Subject:
Year. Month. Date. ( )

Example.) Prove that for any $n \in \mathbb{Z}^+$, if $n \geq 14$ then n can be expressed as a sum of 3's and/or 8's.

$14 = 3 + 3 + 8$

$15 = 3 + 3 + 3 + 3 + 3$

$16 = 8 + 8$

$17 = 8 + 3 + 3 + 3$

⋮

$P(n)$: n can be expressed as a sum of 3's and 8's.

strong form of induction: $\left(P(a_0) \wedge \forall k \geq a_0 \left[P(a_0) \wedge P(a_0+1) \wedge \dots \wedge P(k) \rightarrow P(k+1) \right] \right) \Rightarrow \forall n \geq a_0 \, [P(n)]$

① $P(14)$ is true.

$(k+1) = (k-2) + 3$

⇓ Induction hypotheses

$k-2 \geq 14 \Rightarrow k \geq 16$

② ⟸ $(k-2)$ can be expressed as a sum of 3's and 8's.

$(k+1)$ can be expressed as a sum of 3's and 8's.

15، 16 [illegible] 17 [illegible] 15، 16 [illegible]

③ $P(15)$ is true

④ $P(16)$ is true

$P(14) \wedge P(15) \wedge \dots \wedge P(k) \rightarrow P(k+1) \qquad k \geq 14$

$P(14) \rightarrow P(15)$ ✗

$P(14) \wedge P(15) \rightarrow P(16)$ ✗ $\qquad P(14) \wedge P(15) \wedge P(16) \rightarrow P(17)$ ✓

نمی‌توانیم [illegible] درست نیست

$P(14) \wedge P(15) \wedge P(16) \wedge P(17) \rightarrow P(18)$

PAPCO

Subject:

Year. Month. Date. ( )

Elementary Number Theory

Definition:

If $a,b \in \mathbb{Z}$ and $b \neq 0$ we say that b divide a written $b|a$, when there is an integer n such that $a=bn$. In this case, b is a divisor of a and a is multiplier of b

$$b|a \iff \exists n \in \mathbb{Z}[a=bn]$$

Theorem (properties) → For any $a,b,c \in \mathbb{Z}$

1) $a|a$
2) $(a|b \wedge b|c) \Rightarrow a|c$
3) $1|a$
4) $a|0$
5) $0|a \Rightarrow a=0$
6) $(a|b \wedge a|c) \Rightarrow \forall x,y \in \mathbb{Z}\,[a|bx+ay]$
7) $(a|b \wedge b \neq 0) \Rightarrow |a| \leq |b|$ and
8) $a|b \Rightarrow ca|cb \wedge a|cb$

proof (7)

$a|b \Rightarrow \exists n \in \mathbb{Z}\,[b=an]$

$\Rightarrow \exists n \in \mathbb{Z}\,[|b|=|a||n|]$

$n \neq 0 \Rightarrow |b| \geq |a|$

Subject:

Year. Month. Date. ( )

Theorem For any integers $a, b \in \mathbb{Z}$, There is a common divisor that can be written as a linear combination of a and b

$$\forall a,b \in \mathbb{Z}\ \exists d \in \mathbb{Z}\ [d|a \wedge d|b \wedge \exists x,y \in \mathbb{Z}\ [d = ax + by]]$$

proof (Using mathematical Induction is $n = a+b$)

without loss of generality, we assume that $a, b > 0$

$P(n)$: In any partition of n, $n = a+b$, a and b have a common devisor that can be written in the form of linear combination of a and b $(n, a, b > 0)$

$$\forall n > 0\ [P(n)]$$

~~$P(n)$: $n = a+b \Rightarrow$~~

$a|a \wedge 0|0 \wedge a = ax + by$

$(P(1) \wedge P(1+1) \wedge \ldots \wedge P(k)) \rightarrow P(k+1)$

$k+1 = a+b$ Assume $a > b$ $(a = b \rightarrow a|a \wedge a|b \wedge a = ax1 + bx0)$

$k+1 - b = (a-b) + b$ $(b > 0 \Rightarrow k+1 - b < k$

Induction Hypothesis $\Downarrow$ $(a = b \rightarrow a|a \wedge a|a \wedge a = ax1 + bx1)$

$\exists d \in \mathbb{Z}\ [d|(a-b) \wedge d|b \wedge \exists x,y \in \mathbb{Z}\ [d = (a-b)x + by]] \rightarrow$

$\exists d \in \mathbb{Z}\ [d|a \wedge d|b \wedge \exists x,y \in \mathbb{Z}\ [d = ax + by]]$

Later

P4PCO

Subject:

Year. Month. Date. ( )

corollary - For any $a,b \in \mathbb{Z}$ there is a unique d so that

1) $d \geq 0$

2) $d|a \wedge d|b$ and

3) $\exists x,y \in \mathbb{Z}\,[d = ax + by]$

corollary - For any $a,b \in \mathbb{Z}$, there is unique d so that

1) $d \geq 0$

2) $d|a \wedge d|b$, and

3) $\forall e \in \mathbb{Z}\,[e|a \wedge e|b \Rightarrow e|d]$

Definition:

The unique d in the above corollary is called the greatest common devisor of a and b and is denoted by $gcd(a,b)$ or simply (a,b).

Theorem:

1) $(a,b) = (b,a)$

2) $(a,(b,c)) = ((a,b),c)$

3) $(a,1) = 1$

4) $(a,0) = |a|$

5) $(ca,cb) = |c|(a,b)$

Note: $(a,b) = d \Rightarrow \exists x,y \in \mathbb{Z}\,[d = ax + by]$

$(4,1) \neq 5 \not\Leftarrow 5 = 4\times 1 + 1\times 1$

Subject:

Year. Month. Date. ( )

proof of 5) 1) $|c|(a,b) \geq 0$

2) $(a,b)|a \wedge (a,b)|b$

$\Rightarrow |c|(a,b)|ca \wedge |c|(a,b)|cb$

3) $(e|ca \wedge e|cb) \Rightarrow e|\,|c|(a,b)$

$\exists x,y \in \mathbb{Z}\,[(a,b) = ax+by] \Rightarrow \exists x,y \in \mathbb{Z}[c(a,b) = cax+cby]$

$\Rightarrow \exists x,y \in \mathbb{Z}\,[c(a,b) = an+my]$ $\quad e(nx+my)$

$\Rightarrow e|c(a,b) \Rightarrow [e|\,|c|(a,b)]$

$(a,b) = d \Rightarrow \exists x,y \in \mathbb{Z}\,[ax+by = d]$

Definition Two integer a and b are called co-prime if $(a,b) = 1$

$(a,b) = 1 \Leftrightarrow \exists x,y \in \mathbb{Z}\,[ax+by = 1]$.

Example) prove that

1) $(a,b) = 1 \Rightarrow (a+b,b) = 1$

2) $(a,b) = 1 \Rightarrow (a^m, b^n) = 1$ for any $m,n \in \mathbb{Z}^+$

3) $(a,b) = d \Rightarrow (\frac{a}{d}, \frac{b}{d}) = 1$

4) $(a,b) = d \Leftrightarrow (a^n, b^n) = d^n$ for any $n \in \mathbb{Z}^+$

5) $(a,b) = 1 \Rightarrow (a+b, ab) = 1$

6) $(a,b) = 1 \Rightarrow (a^2-ab+b^2, a+b) \in \{1,3\}$

proof

1) $(a,b) = 1 \Rightarrow \exists x,y \in \mathbb{Z}\,[ax+by = 1]$

$\Rightarrow \exists x,y \in \mathbb{Z}\,[(a+b)x + b(y-x) = 1] \Rightarrow (a+b,b) = 1$

Subject:

Year. Month. Date. ( )

2) $(a,b)=1 \Rightarrow \exists x,y \in \mathbb{Z}[ax+by=1]$.

