-Gaurav Chaulagain
-Discrete Structure

Page
Date

'Model Question'

1. Why breaking down of large integer into set of small integers is preferred while performing integer arithmetic? find sum of numbers 123,684 and 413456 by representing the numbers as 4-tuple by using reminders modulo of pair-wise relatively prime number less than 100.

→ Breaking down of large integer into set of small integers is preferred while performing integer arithmetic because:

i) it can be used to perform arithmetic with integers larger than can ordinally carried out on a computer.

ii) computations with respect to the different modulii can be done in parallel, speeding up the arithmetic.

Solution:

Given two numbers: 123,684 and 413,456

Here we can use the modulii of 99, 98, 97 and 95.

so, we represent two given numbers as:

123684 (mod 99) = 33	413456 (mod 99) = 32
123684 (mod 98) = 8	413456 (mod 98) = 92
123684 (mod 97) = 9	413456 (mod 97) = 42
123684 (mod 95) = 89	413456 (mod 95) = 16
⇒ (33, 8, 9, 89)	⇒ (32, 92, 42, 16)

Adding the corresponding 4-tuples, we get new 4-tuple as:

(33, 8, 9, 89) + (32, 92, 42, 16)

$= (65 \text{ mod } 99, 100 \text{ mod } 98, 51 \text{ mod } 97, 105 \text{ mod } 95)$

$= (65, 2, 51, 10)$

To find the sum, i.e. the integer represented by (65, 2, 51, 10) we need to solve the system of congruences,

$x \equiv 65 \pmod{99}$

$x \equiv 2 \pmod{98}$

$x \equiv 51 \pmod{97}$

$x \equiv 10 \pmod{95}$

Since, 99, 98, 97 and 95 are pairwise relatively prime, the chinese remainder theorem,

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4 \pmod{M} \quad \text{---(i)}$$

Here,

$a_1 = 65$, $m_1 = 99$

$a_2 = 2$, $m_2 = 98$

$a_3 = 51$, $m_3 = 97$

$a_4 = 10$, $m_4 = 95$

$\therefore M = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 89403930$

$M_1 = \frac{M}{m_1} = 903070$, $M_2 = \frac{M}{m_2} = 912285$, $M_3 = \frac{M}{m_3} = 921690$

$M_4 = \frac{M}{m_4} = 941094$

Page
Date

Also,

$y_1 \equiv M_1^{-1} \pmod{m_1}$

$y_2 \equiv M_2^{-1} \pmod{m_2}$

$y_3 \equiv M_3^{-1} \pmod{m_3}$

$y_4 \equiv M_4^{-1} \pmod{m_4}$

Solving for y_1,

$y_1 \equiv M_1^{-1} \pmod{m_1}$

or $M_1 y_1 \equiv 1 \pmod{m_1}$

or $903070\, y_1 \equiv 1 \pmod{99}$

or $91 y_1 \equiv 1 \pmod{99}$

Using modular theorem,

$91 y_1 - 99 t_1 = 1$ — (ii).

Using euclidean theorem,

$\gcd(91, 99) = 1$

$99 = 1 \times 91 + 8$

$91 = 11 \times 8 + 3$

$8 = 2 \times 3 + 2$

$3 = 1 \times 2 + 1$

Using back substitution,

$1 = 3 - 1 \times 2$

$1 = 3 \times 3 - 1 \times 8$.

$1 = 3 \times 91 - 34 \times 8$

$1 = 37 \times 91 - 34 \times 99$

Comparing with eq^n (ii), we get,

$y_1 = 37 \pmod{99}$

Page
Date

solving for y_2,

$y_2 \equiv M_2^{-1} \pmod{m_2}$

or $M_2 y_2 \equiv 1 \pmod{m_2}$

or, $912285\, y_2 \equiv 1 \pmod{98}$

or $3y_2 \equiv 1 \pmod{98}$

or $3 \times 33 y_2 \equiv 33 \pmod{98}$

or $y_2 \equiv 33 \pmod{98}$.

solving for y_3:

$y_3 \equiv M_3^{-1} \pmod{m_3}$

or, $921690\, y_3 \equiv 1 \pmod{97}$

or, $93 y_3 \equiv 1 \pmod{97}$

using modular arithmetic,

$93y_3 - 91t_2 = 1$ —— (iii)

using Eucledean theorem; gcd (97, 93).

$97 = 1 \times 93 + 4$

$93 = 23 \times 4 + 1$

using backword substitution,

$1 = 93 - 23 \times 4$

$1 = 24 \times 93 - 23 \times 97$.

