CSE 16 7-23-24

Lemma

Let $a, b \in \mathbb{Z}^+$ and let $p_1, p_2, \ldots, p_n$ be all primes that divide either a or b. Thus

$$a = p_1^{x_1} \cdot p_2^{x_2} \cdots p_n^{x_n}$$

and

$$b = p_1^{y_1} \cdot p_2^{y_2} \cdots p_n^{y_n}$$

for some $x_i, y_i \geq 0$ $(1 \leq i \leq n)$. Then

(1) $GCD(a,b) = p_1^{\min(x_1,y_1)} \cdot p_2^{\min(x_2,y_2)} \cdots p_n^{\min(x_n,y_n)}$

and

(2) $LCM(a,b) = p_1^{\max(x_1,y_1)} \cdot p_2^{\max(x_2,y_2)} \cdots p_n^{\max(x_n,y_n)}$

Previous example : $a=30$, $b=75$

$$30 = 2\cdot 3\cdot 5 = 2^1\cdot 3^1\cdot 5^1$$
$$75 = 3\cdot 5\cdot 5 = 2^0\cdot 3^1\cdot 5^2$$

$\therefore$

$GCD(30,75) = 2^0\cdot 3^1\cdot 5^1 = 15$ ✓

$LCM(30,75) = 2^1\cdot 3^1\cdot 5^2 = 150$ ✓

Corollary

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

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

Ex.

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

Note

$$a \equiv_n b \rightarrow a^2 \equiv_m b^2 \rightarrow a^3 \equiv_m b^3 \rightarrow \cdots \rightarrow a^n \equiv_m b^n$$

Solution

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

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

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

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

$$\equiv -2 \pmod 5$$

$$\equiv 3 \pmod 5$$

$$\therefore\ 7^{2023} \bmod 5 = \boxed{3}$$

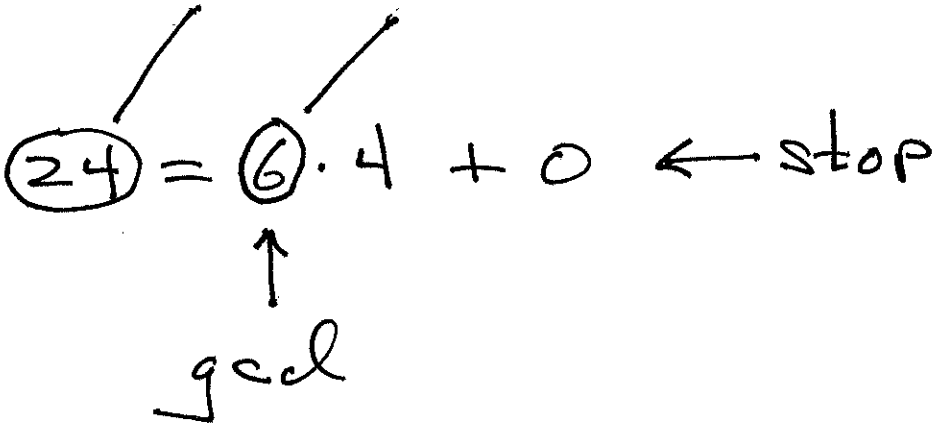
Euclidean Algorithm

Ex. $\gcd(198, 84) = 6$

$198 = 84 \cdot 2 + 30$

$84 = 30 \cdot 2 + 24$

$30 = 24 \cdot 1 + 6 \leftarrow \gcd$



Pseudo code:

GCD(a, b)

1. r = a mod b
2. while r > 0
3. a = b
4. b = r
5. r = a mod b
6. end-while
7. return b

If a, b are initially out of order ($a < b$), the 1st iteration puts them in order.

Ex $\gcd(756, 16200) = 108$

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

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

$$756 = 324 \cdot 2 + 108 \leftarrow \gcd$$

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

$\uparrow$

gcd

Theorem

Euclid's algorithm correctly finds the gcd of 2 numbers.