$\Rightarrow \exists x,y \in \mathbb{Z}[(ax+by)^m = 1]$

$\Rightarrow \exists x,Q \in \mathbb{Z}[a^m x^m + bQ = 1] \Rightarrow (a^m, b) = 1 \Rightarrow (a^m, b^n) = 1$

3) $(a,b)=d \Rightarrow \exists x,y \in \mathbb{Z}[ax+by=d]$

$d|a \wedge d|b$

$\Rightarrow \exists x,y \in \mathbb{Z}[\frac{a}{d}x + \frac{b}{d}y = 1]$

$\Rightarrow (\frac{a}{d}, \frac{b}{d}) = 1$

4) $(a,b)=d \Leftarrow (\frac{a}{d}, \frac{b}{d}) = 1$

$\Leftrightarrow (\frac{a}{d})^n, (\frac{b}{d})^n] = 1$

$\Leftrightarrow (\frac{a^n}{d^n}, \frac{b^n}{d^n}) = 1$

$\Leftrightarrow (a^n, b^n) = d^n$

5) $(a,b)=1 \wedge (a,c)=1 \Rightarrow (a,bc)=1$

$\exists x_1,y_1 \in \mathbb{Z}[ax_1+by_1=1]$

$\exists x_2,y_2 \in \mathbb{Z}[ax_2+cy_2=1]$

$\exists x_1,x_2,y_1,y_2 \in \mathbb{Z}[a^2x_1x_2 + acx_1y_2 + abx_2y_1 + bcy_1y_2 = a(ax_1x_2 + cx_1y_2 + bx_2y_1) + bc(y_1y_2) = 1]$

$\Rightarrow (a, bc) = 1$

$(a,b)=1 \Rightarrow (a+b, a)=1 \wedge (a+b, b)=1 \Rightarrow (a+b, ab)=1$

Theorem (Division Algorithm). For any $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. There exists unique (q,r) so that $a = bq + r$; $0 \leq r < b$

(Here q and r are called quotient and remainder respectively.)

Subject:

Year. Month. Date. ( )

Division Algorithm

Theorem — for any $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$, there is a unique pair of integer (q, r) so that

$$a = bq + r \quad ; \quad 0 \le r < b.$$

proof — $S = \{a - bx \mid x \in \mathbb{Z}, a - bx \ge 0\}$

$x = -|a|$

$a - bx = a - b(-|a|) = a + b|a| \ge 0 \implies S \neq \emptyset$

استفاده از اصل خوش‌ترتیبی

$\exists s \in S \; \forall s \in S \; [r \le s]$ ← well-ordering principle

$r \in S \implies \exists q \in \mathbb{Z} \; [r = a - bq]$

$\implies \exists q \in \mathbb{Z} \; [a = bq + r]$

چون r کوچکترین عضو S است $r - b$ عضو S نیست

We claim that $0 \le r - b = a - bq - b = a - b(q+1) \implies$

$r - b \in S$ that is contradiction

$\implies \exists q \exists r \; [0 \le r < b \wedge a = bq + r]$

uniqueness: $a = bq + r \quad 0 \le r < b$

$a = bq' + r' \quad 0 \le r' < b$ ×

$b(q - q') = r' - r \implies b \mid (r' - r) \implies b \le |r' - r| < b \implies$

$r' - r = 0 \implies r = r' \implies q = q'$

Subject:

Year. Mouth. Date. ( )

Diophantine Equations

Example) (linear Diophantine equation of two variables)

$$ax+by=c \qquad a,b,c \in \mathbb{Z}$$

Theorem The Diophantine equation $ax+by=c$ has a solution iff $(a,b)|c$

proof

$ax+by=c$ has a solution $\Rightarrow (a,b)|c$

$\downarrow$

$\exists x_0, y_0 \in \mathbb{Z} \left[ax_0+by_0=c\right] \wedge (a,b) \mid a,b$

$\Rightarrow (a,b)|c$

$(a,b)|c \Rightarrow$ $ax+by=c$ has a solution

$(a,b)|c \Rightarrow \exists e \in \mathbb{Z} \left[c=(a,b)e\right]$

$\exists x_0, y_0 \in \mathbb{Z} \left[(a,b)=ax_0+by_0\right] \Rightarrow$

$\exists x_0, y_0 \in \mathbb{Z} \left[e(a,b)=a(ex_0)+b(ey_0)=c\right] \Rightarrow$

$ax+by=c$ has a solution

Subject:

Year Month Date ( )

Theorem - If (x_0, y_0) is a solution to $ax+by=c$, then any solution to the equation is obtained from

$$x = x_0 + k\frac{b}{(a,b)}, \text{ and}$$

$$y = y_0 - k\frac{a}{(a,b)}$$

where $k \in \mathbb{Z}$

$$a\left(x_0 + k\frac{b}{(a,b)}\right) + b\left(y_0 - k\frac{a}{(a,b)}\right) = ax_0 + by_0 = c$$

any pair of integers in the form of above expression, is a solution to the equation

Assume (x, y) is a solution to the equation

$$\Rightarrow ax+by=c \Rightarrow a(x-x_0) = b(y_0-y) \Rightarrow \frac{a}{(a,b)}(x-x_0) = \frac{b}{(a,b)}(y_0-y)$$

$$\Rightarrow \frac{b}{(a,b)} \mid \frac{a}{(a,b)}(x-x_0) \xrightarrow{①} \frac{b}{(a,b)} \mid (x-x_0)$$

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$$

Euclid's lemma

$$\Rightarrow \exists k \in \mathbb{Z} \left[x = x_0 + k\frac{b}{(a,b)}\right].$$

Similarly, $\exists k' \in \mathbb{Z} \left[y = y_0 - k'\frac{a}{(a,b)}\right]$

$$\Rightarrow \frac{a}{(a,b)}\left(x_0 + k\frac{b}{(a,b)}\right) + b\left(y_0 - k\frac{a}{(a,b)}\right) = c \Rightarrow$$

$$\frac{ab}{(a,b)}(k-k') = 0 \Rightarrow k = k'$$

Therefore any solution to the equation is of the form above

PAPCO

Subject:

Year. Month. Date. ( )

Example) According to the Division Algorithm.

$\forall a \in \mathbb{Z}\ \exists q \in \mathbb{Z}\ [a = 2q + 0 \vee a = 2q + r]$

(زوجي) even (فردي) odd

Example) Prove that for any positive integer n there is a positive integer m including only 0's and/or 1's so that $n \mid m$.

n	m
2	10
3	111
4	100
5	10
6	1110
7	1001
8	1000

$1 = nq_1 + r_1 \quad 0 \le r_1 < n$

$11 = nq_2 + r_2 \quad 0 \le r_2 < n$

$\underbrace{11\ldots1}_{(n+1)\text{ times}} = nq_{n+1} + r_{n+1} \quad 0 \le r_{n+1} < n$

By each hole principle $\Rightarrow \exists\, 1 \le i < j \le n+1\ [r_i = r_j] \Rightarrow$

$\underbrace{11\ldots1}_{i\text{ times}} - \underbrace{11\ldots1}_{j\text{ times}} = \underbrace{11\ldots100\ldots0}_{i-j\text{ times}\quad j\text{ times}} = n(q_i - q_j)$

Subject.

