Discrete Structure

(BT 12405)

S.Y. B. Tech. Semester IV (CSE)

by

Dr Anagha U. Khiste
Department of Applied Mathematics and Data Science
Indian Institute of Information Technology, Pune
Email: anaghakhiste@iiitp.ac.in

2022-2023

Discrete Structure

Number Theory

- It is a branch of mathematics that deals with the study of integers and its properties.
- It has various applications in discrete mathematics and computer science.
- It is used to assign memory location for computer files, to generate pseudorandom numbers. It is also used in both classical cryptography as well as modern cryptography (constructing check digits and encrypting messages).
- It has different subdivisions such as Elementary number theory, Algebraic number theory, Geometric number theory, Analytic number theory, transdental number theory, combinatorial number theory, etc.

anaghakhiste@iiitp.ac.in

Discrete Structure

Number Theory

- **Divisibility:** If a and b are integers with $a \neq 0$, we say that "a divides b" if there is an integer k such that b $= ak$ and we write $a|b$.
- $a|b$: "a divides b" or "a is a divisor of b" or "b is a multiple of b"
- $a \nmid$ b: "a does not divides b"
- We can express $a|b$ using quantifiers as $\exists k(ak = b)$, where the universe of discourse is the set of integers.

Theorem: Suppose a, b, c are integers, when $a \neq 0$. Then

i. If $a|b$, then $a|bc$

ii. If $a|b$ and $b|c$, then $a|c$

iii. If $a|b$ and $a|c$, then $a|(bx + cy)$ for any integers x and y

iv. If $a|b$ and $b|a$, then $a = \pm b$

v. If $a|b$ and $m \neq 0$, then $ma|mb$

anaghakhiste@iiitp.ac.in

Discrete Structure

Number Theory

- **The Division Algorithm:**
  Given any integers a and b with $a > 0$, then there exist unique integers q and r such that
  $$b = aq + r, \quad 0 \le r < a.$$
- If $a \nmid b$, then r satisfies stronger inequality, $0 < r < a$.
- Notations: $q = b$ **div** a & $r = b$ **mod** a

Ex.1. What are the quotient and remainder when -11 is divided by 3?
Solution: We have $-11 = 3(-4) + 1$.
Hence, the quotient when -11 is divided by 3 is $-4 = -11$ div 3, and the remainder is $1 = -11 \bmod 3$.
Note that the remainder cannot be negative. Consequently, the remainder is not -2, eventhough $-11 = 3(-3) - 2$, because $r = -2$ does not satisfy $0 \le r < 3$.

Discrete Structure

Primes

Prime: An integer $p > 1$ is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

Remark: The integer n is composite if and only if there exists an integer a such that $a \mid n$ and $1 < a < n$.

Theorem 1 (The Fundamental Theorem of Arithmetic):
Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size.

Ex. The prime factorizations of 641 and 100 are given by

$$641 = 641 \quad \& \quad 100 = 2 \times 2 \times 5 \times 5 = 2^2 5^2 .$$

anaghakhiste@iiitp.ac.in

Discrete Structure

Primes

Theorem 2: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Ex. Show that 101 is prime.

Solution: The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7, it follows that 101 is prime.

Theorem 3: There are infinitely many primes.

Discrete Structure

GCD

- **Greatest Common Divisor (GCD):**

Let a and b be any integers not both zero. Then the non-zero integer g is said to be gcd of a and b if

i. $g|a$ and $g|b$

ii. If $d|a$ and d$|b$, then $d|g$.

- It is the largest common divisor of a and b.
- Notation for "gcd of a and b" : $gcd(a, b)$ or (a, b)
- Similarly, we can define **Least Common Multiple** of a and b, as the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $lcm(a, b)$ or $[a, b]$.

Theorem: Let a and b be positive integers. Then

$$ab = \gcd(a, b) \times lcm(a, b).$$

anaghakhiste@iiitp.ac.in

Discrete Structure

GCD

Theorem: Let g be the smallest positive integer of the form $ax + by$, where a, b, x and y are all integers, then $g = (a, b)$.

Theorem: If g is the gcd of a and b, then there exist an integers x_0 and y_0 such that $g = (a, b) = ax_0 + by_0$.

(i.e., g can be expressed as linear combination of a and b with integral multipliers x_0 and y_0.)

Theorem: Suppose a, b are integers. Then

i. $(a, b) = (b, a)$

ii. If $x > 0$, then $(ax, bx) = x(a, b)$

iii. If $g = (a, b)$, then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$

iv. for any integers x, $(a, b) = (a, b + ax)$

v. If $(a, m) = (b, m) = 1$, then $(ab, m) = 1$

vi. If $c|ab$ and $(b, c) = 1$, then $c|a$.

anaghakhiste@iiitp.ac.in

Discrete Structure

The Euclidean Algorithm

Lemma: Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

The Euclidean Algorithm:

Suppose that a and b are positive integers with $a \geq b$. When we successively apply the division algorithm, we obtain

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < b, \\ b &= r_1 q_2 + r_2, & 0 \leq r_2 < r_1, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Then by above Lemma, it follows that $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$.