Comparing with eq^n (iii),

$y_3 \equiv 24 \pmod{97}$.

solving for y_4,

$y_4 \equiv M_4^{-1} \pmod{m_4}$

or $M_4 y_4 \equiv 1 \pmod{m_4}$

=)

or $941094 y_4 \equiv 1 \pmod{95}$

or $24 y_4 \equiv 1 \pmod{95}$

or $24 \times 4 y_4 \equiv 1 \pmod{95}$

or $y_4 \equiv 4 \pmod{95}$.

$\therefore$ Then,

$a = a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4 \pmod{M}$

$= 3397886480 \pmod{89403930}$

$= 537,140 \pmod{89403930}$

So, 537,140 is the unique solution of the system less than 89403930. Consequtively, 537140 is the sum of given numbers.

5. How zero-one matrix and diagraphs can be used to represent a relation? Explain the process of identifying whether the graph is reflective, symmetric or anti-symmetric by using matrix or diagraph with suitable example.

→

zero-one matrix respresentation:

The relation with finite sets can be represented using the matrix. let A be a set $(a_1, a_2, \dots, a_n)$ and B be the set $(b_1, b_2, \dots, b_n)$, where elements are listed in some arbitrary order, we represent relation from A to B by matrix

$$M_R = [m_{ij}]$$

where,

$$m_{ij} = \begin{cases} 1 & \text{if } (a_i, b_j) \in R \\ 0 & \text{if } (a_i, b_j) \notin R \end{cases}$$

example:

Represent the relation $\{(1,1), (1,2), (1,3), (2,2), (2,3), (3,2), (3,3)\}$ using zero matrix.

i.e

$$M_R = \begin{array}{c c} & \begin{array}{ccc} 1 & 2 & 3 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \end{array}$$

Identifying properties using zero-one matrix

a) Reflexive:

If all the diagonal elements are 1 i.e all $m_{ij} = 1$ whenever $i=j$, then the relation represented by the matrix is reflexive.

b) Symmetric:

If $m_{ij} = 1$ in the matrix then $m_{ij} = 1$ must be true and if $m_{ij} = 0$ then $m_{ji} = 0$ is also true. It means that the relation represented by matrix is symmetric if and only if the matrix is equal to the transpose.

c) Antisymmetric:

If $m_{ij} = 1$ and $i \neq j$, then $m_{ij} = 0$ or in other words either $m_{ij} = 0$ or $m_{ji} = 0$ when $i \neq j$.

Diagraphs representation:

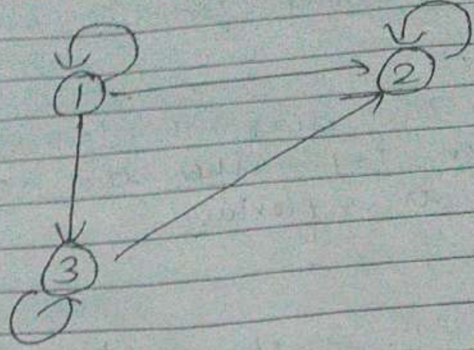
A diagraph is a set of vertices V together with the set of edges. Then vertex a is called initial vertex of the edge (a, b), and the vertex b is called the terminal vertex of this edge.

example: Draw the directed graph for the relation given in above example (i.e in zero-one matrix representation).

{(1,1), (1,2), (1,3), (2,2), (2,3), (3,2), (3,3)}

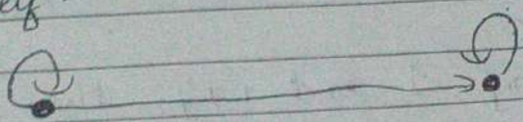
Page
Date

Ayᵐ·

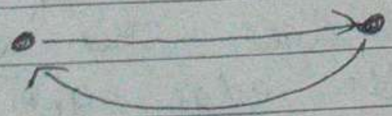


Identifying properties using Diagraphs:

a) Reflexive:
If every vertex has edge from the vertex to itself.



b) Refl Symmetric:
If for every edge of one direction there is two vertices as of first edge.



c) Anti-symmetric:
If no two distinct vertices have an edge going in both directions

Page
Date

4. Prove that $\overline{A \cap B} = \overline{A} \cup \overline{B}$ by using set builder notation. How sets are represented by using bit string? Why is it preferred over unordered representation of sets?