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 $\forall d \in \mathbb{Z}^+$:

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

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

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

■

Proof of Theorem

let $a, b \in \mathbb{Z}^+$. set

$$r_0 = a$$
$$r_1 = b$$

Then

$$r_0 = r_1 \cdot q_1 + r_2, \quad 0 \le r_2 < r_1$$

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

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

$$\vdots$$

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

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

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

$$GCD(a,b) = GCD(r_0, r_1) = GCD(r_1, r_2)$$
$$= \cdots = GCD(r_n, 0) = r_n .$$

Ex. $GCD(1001, 513) = 1$

$$1001 = 513 \cdot 1 + 488$$

$$513 = 488 \cdot 1 + 25$$

$$488 = 25 \cdot 19 + 13$$

$$25 = 13 \cdot 1 + 12$$

$$13 = 12 \cdot 1 + \boxed{1}$$

$$12 = 1 \cdot 12 + 0$$

5.1 Mathematical Induction

Ex.

$$1 = 1^2$$

$$1+3 = 2^2$$

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

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

$$\vdots$$

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

or

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

evidently:

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

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

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

Suppose we wish to prove

(*) $$\forall n : P(n)$$

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

A Proof by induction has 2 steps.

I. base

Prove that $P(1)$ is true.

II. Induction

Prove $\forall n \left(P(n) \rightarrow P(n+1)\right)$

Let $n \geq 1$, assume $P(n)$ is true, show as a consequence that $P(n+1)$ is true.

when I & II are complete we conclude * is true.

Remarks

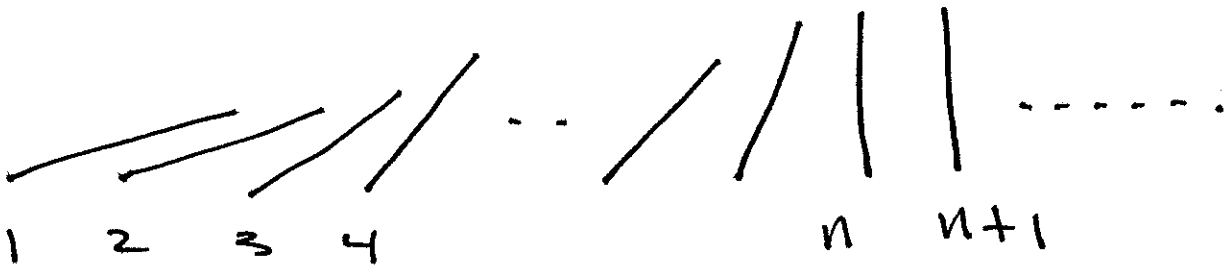
- $P(n)$ is called the induction hypothesis since it is assumed on induction step.

- Induction is not circular reasoning. We do not assume $\forall n\, P(n)$. We only assume $P(n)$ for one particular n.

- We can think of induction as an 'infinite' proof.

1. $P(1)$	by I
2. $P(1) \to P(2)$	by II with $n=1$
3. $\therefore P(2)$	by (1) and (2)
4. $P(2) \to P(3)$	by II, $n=2$
5. $\therefore P(3)$	by (3) and (4)
⋮	⋮

• Domino Analogy



$P(n)$ = 'the n^{th} domino falls'

$\forall n\, P(n)$ = 'all dominos fall'

I. Prove $P(1)$ = '1^{st} domino falls'

II. Prove $\forall n\,(P(n) \to P(n+1))$

= 'if any domino falls, the next one also falls'.

The validity of induction follows from

Theorem (Principle of Mathematical Induction, PMI)

For any Propositional function

$$P : \mathbb{Z}^+ \to \{F, T\}$$

the following sentence is true

$$[P(1) \wedge \forall n (P(n) \to P(n+1))] \to \forall n P(n)$$

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

$\rightarrow P(n)$

Proof.

1. $P(1)$ is the statement

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

i.e. $1 = 1^2$

which is true.

II. show $\forall n \geq 1 : P(n) \rightarrow P(n+1)$

Let $n \geq 1$ be chosen arbitrarily.

Assume $\sum_{k=1}^{n} (2k-1) = n^2$ is true.

(induction hypothesis)

We must show that

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

So

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

$$= n^2 + 2(n+1) - 1 \quad \{ \text{by the ind. hyp.}$$

$$= n^2 + 2n + 1$$

$$= (n+1)^2 .$$

By the P.M.I., result follows for all $n \geq 1$. ∎