In the expression, $\gcd(a, b) = ax_0 + by_0$, the values of x_0 and y_0 can be obtained by writing each r_i as a linear combination of a and b.

Discrete Structure

The Euclidean Algorithm

Ex 1. Find the greatest common divisor of 414 and 662 using the Euclidean algorithm and express this gcd as a linear combination of 414 and 662.

Solution: Successive uses of the division algorithm give:

$$662 = 414 \times 1 + 248$$
$$414 = 248 \times 1 + 166$$
$$248 = 166 \times 1 + 82$$
$$166 = 82 \times 2 + 2$$
$$82 = 2 \times 41.$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder. $2 = 166 - (82 \times 2)$ $= 166 + 82(-2)$

$= 166 + (248 - 166 \times 1)(-2)$ $= 248(-2) + 166(3)$

$= 248(-2) + (414 - 248 \times 1)(3)$ $= 414(3) + 248(-5)$

$= 414(3) + (662 - 414 \times 1)(-5)$ $= 414(8) + 662(-5)$

anaghakhiste@iiitp.ac.in

Discrete Structure

The Euclidean Algorithm

Ex 2. Find the greatest common divisor of 42823 and 6409. Express this gcd as a linear combination of 42823 and 6409.

Solution: Successive uses of the division algorithm give:

$$42823 = 6409 \times 6 + 4369$$
$$6409 = 4369 \times 1 + 2040$$
$$4369 = 2040 \times 2 + 289$$
$$2040 = 289 \times 7 + 17$$
$$289 = 17 \times 17.$$

Hence, $\gcd(42823, 6409) = 17$, because 17 is the last nonzero remainder.

$17 = 2040 - (289 \times 7)$
$= 2040 + (4369 - 2040 \times 2)(-7)$
$= 4369(-7) + (6409 - 4369 \times 1)(15)$
$= 6409(15) + (42823 - 6409 \times 6)(-22)$

$= 2040 + 289(-7)$
$= 4369(-7) + 2040(15)$
$= 6409(15) + 4369(-22)$
$= 42823(-22) + 6409(147)$

anaghakhiste@iiitp.ac.in

Discrete Structure

Diophantine Equation

Any linear equation in two variables having integral coefficients in the form, $ax + by = c$, where a, b, c are given integers.

Theorem: Let a, b, c be the given integers with not both a and b equal to 0 and let $\gcd(a, b) = g$.

i. If $g \nmid c$, then the equation $ax + by = c$ has no integral solution.

ii. If $g \mid c$, then the equation $ax + by = c$ has infinitely many integral solutions.

If the pair (x_0, y_0) is one integral solution, then all other solutions are of the form $x = x_0 + \frac{k}{g}b$ and $y = y_0 - \frac{k}{g}a$, where k is an integer.

anaghakhiste@iiitp.ac.in

Discrete Structure

Diophantine Equation

Ex. Find the integral values of x and y satisfy the equations

1. $36x + 48y = 125$
2. $71x - 50y = 1$
3. $42823x + 6409y = 17$

1. Solution: Since $(36,48) = 12 \nmid 125$

Thus there is no integral solution, i.e., there is no integers x and y such that $36x + 48y = 125$.

2. Solution: Since $(71,50) = 1|1$

Thus it has infinitely many integral solutions. Using Eclidean algorithm we get a solution, say $x_0 = -19$ and $y_0 = -27$.

Since $x = x_0 + \frac{k}{g}b$ and y $= y_0 - \frac{k}{g}a$, where k is an integer, we have $x = -19 - 50k$ and y $= -27 - 71k$.

Hence, solution set $= \{(x, y) \in Z \times Z : x = -19 - 50k$ and y $= -27 - 71k$, for some k $\in Z\}$

anaghakhiste@iiitp.ac.in

Discrete Structure

Modular Arithmetic (Congruences)

- **Definition:** If a and b are integers and m is a positive integer, then a is congruent to b modulo m, i.e., $a \equiv b(mod\ m)$
  iff $m|(a-b)$,
  iff $a = b + mk$, for some integer k.
- If a is not congruent to b modulo m, then we write $a \not\equiv b\ (mod\ m)$
- **Theorem:** If a and b are integers and m is a positive integer, then $a \equiv b(mod\ m)$ if and only if $r_1 = r_2$ where r_1 and r_2 are the remainders when a and b are divided by m resp.
- Ex. True/ False

i. $87 \equiv 23(mod\ 4)$
ii. $72 \equiv -5(mod\ 7)$
iii. $27 \equiv 8(mod\ 9)$

anaghakhiste@iiitp.ac.in

Discrete Structure

Modular Arithmetic (Congruences)