Year. Month. Date. ( )

Theorem (Euclidean Algorithm) In the following procedure, $r_K = (a,b)$

$$a = bq_1 + r_1 \quad , \quad 0 < r_1 < b$$

$$b = r_1 q_2 + r_2 \quad , \quad 0 < r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \quad , \quad 0 < r_3 < r_2$$

$$\vdots$$

$$r_{k-2} = r_{k-1} q_k + r_k \quad 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_k q_{k+1}$$

$r_k | a$, $r_k | b$, $r_k \geq 0$

Example) Find the greatest common devisor of 250 and 111, and write it as a linear combination of 250 and 111.

$$250 = 111(2) + 28$$

$$111 = 28(3) + 27$$

$$28 = 27(1) + 1 \quad \text{---} \textcircled{1} \rightarrow (250, 111)$$

$$27 = 1(27) + 0$$

$$1 = 28 - 1(27)$$

$$= 28 - 1(111 - 3(28))$$

$$= 4(28) - 1(111)$$

$$= 4(250 - 2(111)) - 1(111)$$

$$= 4(250) + (-9)(111)$$

Subject:

Year. Month. Date. ( )

Solve:

$(m-9)^2 m! + (n-8)^2 n! + 50\,p! + 49\,q! = \sqrt{\overline{mnpq}}$

where m, n, p, q are integer and $\overline{mnpq}$ is a 4-digit number with the digit $m, n, p,$ and q

$\overline{mnpq}_{min} = 99$

$\overline{mnpq}_{max} = 99$ $\qquad \overline{mnpq} = 99^2 = 9801$ ($m\ n\ p\ q$)

Lemma if $a, b \in \mathbb{Z}^+$ and p is a prime, then

$p \mid ab \Rightarrow p \mid a \vee p \mid b$

Proof

$p \nmid a \Rightarrow (p, a) = 1$

$\xrightarrow[\text{lemma}]{\text{Euclidean}} p \mid b$

Extension $p \mid a_1 a_2 \dots a_n \Rightarrow \exists\, 1 \le i \le n \ [p \mid a_i]$

Theorem (Fundamental Theorem of Arithmatic)

Any integer $n > 1$ can be written as product of primes uniquely, up to the order of the primes. (Here, a singel prime can be considered as a product of factor.)

proof

Existence + Uniqueness

$\forall k$ $2, 3, \dots, k$ Can be written $\qquad 2, 3, \dots, k$ can be written

$\forall k$ $k+1$ Can be written $\qquad k+1 = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$

$k+1 = m_1 m_2 \qquad 1 < m_1, m_2 < 2 \qquad p \mid q_1 q_2 \dots q_t \Rightarrow p_1 \mid q_1 \Rightarrow p_1 = q_1$

PaPCO

Subject:

Year. Month. Date. ( )

$\Rightarrow \quad k+1 > \frac{k+1}{p_1} = p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_t$

Induction Hypothesis $\Rightarrow s = t, p_2 = q_2, \ldots, p_s = q_t$

Factorization of $n > 1$ is the unique product of prime which equals n.

Theorem if $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ and $= p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ where $\alpha_i, \beta_i \geq 0$

then

$$(a,b) = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$$

$$[a,b] = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$$

Proof - As an exercise.

Theorem (Bertrand's conjecture) for any integer $n > 1$, There is a prime between n and $2n$

2	3	4
3	5	6
4	7	8
5	7	10
6	7	12
7	13	14

Subject:

Year. Month. Date. ( )

Exercise) For any $n>1$,

$$1+\frac{1}{2}+\dots+\frac{1}{k}=\sum_{k=1}^{n}\frac{1}{k}\notin\mathbb{Z}$$

($n!$ is factorized as $p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_k$ for any $n>1$)

$2!=2$ $\quad 3!=2\times3$ $\quad 4!=2^3\times3$

$5!=2^3\times3\times5$ $\quad 6!=2^4\times3^2\times5$

Theorem) $\sum_{p\,\text{primes}}\frac{1}{p}$ is divergent.

$$\frac{1}{p_1}+\frac{1}{p_2}+\dots+\frac{1}{p_i}+\dots$$

این سری به چه عددی همگرا می‌شود

$$\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\dots=1$$

3,5 $\quad$ 5,7 $\quad$ 7,9 $\quad$ 9,11 $\quad$ 11,13 $\quad$ 17,19

twin

به این اعداد چه می‌گوییم؟

Congruence (modular Arithmatic) همنشتی

$a\equiv b \pmod m \iff m\mid a-b$

$25\equiv3 \pmod{11}$ $\quad 8\equiv3 \pmod5$

Subject:
Year. Month. Date. ( )

congruence is an equivalence relation
(in a specifice module)

در سیستم modular تنها m عدد وجود دارد که عبارتند از ← $m \rightarrow \{0, 1, 2, \dots, m-1\}$
یعنی همیشه یکی از این اعداد این مجموعه حاصل می‌شود

$m = 8 \quad 10 = 2 \quad 25 = 1$

$2 \times 8 - 15 + 2 \equiv$ ⟸ در modular 8
$2 \times 0 - 1 + 2 = 3$
$2 \times 15 + 22 = 4$

$m = 26$
$\frac{7}{9} = ?$ باید مضربی از 26 را به 7 اضافه کنیم تا بر 9 بخش پذیر شود

$\frac{7 - 2 \times 26}{9} = \frac{-45}{9} = -5 = 21$

$\frac{1}{9} = x \qquad 9x \equiv 1 \pmod{26}$
$\quad \hookrightarrow x = 3$

$ax \equiv b \pmod{}$ معادله همنهشتی
$x \in \{1, \dots, m\}$ یعنی x را پیدا کن بین 1 تا m

$m \mid ax - b \Rightarrow my = ax - b$
$\Rightarrow ax - my = b$
این معادله جواب دارد ⟹ $(a, m) \mid b$ ⟹ There is a solution

Subject:

Year. Month. Date. ( )

$(a,m)=1 \Rightarrow$ The solution is unique.

$(a,m)=d \Rightarrow$ There is d solution.

Theorem (Euler - Fermat):

if $(a,m)=1$ $\quad a^{\varphi(m)} \equiv 1 \pmod m$.

$x = b\, a^{\varphi(m)-1} \pmod m$

is the unique solution of $ax \equiv b \pmod m$ if $(a,m)=1$

Relations and Functions:

Definition: For sets A and B, the cartesian product of A and B is denoted by $A \times B$ and equals $\{(a,b) \mid a \in A, b \in B\}$.

- $A \times B \neq B \times A$; $\{A \neq B,\ A \neq \emptyset,$ and $B \neq \emptyset\}$
- $|A \times B| = |A| \times |B|$
- $A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i$ for $1 \le i \le n\}$.
  $A_1 \times A_2 \times A_3 \neq A_1 \times (A_2 \times A_3) \neq (A_1 \times A_2) \times A_3$

Definition: For sets A and B, any subset of $A \times B$ is called a relation from A to B. Any subset of $A \times A$ is called a binary relation on A.

The number of relation from A to $B = 2^{|A||B|}$ when A and B are finite sets.

Subject:

Year. Month. Date. ( )

Theorem For any given sets A, B and C:

a) $A \times (B \cap C) = (A \times B) \cap (B \times C)$

b) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

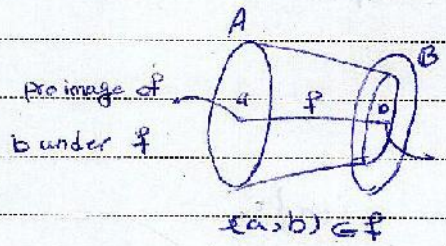
c) $(A \cap B) \times C = (A \times C) \cap (B \times C)$ and

d) $(A \cup B) \times C = (A \times C) \cup (B \times C)$.

Proof - As an exercise

Definition For nonempty sets, A and B, a function f from A to B is denoted by $f: A \to B$ and is a relation from A to B in which every element of A appears exactly once as the first component and ordered pair in the relation.

$$\forall x \in A\ \exists y \in B\ [(x,y) \in f] \wedge \forall x \in A\ \forall y_1, y_2 \in B\ [(x,y_1) \in f \wedge (x,y_2) \in f \to y_1 = y_2]$$



$f: A \to B$

Domain — codomain

For any $X \subseteq A$

$$f(X) = \{y \in B \mid \exists x \in X\ [(x,y) \in f]\}$$

is called the image of X under f. Particularly f(A) is called the range of f.

The number of functions of $f: A \to B = |B|^{|A|}$ where A and B are finite sets.

Subject:

Year. Mouth. Date. ( )

Definition- A function $f: A \to B$ is called one-to-one or injective if each element of B appears at most once as the image of an element of A.

$\forall y \in B [(x_1, y) \in f \wedge (x_2, y) \in f) \to x_1 = x_2]$, or

$\forall x_1, x_2 \in A [f(x_1) = f(x_2) \to x_1 = x_2]$.