→

To prove: $\overline{A \cap B} = \overline{A} \cup \overline{B}$

$\overline{A \cap B} = \{x \mid x \in (\overline{A \cap B})\}$
$= \{x \mid x \notin (A \cap B)\}$ [∵ By negation sign law]
$= \{x \mid x \notin A \cup x \notin B\}$ [∵ By negation law].
$= \{x \mid x \in \overline{A} \cup x \in \overline{B}\}$ [By complement law].
$= \{x \mid x \in (\overline{A} \cup \overline{B})\}$ [By union law].
$= \overline{A} \cup \overline{B}$

proved//

There are various ways to represent sets using a computer. One method is to store the elements of the set in an unordered fashion. However, if this is done, the operation of computing the union, intersection or difference between two sets would be time-consuming, because each of these operation would require large amount of time for searching elements.

For representing sets by using bit string,

Assume that universal set U is finite (and of reasonable size so that the number of elements of U is not larger than the memory size of the computer being used). First specify an arbitrary ordering of the elements of U, for instance $a_1, a_2, \ldots, a_n$. Represent a subset A of U with the bit string of length n, where the ith bit of the string is 1 if a_i belongs to A and 0 if a_i does not belong to A.

→ example.

Let U = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10}.

The bit string that represents the set of odd integers in U, namely {1, 3, 5, 7, 9} can be represented as

1 0 1 0 1 0 1 0 1 0.

5. How can you relate domain and co-domain of functions in programming language? Discuss composite and inverse of function with suitable examples.

→

In programming language, the domain and codomain of function are often specified.
For instance, the C++ statement,

int function (float x) {...}.

and
the Java statement,

int floor (float real) {....}

both tells us that the domain of the floor function is the set of real numbers (represented by floating point numbers) and its codomain is the set of integers.

Page
Date

Inverse of function:

Let f be one-to-one correspondence from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a)=b$. The inverse function of f is denoted by f^{-1}. Hence, $f^{-1}(b)=a$ when $f(a)=b$.

example:

$f(x) = x+1$;

Since, it is a bijective function,

let $y = x+1$

interchanging 'x' and 'y'

$x = y+1$

$\Rightarrow y = x-1$.

i.e $f^{-1}(x) = x-1$.

Composite of function:

Let g be a function from the set A to the set B and let f be a function from the set B to the set C. The composition of the function f and g, denoted for all $a \in A$ by $f \circ g$, is defined by

$$(f \circ g)\, a = f(g(a)).$$

for example,

$f(x) = 2x+1$, $g(x) = 4x$.

Then,

$$(f \circ g)\, x = f(g(x)) = f(4x) = 2 \times 4x + 1 = 8x+1$$

Page
Date

6. State Euclidean and Extended Euclidean theorem. Write down extended Euclidean algorithm and illustrate it with example.

→

Euclidean Theorem:-

It is used to find the Greatest Common Divisor of two integers. This algorithm is used to find GCD of two integers uses successive division to reduce the problem of finding the gcd to the same problem with smaller integers until one of integer is 0.

i.e.

It is based on following rule,

Let $a = qb + r$, where a, b, q and r are integers.

then $gcd(a,b) = gcd(b, r)$.

Extended Euclidean ~~algorith~~ Theorem:

It is an extension of euclidean algorithm that can express gcd of a,b as a linear combination with integer coeff of a and b i.e.

Using extended Euclidean algorithm, we can express gcd of a and b in the form of

$gcd(a,b) = sa + tb$

where, s and t are integers.

example. GCD of (252, 198)

using Euclidean theorem,

$252 = 1 \times 198 + 54$

$198 = 3 \times 54 + 36$

$54 = 1 \times 36 + 18$
$36 = 2 \times 18 + 0$.

Hence,
$gcd(252, 198) = 18$

Using extended euclidean theorem,

$$18 = 54 - 1 \times 36$$
$$= 54 - 1 \times (198 - 3 \times 54)$$
$$= 54 - 198 + 3 \times 54$$
$$= 4 \times 54 - 198$$
$$= 4 \times (252 - 1 \times 198) - 198$$
$$= 4 \times 252 - 4 \times 198 - 198$$
$$= 4 \times 252 - 5 \times 198.$$

i.e. $18 = 252t + 198s$
where, $t = 4$ & $s = -5$.

Hence, the illustration of extended euclidean theorem is performed.

---

7. State and prove generalized pigeonhole principle? How many cards should be selected from a deck of 52 cards to guarentee at least three cards of same suit?

