$sa + tm \equiv 1 \pmod 7$

$t \cdot 7 \equiv 0 \bmod (7)$

$s \cdot a = 1$

$= (-2) \cdot 3 = 1 \bmod (7)$

so inverse (-2) of 3.

—o—

$3x \equiv 4 \pmod 7$ — ①

$(-2)\, 3x \equiv (-2)\, 4 \pmod 7$

$= 6x = (-8) \bmod (7)$ [as $(-2)\,3 \equiv 1 \bmod 7$]

$x \equiv (-8)$

$-8 \equiv 6 \pmod 7$

[as $-8 = 7(-2) + 6$]

so, $x = 6$

① $\Rightarrow 18 \equiv 4 \pmod 7$

$x = 6$

$= 13, 20$ ... $(6+7 = 13,)$

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

~~Proof~~

$m_1, m_2, \ldots m_n \longrightarrow RP$

$x \equiv a_1 \pmod{m_1}$; $x \equiv a_2 \pmod{m_2}$

$x \equiv a_1 \pmod{m_1}$; $x \equiv a_2 \pmod{m_2}$

$x \equiv a_n \pmod{m_n}$

$m = m_1 m_2 \cdots m_n \rightarrow 0 \leq x < m$

$M_k = \frac{m}{m_k} \longrightarrow \gcd(m_k, M_k) = 1$

y_k is the inverse M_k module

i.e. $M_k y_k = 1 \pmod{m_k}$

$x = a_1 m_1 y_1 + a_2 m_2 y_2 + a_n m_n y_n$

$m = 3 \cdot 5 \cdot 7 = 105$ $\quad x = a_k M_k y_k$

$= a_k \pmod{m_k}$

$M_1 = \frac{105}{3} = 35$

$M_2 = \frac{105}{5} = 21$

$M_3 = \frac{105}{7} = 15$ $\quad x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 + 3 \cdot 15 \cdot 1$

y_1 inverse of $(35, 3)$

$y_1 = 2$

$y_2 = 1$, $y_3 = 1$

10 cycle C Day

PKC

RSA

Matrices

Mathematical Reasoning

* Rules of Inference

$$\begin{array}{l} p \\ \underline{p \to q} \\ \therefore q \end{array}$$

tautology

$(p \wedge (p \to q)) \to q$

Modus Ponens

Rule of Inf	Tautology	Name
$\dfrac{p}{\therefore p \vee q}$	$p \to (p \vee q)$	Addition
$\dfrac{p \wedge q}{\therefore p}$	$(p \wedge q) \to p$	Simplification

$* [$ … $/3$ the $n^2/9$

$x =$

$= 13,$

$\wedge (p \to q)] \to \neg p$ Modus tollens

* It is not sunny this afternoon & it is colder than yesterday
* We will go swimming only if it is suny
* If we do not go swimming then we will take a cane trip
* If we take a canoe trip, then we will be home by sunset
* We will be home by sunset

Step	Reason
1. $\neg p \wedge q$	Hypothesis
2. $\neg p$	Simplification (Rule 2)
3. $r \to p$	Hypo
4. $\neg r$	
5. $\neg r \to s$	
6. s	

Vacuous $F \to F$, $F \to T$

Trival $T \to T$, $F \to T$

Fallacies

RoI for Quantified Stat.

DIRECT Proof $P \to q$

Proof: Contrapositive

$\forall$ $\exists$

II cycle B Day

1) Universal Instantiation

$$\frac{\forall x\ P(x)}{P(c) \text{ if } c \in U}$$

ii) $P(c)$ for an arbitrary $c \in U$
$\therefore \forall x\ P(x)$ → Univ. Generalizati

iii) $\exists x\ P(x)$
$\therefore P(c)$ for some element $c \in U$ → Univ insta

iv) $P(c)$ for some element $c \in U$
$\therefore \exists x\ P(x)$

$\sqrt{2}$ is irrational

Proof by contradiction.

3.2 Mathematical Induction

1. Basis Step: $P(1)$
2. Inductive step: $P(n) \rightarrow P(n+1)$

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

$1+3 = 4 = 2^2$

$1+3+5+ \cdots + (2n-1) + \{2(n+1)-1\}$

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

nth position $\quad$ (n+1)th posi

$$1+3+5+ \cdots + \underbrace{(2n-1)}_{[n]} + \underbrace{(2n+1)}_{(n+1)} = (n+1)^2$$

1. Basis Step: $P(1)$

$P(1) \rightarrow 1 = 1^2$

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

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

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

11 cycle C Day

Mathematical Induction

* Basis step $\Rightarrow$ P(1) $\to$ true

Inductive n $\Rightarrow$ $[P(n) \to P(n+1)]$ true for $\forall n$

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

Ex. $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$

Basis step:

$\boxed{n=0}$ $2^{0+1} - 1 = 2^1 - 1 = 2 - 1 = 1$

Inductive step:

$1 + 2 + 2^2 + \cdots + 2^n + 2^{n+1} = 2^{n+1+1}$

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

$= 2^{(n+1)}\{1 + 1\} - 1 = 2^{n+1} \cdot 2 - 1$

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

Ex:

$$\sum_{i=0}^{n} = a + ar + ar^2 + \cdots + ar^n = \frac{ar^{n+1} - a}{r-1}$$

when $r \neq 1$

Basis step: $P(0)$

$$a = \left(\frac{ar - a}{r - 1}\right) = \frac{2a - a}{2 - 1} = a$$

Inductive step:

$$RHS = \frac{ar^{n+2} - a}{r-1}$$

$$LHS = \underbrace{a + ar + ar^2 + \cdots + ar^n}_{} + ar^{n+1}$$

$$\frac{ar^{n+1} - a}{r-1} + ar^{n+1}$$

$$= \frac{ar^{n+1} - a + ar^{n+2} - ar^{n+1}}{r-1}$$

$$= \frac{ar^{n+2} - a}{r-1}$$

3.3 Recursive Definition

Ex: $f(0) = 3$ $\quad f(1) = ?$

$f(n+1) = 2f(n) + 3 \quad f(2) = ?$

$f(0+1) = 2f(0) + 3$

$f(1+1) = 2f(1) + 3$

$f(2+1) = 2f(2) + 3$

12cycle B Day

* Seq. Search Alg.

Procedure search (i, j, x)
if $a_i = x$, then loc $:= i$
else if $i = j$ then loc $:= 0$
else search $(i+1, j, x)$

— o —

factorial (n (+ve) int)
if n = 1 then
fac (n) = 1

else,
fac (n) :=
n * factorial (n − 1)

iterative fact (n : (+ve) int)
x = 1
for i = 1 to n
x = i * x
{x is n!}

Chaptr Self study Imp.

3.5 Program Correctness

$p\{s\}q \longrightarrow$ Hoare triple

Ex, $y=2,\ z=x+y$

$p: x=1,\quad q: z=3$

Rules of Inference

$$\frac{\begin{matrix} p\{s_1\}q \\ q\{s_2\}r \end{matrix}}{p\{s_1, s_2\}r}$$

Self study

Lect. missin'

13 B

Transitive Rel^n

Relation R/ Set A

transitive $(a, b) \in R$

& $(b, c) \in R$

then $(a, c) \in R$ for $(a, b, c) \in A$

$R_1 = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$

Transitive

$R_4 = \{(2,1), (3,1), (3,2), (4,1), (4,2), (4,3)\}$

Non

$R_6 = \{(3,4)\}$ Trasitive

Divides Rel^n

$(a, b) \in R$

$(b, c) \in R$

$(a, c) \in R$

$\left.\begin{matrix} a/b \\ b/c \end{matrix}\right\} \rightarrow a/c$

$b = ak$

$c = bl$

$= akl$

$a/c/kl$

Combining Rel^{n}s

$A = \{(1,2,3)\}$ $B = \{1,2,3,4\}$

$R_1 = \{(1,1), (2,2), (3,3)\}$

$R_2 = \{(1,1), (1,2), (1,3), (1,4)\}$

$R_1 \cup R_2 =$

$R_1 \cap R_2 =$

$R_1 - R_2 =$

$R_2 - R_1 =$

Composite Rel^n:

$R : A \to B$

$S : B \to C$

$S \circ R$: Ordered pairs (a, c) where $a \in A$ & $c \in C$

$\exists$ $b \in B$ such that $(a, b) \in R$

Ex: R: $\{1, 2, 3\}$ to $\{1, 2, 3, 4\}$

S: $\{1, 2, 3, 4\}$ to $\{0, 1, 2\}$

$R = \{(1,1), (1,4), 2,3), (3,1), (3,4)\}$

$S = \{(1,0), (2,0), (3,1), (3,2), (4,1)\}$

$S \circ R = \{ 1,0), (1,1), (2,1), (2,2), (3,0), (3,$

$R = \{(\overset{\text{1st}}{\downarrow} \; , \; \overset{\text{2nd}}{\downarrow})\}$

$S = \{(\overset{\text{1st}}{\downarrow} \; , \; \overset{\text{2nd}}{\downarrow})\}$

New $S \circ R = \{$ (common of 2nd of R & 1st of S), (& S 2nd

R: set A

R^n, $n = 1, 2, 3 \cdot$

$R^1 = R$ & $R^{n+1} = R^n \circ R$

Ex) $R = \{(1,1), (2,1), (3,2), (4,3)\}$

$R = \{(1,1), (2,1), (3,2)$ $\therefore R = \{(1,1), (2,1), (3,1)\}$

$R^2 = ?$

Ex 2 R on set A $\Rightarrow$ transitive
if $R^n \subseteq R$ for $n = 1, 2, 3 \ldots$

Mathematical induction:

$n = 1 \longrightarrow$ OK

Assume, $R^n \subseteq R$

Now Prove, for R^{n+1} from Assumption

Ans: Assume $(a, b) \in R^{n+1}$

Since $R^{n+1} = R^n \circ R$

$x \in A$ such that

$(a, x) \in R$ & $(x, b) \in R^n$

then $R^n \subseteq R$

Since $R \rightarrow$ transitive

$(a, x), (x, b) \in R$ then $(a, b) \in R$

$\overline{III}$ layers

n Ary Relations & their App & degree $\to n$

$A_1, A_2, \ldots A_n \to$ sets (domains)

$A_1 \times A_2 \ldots \times A_n$

Ex: R : (a, b, c) with $a < b < c$

then, $(1, 2, 3) \in R$ $\boxed{\text{deg : 3}}$

(A, N, ~~B~~ S, D, T)

* Primary Key
* Composite Key

6.2 chapter Self study

C.T - ch.3 ch 4