The number of one-to-one function $f: A \to B$ where A and finite $= P(|B|, |A|)$

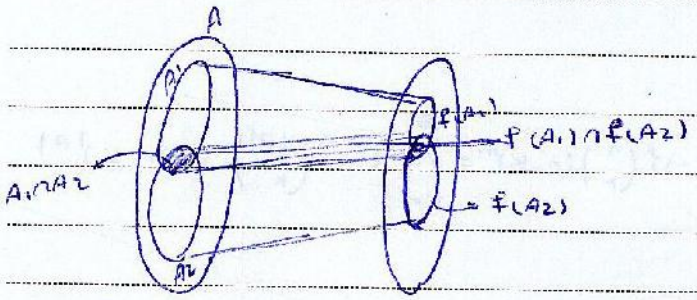
$|B| \geq |A|$

Theorem- Let $f: A \to B$ and $A_1, A_2 \subseteq A$ then,

a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$

b) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$, and

c) $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ if f is injective.



proof b) $y \in f(A_1 \cap A_2) \to \exists x \in (A_1, A_2) [(x, y) \in f]$

$\to \exists x \in A_1 [(x, y) \in f] \wedge \exists x \in A_2 [(x, y) \in f]$

$\to y \in f(A_1) \wedge y \in f(A_2)$

$\to y \in f(A_1) \cap f(A_2)$

$\to f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2) \to y$

Subject:

Year. Month. Date. ( )

c) $y \in f(A_1) \cap f(A_2) \Rightarrow y \in f(A_1) \wedge y \in f(A_2)$

$\Rightarrow \exists x \in A_1 [(x,y) \in f] \wedge \exists x \in A_2 [(x,y) \in f]$

$\overset{f \text{ is injective}}{\Rightarrow} \exists x \in A_1 \cap A_2 [(x,y) \in f] \Rightarrow y \in f(A_1 \cap A_2) \overset{\text{injective}}{\Rightarrow}$

$f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$

Definition. A function $f: A \to B$ is called onto or surjective if $f(A) = B$. In otherwords.

$\forall y \in B \; \exists x \in A [(x,y) \in f]$

The number of onto function from A to B where A and B are finite sets:

Assume $A = \{a_1, \ldots, a_m\}$ and $B = \{b_1, \ldots, b_n\}$. Euideutaly $m \geq n$.

Inclusion and Exclusion

$C_i : b_i \notin f(A)$

$1 \leq i \leq n$

$|S| = n^m$

$= n^m - \binom{n}{1}(n-1)^m + \binom{n}{2}(n-2)^m - \ldots + (-1)^{n-1}\binom{n}{n-1}1^m$

$= \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m = \sum_{k=0}^{|B|} (-1)^k \binom{|B|}{k} (|B|-k)^{|A|}$

Subject:

Year. Month. Date. ( )

$|A| = m$, $|B| = n$

The number of onto functions from A to B =

$$n!\, S(m,n) = n!\left(\frac{1}{n!}\sum_{k=0}^{n}(-1)^k\binom{n}{n-k}(n-k)^m\right)$$

$S(m,n)$: stirling's number of second kind

Theorem – Let $m,n \in \mathbb{Z}^+$ then

$$S(m+1,n) = S(m,n-1) + nS(m,n)$$

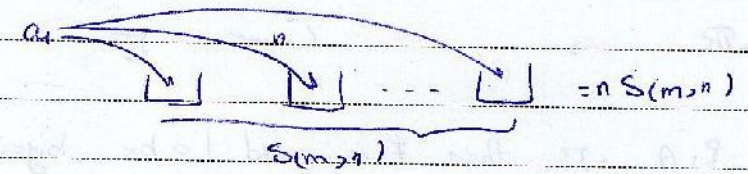
$a_1, a_2, \ldots, a_{m+1}$

case 1)

a_1 is in a container alone.

$S(m,n-1)$

case 2) other wise



$\Rightarrow S(m+1,n) = S(m,n-1) + nS(m,n)$

Definition – For any set A, any function $f: A \times A \to A$ is called a binary operation on A.

$+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$

$+ : (\sqrt{2}, \sqrt{-2}) = 0$

$+ : (2.1, 3.2) = 5.3$

Subject:
Year. Month. Date. ( )

Definition _ A function $g: A \to A$ is called a unary or monary operation on A

Definition _ A binary operation f on A is said to be commutative if $f(a,b) = f(b,a)$ for all $(a,b) \in A \times A$.
It is called associative if for any $a, b, c \in A$

$$f(f(a,b),c) = f(a, f(b,c))$$

Example _ $f(a,b) = a|b|$ from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$

$$f(2,-3) = 2|-3| = 6 \neq f(-3,2) = -3|2| = -6$$

$$f(f(a,b),c) = f(a|b|, c) = a|b||c|$$

$$f(a, f(b,c)) = a|f(b,c)| = a|b|c|| = a|b||c|$$

$/ : \mathbb{R} \times \mathbb{R} - \{0\} \to \mathbb{R}$ $\longrightarrow$ تقسیم نیست

Definition _ If $f: A \to B$, then f is said to be bijective or to be one-to-one correspondence, if f is both one-to-one and onto.

Example) $f: \mathbb{R} \to \mathbb{R}$

$f(x) = 2x - 1$

Infinite, Enumerable

PAPCO

Subject:

Year. Month. Date. ( )

$0.d_1d_2d_3d_4\cdots$

$d_1 \neq 2 \quad d_2 \neq 1 \quad d_3 \neq 0 \quad d_4 \neq 8$

1	0.251252 92 - -
2	0.720192 52 - -
3	0.010622202 - -
4	0.299857656 - -
5	
⋮	

Definition The function $1_A : A \to A$, defined $1_A(a) = a$ for all $a \in A$, is called the identity function for A.

Definition If $f, g : A \to A$ we say that f and g are equal, and write $f = g$, if $f(a) = g(a)$ for all $a \in A$

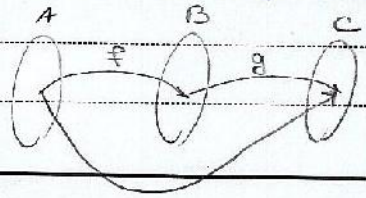
Definition If $f : A \to B$ and $g : B \to C$, we define the composite function $gof : A \to C$ by $(gof)(a) = g(f(a))$ for each $a \in A$

Example) $A = \{1,2,3,4\}$, $B = \{a,b,c\}$, $C = \{w,x,y,z\}$

$f = \{(1,a),(2,a),(3,b),(4,c)\}$

$g = \{(a,x),(b,y),(c,z)\}$

$\Rightarrow gof = \{(1,x),(2,x),(3,y),(4,z)\}$



$g \circ f$

Subject:

Year. Month. Date. ( )

Example) $f: A \to B$

$f \circ 1_A(x) = f(1_A(x)) = f(x)$

$A \to B$ $\qquad$ $A \to B$

$\Rightarrow f \circ 1_A = f$

$1_B \circ f = 1_B(f(x)) = f(x) \Rightarrow 1_B \circ f = f$

$A \to B$ $\qquad$ $A \to B$

Theorem Let $f: A \to B$ and $g: B \to C$

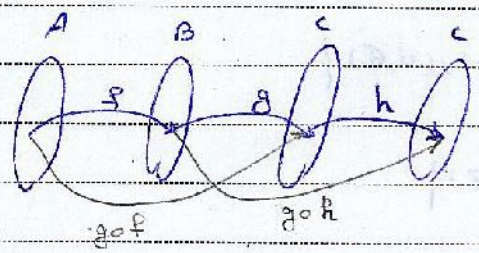
a) If f and g are one-to-one, then $g \circ f$ is one-to-one.

b) If f and g are onto, then $g \circ f$ is onto.

Proof As an exercise!

Theorem If $f: A \to B$, $g: B \to C$, and $h: C \to D$, then

$(h \circ g) \circ f = h \circ (g \circ f)$



Subject:

Year. Month. Date. ( )

Definition If $f: A \to B$, then f is said to be invertible if there is a function $g: B \to A$ such that $gof = 1_A$ and $fog = 1_B$.