→

statement:

If N objects are placed into k boxes, then there is at least one box containing at least $\lceil \frac{N}{k} \rceil$ objec proof:

we will use proof by contraposition.

suppose that none of the boxes contains more than $\lceil \frac{N}{k} \rceil - 1$ objects. Then, the total number of objects is at most,

$$k\left(\left\lceil \frac{N}{k} \right\rceil - 1\right) < k\left(\left(\frac{N}{k}+1\right)-1\right) = N$$

where the inequality $\lceil N/k \rceil < (N/k)+1$ has been used. This is a contradiction because there are total of N objects.

solution:

Given,

There are 4 boxes from which same suit card can be selected. That is 52 cards is divided into 4 boxes.

Then,

pegionholes $(n) = 4$

Also, $k+1 = 3$

i.e $k = 2$

pegions $(m) = ?$

we have,

By Pegionhole theorem,

$m = nk + 1$

$= 4 \times 2 + 1$

$\therefore m = 9$

Hence, 9 cards can be selected from a deck of 52 cards to guarentee that at least three cards are of same suit.

Page
Date

Represent the argument "If it does not rain or if it is not foggy then the sailing race will be held and the lifesaving demonstration will go on. If sailing race is held then trophy will be awarded. The trophy was not awarded. Therefore, it rained" in propositional logic and prove the conclusion by using rule of inferences.

Let,

$p \rightarrow$ It rains

$q \rightarrow$ It is foggy

$r \rightarrow$ The sailing race will be held

$s \rightarrow$ lifesaving demonstration will go on.

$t \rightarrow$ Trophy will be awarded.

expressions: $(\sim p \vee \sim q) \rightarrow (r \wedge s)$, $r \rightarrow t$, $\sim t$

conclusion: p

Assertion	Reason
i) $\sim t$	Hypothesis
ii) $r \rightarrow t$	Hypotheses
iii) $\sim r$	modus tollens of (i) & (ii)
iv) $\sim r \vee \sim s$	Addition from (iii)
v) $(\sim p \vee \sim q) \rightarrow (r \wedge s)$	Hypothesis
vi) $\sim (r \wedge s)$	logically equivalent to (iv)
vii) $\sim (\sim p \vee \sim q)$	Modus tollens from (v) and (vi)
viii) $p \wedge q$	logically equivalent to (vii)
ix) p	simplification of (viii).

prov

9. Discuss common mistakes in proof briefly. Show that n is even if n^3+5 is odd by using indirect proof.

→ There are many common errors made in constructing mathematical proofs. We will briefly describe some of these here. Among the most common errors are mistakes in arithmetic and basic algebra. Even professional mathematicians make such errors, especially when working with complicated formulae. Whenever you use such computations you should check them as carefully as possible.

Each step of mathematical proof needs to be correct and conclusions need to follow logically from the steps that precede it. Many mistakes result from the introduction of steps that do not logically follow from those that precede it.

for example;

step	Remark
1. $a=b$	Given
2. $a^2=ab$	Multiply both sides of (1) by a.
3. $a^2-b^2=ab-b^2$	Subtraction b^2 to both sides of (2)
4. $(a-b)(a+b)=b(a-b)$	Factor both sides of (3)
5. $a+b=b$	Divide both sides by $(a-b)$
6. $2b=b$	Replace a by (b) in (5)
7. $2=1$	Divide both sides of (6) by b.

using indirect proof,

⇒

suppose, n is odd. so we, $n = 2k+1$ for some integer k.

Then,

$$n^3+5 = (2k+1)^3+5$$
$$= (2k)^3 + 3\times 2k\times 1(2k+1) + (1)^3 + 5$$
$$= 8k^3 + 6k\times 2k + 6k + 6$$
$$= 8k^3 + 12k^2 + 6k + 6$$
$$= 2(4k^3 + 6k^2 + 3k + 3)$$
$$= 2M$$

where $M = (4k^3+6k^2+3k+3)$.

∴ if n^3+5 is even, n is odd.

Hence, by indirect proof, if n^3+5 is odd, n is even.

proved//

10. How mathematical induction differs from strong induction? Prove that $1^2+2^2+3^2+\dots+n^2 = n(n+1)(2n+1)/6$ by using strong induction.

→ In mathematical induction, if regular induction [P(n) is true) does not given enough information to prove that P(n+1) is true. for that, we have to use strong induction. With strong induction, we assume that P(1), P(2), ..., P(n) are true, so you have more information to prove the truth of P(n+1).

Solution:

⇒

Basic step:
Plugging in $n = 1$, we have that, $P(1)$ is the statement,
$$1^2 = 1 \cdot 2 \cdot 3 / 6$$
i.e. $1 = 1$.

