CSE 16 5-7-24

Theorem

Euclid's algorithm correctly finds the GCD of a, b.

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

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

and

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

Thus

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

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

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

Proof of theorem

Let $a,b \in \mathbb{Z}^+$. Set $r_0 = a, r_1 = b$. By division algorithm

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

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

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

$$\vdots \qquad\qquad \vdots$$

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

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

Since $r_1 > r_2 > r_3 > \cdots\cdots \ge 0$, some remainder must be zero, call it $r_{n+1} = 0$. Then

$$\begin{aligned} GCD(a,b) &= GCD(r_0, r_1) \\ &= GCD(r_1, r_2) \\ &\vdots \\ &= GCD(r_n, 0) = r_n \end{aligned}$$

Ex $\gcd(1001, 513) = 1$

$1001 = 513 \cdot 1 + 488$

$513 = 488 \cdot 1 + 25$

$488 = 25 \cdot 19 + 13$

$25 = 13 \cdot 1 + 12$

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

$12 = 1 \cdot 12 + 0$

Theorem

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:

$$a \equiv_m b \to a^2 \equiv_m b^2 \to a^3 \equiv_m b^3 \to \cdots \to a^n \equiv_m b^n$$

so

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

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

$$\therefore 7^{2023} \equiv_5 (49)^{1011} \cdot 7$$

$$\equiv_5 (-1)^{1011} \cdot 2$$

$$\equiv_5 -2$$

$$\equiv_5 \boxed{3}$$

← remainder.

5.1 Mathematical Induction

Ex $1 = 1^2$

$1+3 = 2^2$

$1+3+5 = 9 = 3^2$

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

$\vdots$

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

i.e.

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

Wish to Prove:

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

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

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

Suppose we wish to prove

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

A Proof by Mathematical Induction Proceeds:

I. base: Prove $P(1)$ is true

II. induction: Prove $\forall n : (P(n) \to P(n+1))$
Let $n \geq 1$, assume $P(n)$ is true,
show $P(n+1)$ as a consequence.

once I & II are complete, then * is Proved.

Rmks

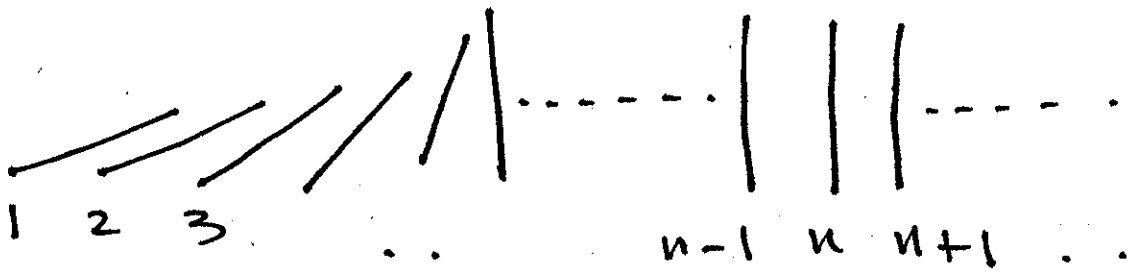
- $P(n)$ is called the induction hypothesis
- induction is not circular reasoning we do not assume $\forall n\ P(n)$, only $P(n)$ is true for one n.
- we can think of induction as an 'infinite' proof!

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

⋮

This 'Proof' is not valid since Proofs are supposed to be finite.

- Domino Analogy



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

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

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

'if any domino falls, the next domino also falls'

Conclusion: $\forall n\, P(n)$

'all dominos fall'

Principle of Mathematical Induction

Theorem (PMI)

For any Prop. fcn. $P: \mathbb{Z}^+ \to \{F, T\}$, the following is true

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

Proof later

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

Proof.

I. $P(1)$ is $1 = 1^2$ which is true.

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

Let $n \geq 1$. Assume $P(n)$

$$\sum_{k=1}^{n} (2k-1) = n^2 \quad \{ \text{induction hypothesis}$$

We must show $P(n+1)$

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

Then

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

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

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

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

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

Since $n \geq 1$ was arbitrary, we have $\forall n\,(P(n) \to P(n+1))$. By the PMI:

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

Ex. let $x \in \mathbb{R}$, $x \neq 1$. show

$$\forall n \geq 1 : \boxed{\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}} \leftarrow P(n)$$

Proof

I. $P(1)$ says : $x^0 = \frac{x^1 - 1}{x - 1}$, i.e. $1 = 1$,

which is true.

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

Let $n \geq 1$. Assume

$$\sum_{k=0}^{n-1} x^k = \frac{x^n - 1}{x - 1}$$

We must show

$$\sum_{k=0}^{n} x^k = \frac{x^{n+1} - 1}{x - 1}.$$

so

$$\sum_{k=0}^{n} x^k = \left(\sum_{k=0}^{n-1} x^k \right) + x^n$$

$$= \left(\frac{x^n - 1}{x - 1} \right) + x^n \quad \left\{ \text{by the ind. hyp.} \right.$$

$$= \frac{x^n - 1}{x - 1} + \frac{x^n (x - 1)}{x - 1}$$

$$= \frac{x^n - 1 + x^{n+1} - x^n}{x - 1}$$

$$= \frac{x^{n+1} - 1}{x - 1}.$$

Ex. $\forall n \geq 1 : \boxed{\sum_{k=1}^{n} k = \frac{n(n+1)}{2}} \leftarrow P(n)$

Proof

I. $P(1)$ says: $1 = \frac{1(1+1)}{2}$, i.e. $1 = 1$

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

Let $n \geq 1$. Assume

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

We must show

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

Then

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

$$= \left(\frac{n(n+1)}{2}\right) + (n+1) \quad \left\{ \text{by the ind. hyp.} \right.$$

$$= \frac{n(n+1) + 2(n+1)}{2}$$

$$= \frac{(n+1)(n+2)}{2} \,. \qquad \blacksquare$$

Ex $\forall n \geq 1 : \boxed{\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}}$ ← P(n)

Proof

1. P(1) says $1^2 = \frac{1(1+1)(2\cdot 1+1)}{6}$, i.e.

$1^2 = \frac{1 \cdot 2 \cdot 3}{6}$, i.e. $1 = 1$ ✓

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

Let $n \geq 1$, assume

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

We must show

$$\sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

So

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

$$= \left(\frac{n(n+1)(2n+1)}{6} \right) + (n+1)^2$$

$$\vdots \quad \text{algebra}$$

$$= \frac{(n+1)(n+2)(2n+3)}{6}$$

Exercise: Show

$$\forall_{n \geq 1} : \sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2} \right)^2$$