Theorem The function g satisfying the condition in the above difinition is unique (if it exists).

$$g = g o 1_B = g o (foh) = (gof) oh = 1_A oh = h$$

The unique g is the above difinition is called inverse of f and is denoted by f^{-1}.

$$f: A \to B \iff \exists g: B \to A \; [fog = 1_B \wedge gof = 1_A]$$

$$g = f^{-1}$$

$$R^c = \{(x,y) \mid (y,x) \in R\}$$

$$R = \{(1,2),(2,3)\} \to R^c = \{(2,1),(3,2)\}$$

$$f = \{(1,2),(3,2)\} \to f^c = \{(2,1),(2,3)\}$$

f^c is a function

$$fof^c = 1$$

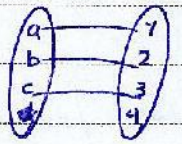
$$f^c of = 1$$

P4PCO

Subject:

Year. Month. Date. ( )

Theorem - A function $f: A \to B$ is invertible if and only if it is one-to-one and onto



proof -

(1) $f: A \to B$ is invertible

$\Rightarrow \exists g: A \to B \quad [g \circ f = 1_A \wedge f \circ g = 1_B]$

$\forall a_1, a_2 \; [f(a_1) = f(a_2) \to a_1 = a_2]$ function is one-to-one

(یک‌به‌یک)

$f(a_1) = f(a_2) \Rightarrow g(f(a_1)) = g(f(a_2)) \Rightarrow (g \circ f)(a_1) = (g \circ f)(a_2) \Rightarrow$

$1_A(a_1) = 1_A(a_2) \Rightarrow a_1 = a_2 \Rightarrow$

$*$ is satisfied

$b \in B \Rightarrow g(b) \in A \Rightarrow f(g(b)) = f \circ g(b) = 1_B(b) = b. \Rightarrow$

f is onto

(2) one-to-one + onto $\Rightarrow$ invertible

f is onto $\Rightarrow \forall b \in B \; \exists a \in A \; [f(a) = b]$

f is one-to-one $\Rightarrow \exists g: B \to A \; [f(a) = b \to g(b) = a]$

$\Rightarrow g \circ f = 1_A \wedge f \circ g = 1_B$

$\Rightarrow f$ is invertible

Subject:

Year. Month. Date. ( )

Theorem If $f: A \to B$ and $g: B \to C$ are invertible functions. then $g \circ f : A \to C$ is invertible and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$

$f^{-1}: B \to A$, $g^{-1}: C \to B \Rightarrow f^{-1} \circ g^{-1}: C \to A$

$(g \circ f) \circ (f^{-1} \circ g^{-1}) = g \circ f \circ (f^{-1} \circ g^{-1})$

$= g \circ ((f \circ f^{-1}) \circ g)$

$= g \circ (1_B \circ g^{-1})$

$= g \circ (g^{-1}) = 1_C$

$(f^{-1} \circ g^{-1}) \circ (g \circ f) = f^{-1} \circ ((g^{-1} \circ g) \circ f) = f^{-1} \circ (1_B \circ f)$

$= f^{-1} \circ f = 1_A$

Theorem Let $f: A \to B$ for finite sets A and B. Where $|A| = |B|$ then, the following statements are equivalent.

(a) f is one-to-one

(b) f is onto, and

(c) f is invertible.

Compare onto & one-to-one for $|A| = |B|$ where B, A, $f: A \to B$ ✓

Subject:

Year. Month. Date. ( )

Computational Complexity.

Algorithms X Algorithms

instance

space of instance

Algorithm

solution space

function

problem =

function → is unique

Algorithm → not unique

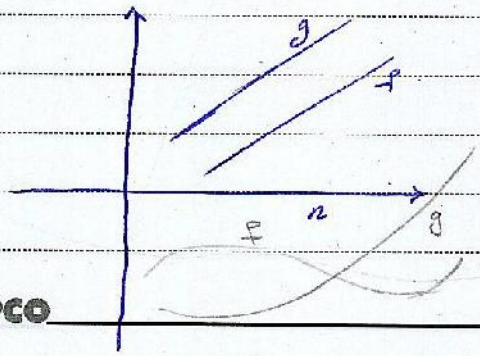
problem = Sorting

Algorithm: Mergesort, quicksort, bubble sort

quicksort, Mergesort, Insertion sort, bubble sort

Definition: Let $f, g: \mathbb{Z}^+ \to \mathbb{R}$. We say that g dominates f (or f is dominated by g) if

$$\exists m \in \mathbb{R}^+ \; \exists k \in \mathbb{Z}^+ \; \forall n \in \mathbb{Z}^+ \left[n \geq k \rightarrow |f(n)| \leq m|g(n)| \right]$$



i.e. g dominates f, g

Subject:

Year. Month. Date. ( )

Example:

$f(n) = 5n$, $g(n) = n^2$

$\exists m \in \mathbb{R}^+ \; \exists K \in \mathbb{Z}^+ \; \forall n \in \mathbb{Z}^+ \; [n \geq K \rightarrow 5n \leq mn^2]$

$m = 5 \quad K = 1$

$\Rightarrow$ g dominates f

$f \in O(g)$ ⟷ f is in the order of g

$\exists H \in \mathbb{R}^+ \; \exists K \in \mathbb{Z}^+ \; \forall n \in \mathbb{Z}^+ \; [n \geq K \rightarrow n^2 \leq m|5n|]$

$\forall n \geq K \; [n \leq 5m]$

$g \not\in O(f)$

$O(g) = \{ f : \mathbb{Z}^+ \rightarrow \mathbb{R} \mid \exists m \in \mathbb{R}^+ \; \exists K \in \mathbb{Z}^+ \; \forall n \in \mathbb{Z}^+ \; [n \geq K \rightarrow |f(n)| \leq m|g(n)|] \}$

$f \in O(g)$

Example: $f(n) = 5n^2 + 2n + 1$ $\quad g(n) = n^2$

$|f(n)| = f(n) = 5n^2 + 2n + 1 \leq 5n^2 + 2n^2 + n^2 = 8n^2 = 8|g(n)| \Rightarrow f \in O(g)$

$|g(n)| = n^2 \leq 5n^2 + 2n + 1 = |f(n)| \Rightarrow g \in O(f)$ $\quad f \in \Theta(g)$

Example: $f(n) = a_t n^t + a_{t-1} n^{t-1} + \dots + a_1 n + a_0$ $\quad a_i \in \mathbb{R}$

$g(n) = n^t$. prove that $f \in O(g)$

$|f(n)| = |a_t n^t + a_{t-1} n^{t-1} + \dots + a_1| \leq |a_t n^t| + |a_{t-1} n^{t-1}| + \dots + |a_1| \leq$

$|a_t||n^t| + |a_{t-1}||n^t| + \dots + |a_1||n^t| = \left(\sum_{i=0}^{t} |a_i|\right) n^t \Rightarrow f \in O(g)$

Subject:

Year. Month. Dute. ( )

Exercise) prove that $n^t \in O(a_t n^t + \dots + a_1 n + a_0)$ where $a_i \in \mathbb{R}$

Example) Prove that $(1^k + 2^k + \dots + n^k) \in \Theta(n^{k+1})$

$1^k + 2^k + \dots + n^k \leq \underbrace{n^k + n^k + \dots + n^k}_{n \text{ times}} = n^{k+1} \Rightarrow 1^k + 2^k + \dots + n^k \in O(n^{k+1})$

$1^k + 2^k + \dots + n^k \geq [\frac{n}{2}]^k + [\frac{n}{2}+1]^k + [\frac{n}{2}+2]^k + \dots + n^k \geq (\frac{n}{2})^k + (\frac{n}{2})^k + \dots + (\frac{n}{2})^k \geq$

(از نصف جمله آخر نوشتیم)

$\frac{n}{2}(\frac{n}{2})^k = \frac{n^{k+1}}{2^{k+1}} \Rightarrow n^{k+1} \leq (2^k+1)(1^k + 2^k + \dots + n^k) \Rightarrow$

(این کوچکتر از همینی است)

$n^{k+1} \in O(1^k + 2^k + \dots + n^k)$

Example) Calculate the time complexity of the following algorithm

```
Begin
    I:=1;
    Factorial:=1;
    While i<=n do
    begin
        Factorial:=i*factorial;
        i:=i+1;
    end;
    writeln('the value of ', n, 'factorial is', Factorial, '.')
end;
```

PAPCO

$(3+3n)$ تعداد دستورالعمل‌هایی که اجرا می‌شود

Max(Time) = t_0

پیچیدگی زمانی $t(n) \leq (3+3n)t_0 \Rightarrow t(n) \in O(n)$

اجرا شدن نیازدارد

Example) Time complexity?