Inductive step:
let us suppose $P(K)$ is true i.e.
$$1^2 + 2^2 + \cdots + K^2 = \frac{K(K+1)(2K+1)}{6}$$

Now we have show that $P(K)$ implies $P(K+1)$. i.e.
$$1^2 + 2^2 + \cdots + K^2 + (K+1)^2 = \frac{(K+1)(K+2)(2K+3)}{6}$$

Now,
$$L.H.S = 1^2 + 2^2 + \cdots + K^2 + (K+1)^2$$
$$= P(K) + (K+1)^2$$
$$= \frac{K(K+1)(2K+1)}{6} + (K+1)^2 \text{ [by inductive hypothesis]}$$
$$= \frac{K+1}{6}\left(K(2K+1) + 6(K+1)\right)$$
$$= \frac{K+1}{6}(2K^2 + 7K + 6)$$
$$= \frac{K+1}{6}(K+2)(2K+3)$$
$$= \frac{(K+1)(K+2)(2K+3)}{6}$$

we have completed the basis step and the inductive step. so, by the principle of mathematical induction, the statement is true for every positive integer, n.

11. Write down recursive algorithm for computing a^n. Argue that your algorithm is correct by using induction.

→ We can base a recursive algorithm on the recursive defination of a^n.

from this defination,

$$a^{n+1} = a \cdot a^n \quad \text{for } n>0$$

Then, initial condition, $a^0 = 1$.

To find a^n, successively use the recursive step to reduce the exponent until it becomes zero.

Algorithm for computing a^n:

```
procedure power (a, n)
  if n=0 then
     return 1
  else
     return a·power(a, n-1)
 [output is a^n]
```

Solution:

⇒

Basis step:

If $n=0$, the first step of the algorithm tells us that power $(a, 0) = 1$. This is correct because $a^0 = 1$ for every nonzero real number a.

Inductive step:

Let us suppose power $(a, k) = a^k$ is true for all $a \neq 0$ for non-negative integer k.

Now,

we have to show that power $(a, k+1) = a^{k+1}$ must also be true. i.e.

$$\text{power}(a, k+1) = a \cdot \text{power}(a, k)$$
$$= a \cdot a^k \text{ (from inductive hypothesis)}$$
$$= a^{k+1} \text{ (True)}$$

Since, Basis step and Inductive step is true, the algorithm is also true.

12. What is meant by chromatic number? How can you use graph coloring to schedule exams? Justify by using 10 subjects assuming that the pairs {(1,2), (1,5), (1,8), (2,4), (2,9), (2,7), (3,6), (3,7), (3,10), (4,8), (4,3), (4,10), (5,6), (5,7)} of subjects have common students.

→ The minimum no. of color required while Graph coloring is called chromatic number.

The scheduling program can be solved by using a graph model, with vertices representing courses and with an edge between two vertices if there is a common student in the courses they represent. Each time slot for a final exam is represented by different colour. A scheduling of the exams correspond to a coloring of the associated graph.

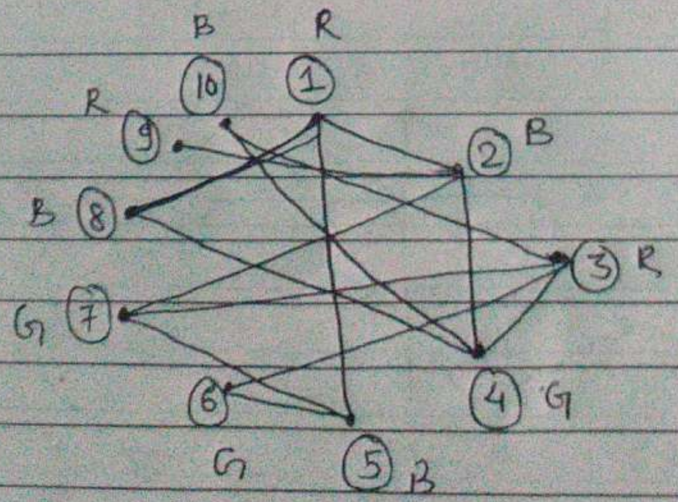
Suppose, there are 10 finals to be scheduled. Suppose that course are numbered through 1 to 10.

~~Suppose the~~

Given, the following pairs of courses have common students:

{ (1,2), (1,5), (1,8), (2,4), (2,9), (2,7), (3,6), (3,7), (3,10), (4,8), (4,3), (4,10), (5,6), (5,7)}

The following graph shows associated with the set of classes is shown.



From, graph coloring we found that three colors are to be used. Hence, 3 time slots are needed for examination.