$

Pseudo-code

GCD(a, b)

1. $r = a \bmod b$
2. while $r > 0$
3. $\quad a = b$
4. $\quad b = r$
5. $\quad r = a \bmod b$
6. end-while
7. return b

Ex. $GCD(756, 16200) = 108$

$$756 = 16200 \cdot 0 + 756$$

$$16200 = 756 \cdot 21 + 324$$

$$756 = 324 \cdot 2 + \boxed{108} \leftarrow \text{gcd}$$

$$324 = 108 \cdot 3 + 0 \leftarrow \text{stop}$$

Theorem

Euclid's algorithm correctly finds the gcd.

Lemma

If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then $GCD(a, b) = GCD(b, r)$.

Proof

Let $d \in \mathbb{Z}$. Then

$$d|a \wedge d|b \rightarrow d|b \wedge d|(a-bq)=r$$

and

$$d|b \wedge d|r \rightarrow d|(bq+r)=a \wedge d|b .$$

Thus

$$d|a \wedge d|b \leftrightarrow d|b \wedge d|r$$

$$\therefore \{\text{com. div. of } a, b\} = \{\text{com. div. of } b, r\}$$

$$\therefore \quad GCD(a,b) = GCD(b,r) .$$

∎

Proof of theorem

Let $a, b \in \mathbb{Z}$. set $r_0 = a$, $r_1 = b$.

$$r_0 = r_1 q_1 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 \cdot q_2 + r_3 \qquad 0 \le r_3 < r_2$$

$$r_2 = r_3 \cdot q_3 + r_4 \qquad 0 \le r_4 < r_3$$

$$\vdots$$

$$r_{n-2} = r_{n-1} \cdot q_{n-1} + \boxed{r_n} \qquad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = \boxed{r_n} \cdot q_n + 0$$

since $r_1 > r_2 > r_3 > \cdots \ge 0$, some remainder must be 0, say $r_{n+1} = 0$

Then

$$GCD(a,b) = GCD(r_1, r_2) = \cdots\cdots$$

$$= GCD(r_n, 0) = r_n .$$

∎

5.1 Mathematical Induction

Ex.

$$1 = 1^2$$

$$1+3 = 2^2$$

$$1+3+5 = 3^2$$

$$1+3+5+7 = 4^2$$

$$\vdots$$

$$1+3+5+\cdots+(2n-1) = n^2$$

i.e.

$$\sum_{k=1}^{n} (2k-1) = n^2$$

We wish to prove:

$$\forall n \geq 1 : \sum_{k=1}^{n} (2k-1) = n^2$$

Let $P(n)$ be a pred. fcn. with domain $\mathbb{Z}^+$, i.e.

$$P : \mathbb{Z}^+ \longrightarrow \{\text{false}, \text{true}\}$$

suppose we wish to prove

$$* \qquad \forall n \; P(n)$$

i.e. $P(n)$ is true for all $n \in \mathbb{Z}^+$.