یک آرایه A: A[1] A[2] ... A[n]

یک عدد Key

باید جستجو کنیم ببینیم key در A است یا نه

زمانی که صرف می‌شود به نوع جستجو بستگی دارد.

- Best Case: 1

- worst Case: n

- Averge Case: فرض کنیم در array عدد key را با احتمال P پیدا کنیم و میانگین بگیریم

P: احتمال اینکه کلید در آرایه باشد

q: کلید در آرایه نباشد $\Rightarrow P+q=1$

اگر کلید در Array هست احتمال اینکه کلید در هر یک از خانه‌ها باشد یکسان است

$$P: \frac{P}{n}\cdot 1+\frac{P}{n}\cdot 2+\dots+\frac{P}{n}\cdot n+qn=\frac{P}{n}\left(\frac{n(n+1)}{2}\right)+qn=\frac{P(n+1)+2qn}{2}$$

$$\frac{n+qn+(1-q)}{2}\in\Theta(n)$$

Subject:

Year. Month. Date. ( )

The Pigeonhole Principle

If m pigeon occupy n pigeonholes and $m > n$, then there is at least one pigeonhole with two or more pigeons roosting in it.

Example) Any subset of size six from the set $S = \{1, 2, 3, \ldots, 9\}$ must contain two elements whose sum is 10.

$\{1,9\}, \{2,8\}, \{3,7\}, \{4,6\}, \{5\}$ ← ...

$A \subseteq S \rightarrow A = \{x_1, x_2, \ldots, x_6\}$

Example) Prove that if 101 integer are selected from set $\{1, 2, \ldots, 200\}$ then there are two integers such that one divides the other.

$n = 2^k \cdot t$, t is odd $\quad t \in \{1, 3, 5, \ldots, 199\} = A$

$|A| = 100$

$n_1 = 2^{k_1} \cdot t$, $n_2 = 2^{k_2} \cdot t \rightarrow n_1 | n_2$ or $n_2 | n_1$

Subject:

Year. Month. Date. ( )

Definition A relation R on a set A is called partial order, or partial ordering relation, if R is reflexive, antisymmetric and transitive. That is holds the following proportion:

$\forall a \in A\,[aRa]$ reflexive

$\forall a,b \in A\,[(aRb \wedge bRa \rightarrow a=b]$ antisymmetric

$\forall a,b,c \in A\,[(aRb \wedge bRc) \rightarrow aRc]$

If R is a partial order on A, (A,R) is called a partially ordered set (poset)

Example) $(Z, \leq)$ is a poset

$(Z, <)$ not poset $\Rightarrow \forall a,b \in A\,[(aRb \wedge bRa \not\rightarrow a=b]$

subset ... $(\mathcal{P}(A), \subseteq)$ is a poset

$\forall A_1 \in \mathcal{P}(A)\,[A_1 \subseteq A_1]$

$\forall A_1, A_2 \in \mathcal{P}(A)\,[A_1 \subseteq A_2, A_2 \subseteq A_1 \Rightarrow A_1 = A_2]$

$\forall A_1, A_2, A_3 \in \mathcal{P}(A)\,[A_1 \subseteq A_2 \wedge A_2 \subseteq A_3 \Rightarrow A_1 \subseteq A_3]$

Example) How many reflexive relation are there on A?

antisymmetic

transitive

Symmetic

$|A| = n$

reflexive $= 2^{n^2-n}$

Antisymmetic $= 2^n \cdot 3^{\frac{n^2-n}{2}}$

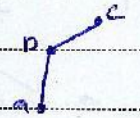
Subject:

Year. Month. Date. ( )

Symmetric $= 2^{n} \cdot 2^{\frac{n^2-n}{2}} = 2^{\frac{n^2+n}{2}}$ (a,a)

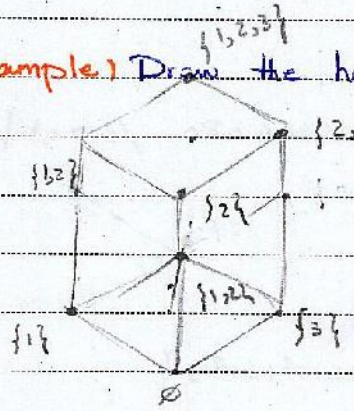
Definition A relation R on A is called an equivalence relation on A if it is reflexive, symmetric and transitive

Hasse diagram



$R = \{(a,a),(b,b),(c,c),(a,b),(b,c),(a,c)\}$

Example) Draw the hasse diagram of $(\mathcal{P}(A), \subseteq)$ where $A = \{1,2,3\}$



Definition If (A,R) is a poset, then an element $n \in A$ is called a maximal element of A if $\forall a \in A [a \neq n \rightarrow n R a]$

An element $y \in A$ is called a minimal element of a if $\forall a \in A [a \neq y \rightarrow a R y]$

Subject:

Year. Month. Date. ( )

هر مجموعه‌ای می‌تواند بیش از یک maximal و minimal داشته باشد

$A=\{1,2\}$, $R=\{(1,1),(2,2)\}$

maximal = 1 , 2 → هیچ عنصری ارتباط ندارد

minimal = 1,2 → هیچ عنصری با بالایی ارتباط ندارد

$A=\{1,2,3\}$ $R=(\mathcal{P}, \subseteq)$

maximal = $\{1,2,3\}$ زیر مجموعه‌ی هیچ مجموعه‌ای جز خودش نیست

minimal = $\{\}$ هیچ مجموعه‌ای subset این نیست

تمرین مجموعه

$(\mathcal{P}(A) \setminus \{\emptyset, A\}, \subseteq)$

maximal : $\{1,2\}$, $\{1,3\}$, $\{2,3\}$

minimal : $\{1\}$, $\{2\}$, $\{3\}$

$(\mathbb{Z}, \leq)$ حتماً یک poset - maximal / minimal ندارد

مگر اگر متناهی باشد حتماً maximal / minimal دارد

Theorem.- If (A, R) is a poset and A is finite, then A minimal and a minimal of A both exist.

$a_1 \to a_2 \to a_3 \dots \to a_n$ اگر a به a ربط نداشت a_2 a_1 ربط دارد

در آخر به a_n می‌رسیم چون اگر a_n به چیزی ربط داشته باشد به تناقض می‌رسیم

PAPCO

Subject:

Year. Month. Date. ( )

Definition If (A, R) is a poset, then an element $n \in A$ is called a least element if $\forall a \in A\ [nRa]$. An element $y \in A$ is called a greatest element (maximal) of A if $\forall a \in A\ [aRy]$

Definition - Let (A, R) be a poset with $B \subseteq A$. An element $n \in A$ is called a lowerbound of B if $\forall b \in B\ [nRb]$. An element $y \in A$ is called an upper bound of B if $\forall b \in B\ [bRy]$

Example) $(\mathbb{R}, \leq)$

$B \subset [0, 1)$

upperbound $\rightarrow -1, -10, -\sqrt{2}, 0, \ldots$

lowerbound $\rightarrow 1, 2, \sqrt{3}, \ldots$

least upperbound (lub)

greatest lowerbound (glb)

Example) The relation is '$\leq$'.

a) $A = \mathbb{R}$, $B = [0, 1)$; $glb(B) = 0$ $\quad lub(B) = 1$

b) $A = \mathbb{R}$, $B = \{q \in \mathbb{Q} \mid q^2 < 2\}$; $glb(B) = -\sqrt{2}$, $lub(B) = \sqrt{2}$

c) $A = \mathbb{Q}$, $B = \{q \in \mathbb{Q} \mid q^2 < 2\}$

no glb or lub exist.

Subject:

Year. Month. Date. ( )

Definition The poset (A, R) is called a lattice if for any $x, y \in A$, the elements $lub(\{x, y\})$ and $glb(\{x, y\})$ both exist.

poset — lattice 반례

- $(\mathbb{Z}, \leq)$ is a lattice

$\forall x, y \in \mathbb{Z}\ [lub(\{x, y\}) = max(\{x, y\}) \wedge glb(\{x, y\}) = min(\{x, y\})]$

- $(\mathcal{P}, \subset)$ $\forall A_1, A_2 \in \mathcal{P}\ [lub(\{A_1, A_2\}) = A_1 \cup A_2,\ glb(\{A_1, A_2\}) = A_1 \cap A_2]$

Subject: زندگی خیلی خوب نیست اما ارزش تلاش کردن را دارد هر چند هیچ جوابی نگیری تا زمانیکه امید داری.
Year. Month. Date. ( )

Recurrence Relations (Equations)

یک معادله ای برای سری پیدا کنیم که باید حل بشود

$a: \mathbb{Z}^{\geq 0} \longrightarrow \mathbb{R}$

یک رابطه ای بین مقادیر مختلف داده شده دنباله sequence را بیان کرد.

$a_n = 2a_{n-1}$ where $n \geq 1$ — یعنی a_n را برحسب a_{n-1} بیان کنید

$a_{n-1} = 2a_{n-2}$

$\vdots$

$a_2 = 2a_1$

$a_1 = 2a_0$

$\Longrightarrow a_n = 2^n a_0$ — first order, order $= 1$

$a_0 = 2 \Longrightarrow a_n = 2^{n+1}$

یک جمله دنباله که به چند جمله ی قبل مربوط است order آن را می گویند

$a_n - 2a_{n-5} + 3a_{n-3} = 0$ of order 5

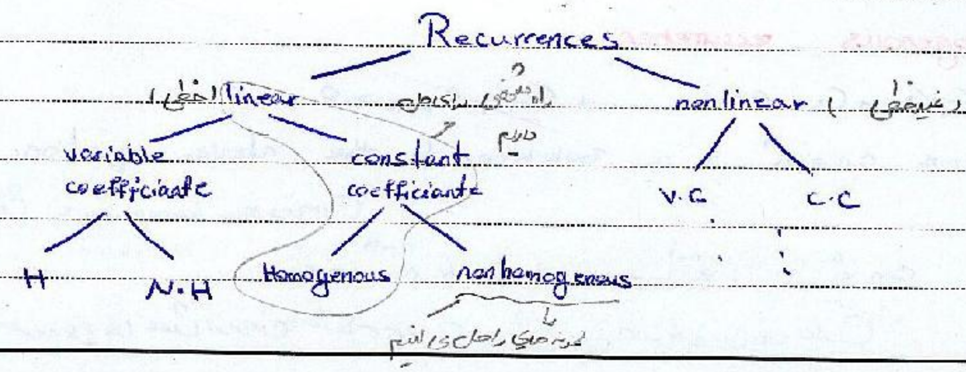
$a_n^2 + 3a_n = 5n^2 + 1$ خطی نیست (اگر a_n ها به صورت $a_n + b_n$ باشند)

$a_n + 3a_{n-1} + 2a_{n-4} = 0$ خطی است

$\sin a_n = 2\ln n + 1$ خطی نیست

$a_n + n a_{n-1} + 2n^2 a_{n-1} = 0$

ضریب متغیر



PAPCO

Subject:
Year. Month. Date. ( )

اگر nonlinear باشد سعی می‌کنیم به linear تبدیل کنیم

linear Recurrence of with constant coefficiante.

$$c_n a_n + c_{n-1} a_{n-1} + \dots + c_{n-k} \, a_{n-k} = f(n)$$

$$c_i \in \mathbb{R}$$

order : k یعنی جمله nام با k تای قبلی در ارتباط است

$f(n) = 0$ homogenous.

$f(n) \neq 0$ nonhomogenous.

- If a_n and b_n are two solutions to a homogenous linear recurrence, then $c a_n + d b_n$, where $b, d \in \mathbb{R}$, is also a solution to the same. ⟵ ترکیب خطی‌شان جواب دارد

اگر جواب‌ها چندجمله‌ای باشند مثلاً 1، n، n^2 به صورت خطی مستقل هستند

یک معادله Homogenous مرتبه k با داشتن k جواب مستقل می‌توانیم همه‌ی جواب‌ها را به دست بیاوریم

چون ترکیب خطی آنها جواب می‌شود

- The dimension of the space of solution to a linear homogenous equation of order k is k.

Homogenous recurrence

$$c_n a_n + c_{n-1} a_{n-1} + \dots + c_{n-k} a_{n-k} = 0$$

Assume $a_n = x^n$ is a solution to the above equation.

$a_n = 0$ جواب بدیهی homogenous است

$$c_n x^n + c_{n-1} x^{n-1} + \dots + c_{n-k} x^{n-k} = 0$$

همه‌ی صفر بودن جواب‌ها باعث از دست رفتن مستقل بودن می‌شود پس صفر جزو جواب‌ها نیست

PAPCO

Subject:
Year. Month. Date. ( )

$$x^{n-k}\left(c_0 x^k + c_1 x^{k-1} + \dots + c_{n-k}\right) = 0 \Rightarrow$$

$$c_0 x^k + c_1 x^{k-1} + \dots + c_{n-k} = 0$$

اگر ریشه‌ها متمایز باشند جواب‌ها قطعاً مستقل است

characteristic equation

has exactly k solution in C قطعاً

$a_n = x^n$ معادله‌ی بالا [illegible]

فرم عمومی جواب پیدا می‌شود

Example) Solve $F_n = F_{n-1} + F_{n-2}$ where $n \geq 2$, $F_0 = 0$, $F_1 = 1$.

$$F_n - F_{n-1} - F_{n-2} = 0$$ order: 2

$$x^2 - x - 1 = 0$$ پس از درجه 2 تبدیل می‌شود

$$x = \frac{1 \pm \sqrt{5}}{2}$$

$$F_n = C_1\left(\frac{1+\sqrt{5}}{2}\right)^n + C_2\left(\frac{1-\sqrt{5}}{2}\right)^n$$ C_1 و C_2 بسته به شرایط اولیه انتخاب می‌شود

$$F_0 = C_1 + C_2 = 0 \Rightarrow C_1 = -C_2$$

$$F_1 = C_1\left(\frac{1+\sqrt{5}}{2}\right) + C_2\left(\frac{1-\sqrt{5}}{2}\right) = 1$$

$$C_1\left(\frac{1+\sqrt{5}}{2}\right) - C_1\left(\frac{1-\sqrt{5}}{2}\right) = 1 \Rightarrow C_1 = \frac{1}{\sqrt{5}}, \quad C_2 = -\frac{1}{\sqrt{5}} \Rightarrow$$

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$ $\frac{1+\sqrt{5}}{2} = \varnothing$ golden ration

$$\Rightarrow F_n = \frac{1}{\sqrt{5}}\left(\varnothing^n - (-\varnothing)^{-n}\right)$$

PAPCO

Subject:

Year. Month. Date. ( )

Example) For $b \in \mathbb{R}^+$, consider the $n \times n$ determinant D_n given by

$$\begin{vmatrix} b & b & 0 & 0 & \cdots & 0 & 0 \\ b & b & b & 0 & \cdots & 0 & 0 \\ 0 & b & b & b & \cdots & 0 & 0 \\ 0 & 0 & b & b & \cdots & 0 & 0 \\ \vdots & & & & & & \\ 0 & 0 & 0 & 0 & \cdots & b & b \\ 0 & 0 & 0 & 0 & \cdots & b & b \end{vmatrix}$$

Find the value of D_n as a function of n.

$$D_n = bD_{n-1} - b \begin{vmatrix} b & 0 & 0 & \cdots & 0 \\ b & b & b & \cdots & 0 \\ 0 & b & b & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & b \end{vmatrix}$$

$$= bD_{n-1} - b(bD_{n-2}) = bD_{n-1} - b^2 D_{n-2}$$

$$D_n - bD_{n-1} - b^2 D_{n-2} = 0 \qquad D_1 = |b| = b \qquad D_2 = \begin{vmatrix} b & b \\ b & b \end{vmatrix} = 0$$

$$x^2 - bx + b^2 = 0 \Rightarrow x = \frac{b \pm \sqrt{-3b^2}}{2} = b\left(\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right)$$

$$D_n = c_1 b^n \left(\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^n + c_2 b^n \left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right)$$

$$D_n = c_1 b^n \left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right)^n + c_2 b^n \left(\cos\frac{\pi}{3} - i\sin\frac{\pi}{3}\right)^n$$

$$= c_1 b^n \left(\cos\frac{n\pi}{3} + i\sin\frac{n\pi}{3}\right) + c_2 b^n \left(\cos\frac{n\pi}{3} - i\sin\frac{n\pi}{3}\right)$$

$$= b^n \left(\underbrace{(c_1 + c_2)}_{k_1}\cos\frac{n\pi}{3} + i\underbrace{(c_1 - c_2)}_{k_2}\sin\frac{n\pi}{3}\right)$$

$$D_1 = b\left(k_1\frac{1}{2} + ik_2\frac{\sqrt{3}}{2}\right) = b$$

$$D_2 = b^2\left(k_1\frac{1}{2} + ik_2\frac{\sqrt{3}}{2}\right) = 0 \Rightarrow k_2 = \frac{1}{i\sqrt{3}} = \frac{-i}{\sqrt{3}} \Rightarrow k_1 = 1 \Rightarrow$$

PAPCO

$$D_n = b^n\left(\cos\frac{n\pi}{3} + \frac{1}{\sqrt{3}}\sin\frac{n\pi}{3}\right)$$

Subject:

Year. Month. Date. ( )

Repeated Root.

Example: Solve $a_n - 2a_{n-1} + a_{n-2} = 0$, where $a_0 = 1, a_1 = 2$

$x^2 - 2x + 1 = 0 \Rightarrow (x-1)^2 = 0 \Rightarrow x = 1, 1$

$a_n = c_1 1^n + c_2 1^n = c_1 + c_2$

$a_0 = c_1 + c_2 = 1$

$a_1 = c_1 + c_2 \cdot 2$ $\Rightarrow$ حل شود دستگاه معادلات

$a_n = c_1 1^n + c_2 n 1^n = c_1 + c_2 n$

$a_0 = 1 = c_1$

$a_1 = c_1 + c_2 \Rightarrow c_2 = 1$

$\Rightarrow a_n = 1 + n$

(I) $(n+1) - 2(n-1+1) + (1 + (n-2)) = 0 \Rightarrow$ صحت رابطه

Example: Assume the characteristic of $c_n a_n + c_{n-1} a_{n-1} + \dots + c_{n-k} a_{n-k} = 0$ has the root r of multiplicity of 2. Then nr^n is a solution to the recurrence.

$(x-1)^2 (x-4)^3 = 0$

$c_1 = 1^n \quad c_2 = n1^n$

$c_3 = 4^n \quad c_4 = 4^n n \quad c_5 = 4^n n^2$

Subject:

Year. Month. Date. ( )

Nonhomogeneous Recurrence

$$C_n a_n + C_{n-1} a_{n-1} + \dots + C_{n-k} a_{n-k} = f(n) \neq 0$$

1- Solve $C_n a_n + C_{n-1} a_{n-1} + \dots + C_{n-k} a_{n-k} = 0$ which yeild $a_n^{(h)}$.

2- find a particular solution $a_n^{(p)}$ to the nonhomogeneous equation

3- $a_n = a_n^{(h)} + a_n^{(p)}$ is the general solution to the nonhomogeneous equation.

Example) $a_n - 3a_{n-1} = 5(7^n)$, where $n \geq 1$ and $a_0 = 1$

$$a_n - 3a_{n-1} = 0 \Rightarrow a_n^{(h)} = C3^n$$

$$a_n^{(p)} = A7^n \Rightarrow A7^n - 3(A7^{n-1}) = 5 \times 7^n$$

$$4A(7^{n-1}) = 5 \times 7^n \Rightarrow A = \frac{35}{4}$$

$$a_n^{(p)} = \frac{35}{4} 7^n = \frac{5}{4} 7^{n+1}$$

$$a_n = C a_n^{(h)} + a_n^{(p)} = C3^n + \frac{5}{4}(7^{n+1})$$

$$a_0 = 1 \Rightarrow C = \frac{-31}{4}$$

$$\Rightarrow a_n = \frac{-31}{4}(3^n) + \frac{5}{4}(7^{n+1})$$

Subject:

Year. Month. Date. ( )

Example) Solve $a_n - 3a_{n-1} = 5(3^n)$, where $n \geq 1$, $a_0 = 1$

$a_n^{(h)} = C3^n$

$a_n^{(p)} = A3^n \Rightarrow A3^n - 3A3^{n-1} = (5)3^n$

$0 \neq 5(3^n)$

$A_n^{(p)} = An3^n \Rightarrow An3^n - 3(A(n-1)3^{n-1}) = 5(3^n) \Rightarrow A = 5$

$a_n = C3^n + 5n3^n$

$a_0 = 1 \Rightarrow C = 1$

$\Rightarrow a_n = 3^n + 5n3^n = (1+5n)3^n$

اگر $P(n)$ چنین جمله‌ای باشد، $a_n^{(p)}$ را چه در نظر می‌گیریم؟

$P(n)$	$a_n^{(p)}$
ثابت c	d
n (چندجمله‌ای درجه یک بدون ثابت)	$An + A_0$
n^2	$An^2 + A_1n + A_0$
n^t	$An^t + \cdots + A_1n + A_0$
r^n	Ar^n
$r^n n^t$	$r^n(An^t + A_{t-1}n^{t-1} + \cdots + A_1t + A_0)$
$\cos\alpha n$, $\sin\alpha n$	$A\sin\alpha n + B\cos\alpha n$
$r^n\cos\alpha n$, $r^n\sin\alpha n$	$r^n(A\sin\alpha n + B\cos\alpha n)$

Subject:

Year. Month. Date. ( )

Example) Solve $a_n^2 a_{n-1} = 1$ where $n \geq 1$ and $a_0 = 2$

$$2\log_2^{a_n} + \log_2^{a_{n-1}} = 0 \quad \Rightarrow \quad 2t_n + t_{n-1} = 0 \; ; \; t_0 = 1$$

t_n

$$t_n = c(-\tfrac{1}{2})^n \Rightarrow c = 1$$

$$t_n = (-\tfrac{1}{2})^n$$

$$a_n = 2^{t_n} \Rightarrow a_n = 2^{(-\frac{1}{2})^n}$$

Example) Find the number of ways in which can arrange a row of +'s and −'s where no consecutive $\vec{Y}$+'s appear in it.

$a_n = ?$

$+ \underbrace{- \cdots -}_{a_{n-2}}$

$\Rightarrow a_n = a_{n-1} + a_{n-2} \; ; \quad a_0 = 1$

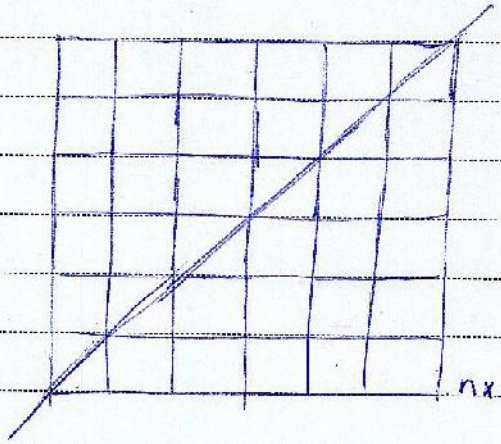
$a_1 = 2$

$\underbrace{- \cdots -}_{a_{n-1}}$

Subject:

Year. Month. Date. ( )

Example)



می‌خواهیم تعداد مربع‌های طرح n‌ام را بدست آوریم

$a_n = ?$

$a_n = a_{n-1} + (n-1)a_{n-2}$; $a_0 = 1$, $a_1 = 1$

$a_2 = a_1 + 1a_0 = 2$

$a_3 = a_2 + 2a_1$

$a_3 = 2 + 2(1) = 4$