- **Theorem:** Let a, b, c, and d are integers and m is a positive integer, then

i. $a \equiv a(mod\ m), \forall\ a \in Z$

ii. If $a \equiv b(mod\ m)$, then b $\equiv a(mod\ m)$

iii. If $a \equiv b(mod\ m)$ and b $\equiv c(mod\ m)$, then $a \equiv c(mod\ m)$

iv. If $a \equiv b(mod\ m)$ and c $\equiv d(mod\ m)$, then
$a + c \equiv b + d(mod\ m)$ and $ac \equiv bd(mod\ m)$
In particular, $a^n \equiv b^n(mod\ m)$

v. If $a \equiv b(mod\ m)$ and c > 0, then $ac \equiv bc(mod\ mc)$

vi. If $a \equiv b(mod\ m)$ and $d|m$, $d > 0$, then $a \equiv b(mod\ d)$

vii. Let f denote a polynomial with integral coefficients.
If $a \equiv b(mod\ m)$, then $f(a) \equiv f(b)(mod\ m)$

anaghakhiste@iiitp.ac.in

Discrete Structure

Modular Arithmetic (Congruences)

- **Fermat's Theorem:** Let p be any prime number. If and $p \nmid a$, then $a^{p-1} \equiv 1(mod\ p)$.

  Furthermore, for every integer a, $a^p \equiv a(mod\ p)$.

For ex. 1) Find 8^6 **mod** 7.

Solution: Here $a = 8, p = 7$.

By Fermat's theorem, $8^6 \equiv 1(mod\ 7)$.

This gives $262144 \equiv 1(mod\ 7)$

- **Euler's Theorem: (Generalizattion of Fermat's Theorem)**

  If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1(mod\ m)$, where $\phi(m)$ is the number of positive integers less than m that are relatively prime to m.

anaghakhiste@iiitp.ac.in

Discrete Structure

- **Modular Arithmetic (Congruences)**
- **Properties of Euler's ϕ function:**

i. $\phi(p) = p - 1$, for any prime p.

ii. $\phi(p^k) = p^k - p^{k-1}$, for any prime p, k is any positive integer.

iii. If a and b are relatively prime, then $\phi(ab) = \phi(a)\phi(b)$

iv. In general, for any integers a and b

$$\phi(ab) = \phi(a)\phi(b)\frac{d}{\phi(d)}, \text{ where } (a, b) = d.$$

v. For any integer n, $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, where p_i are prime factors of n.

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right)$$

anaghakhiste@iiitp.ac.in

Discrete Structure

Ex 1. : Show that $2^{340} \equiv 1(mod\ 11)$.

Solution: Since $p = 11$ and $(2, 11) = 1$

So by Fermats theorem, $2^{10} \equiv 1(mod\ 11)$

$$(2^{10})^{34} \equiv 1^{34}(mod\ 11)$$

$$2^{340} \equiv 1(mod\ 11).$$

Ex 2. :Find 7^{293} **mod** 65.

Solution: Since $(7, 65) = 1$, using Eulers theorem we have,

$7^{\phi(65)} \equiv 1(mod\ 65)$, where $\phi(65) = \phi(5)\phi(13) = 4 \times 12 = 48$,

Thus $7^{48} \equiv 1(mod\ 65)$

$\Rightarrow$ $(7^{48})^6 = 7^{288} \equiv 1^6(mod\ 65)$

As $7^3 \equiv 18(mod\ 65)$

$\Rightarrow$ $7^5 \equiv 18 \times 49(mod\ 65)$

$\equiv 37(mod\ 65)$

Thus, $7^{288} \times 7^5 \equiv 1 \times 37(mod\ 65)$. Hence $r = 37$.

Ex 3. Find 3^{302} **mod** 385.

anaghakhiste@iiitp.ac.in

Discrete Structure

Pseudoprime: Let b be a positive integer. If n is a composite positive integer, and $b^{n-1} \equiv 1 \ (mod\ n)$, then n is called a pseudoprime to the base b.

Ex. Determine whether 341 is a pseudoprime to the base 2 or not?

Solution: Yes, since $2^{340} \equiv 1 (mod\ 341)$.

Theorem: Let a and b be any integers and m be a positive integer, then

i. $ax \equiv ay (mod\ m)$ iff $x \equiv y \left(mod \frac{m}{(a,m)}\right)$

ii. If $ax \equiv ay (mod\ m)$ and $(a, m) = 1$, then $x \equiv y (mod\ m)$

iii. $x \equiv y (mod\ m_i)$ for $i = 1,2, \dots, r$ iff
$x \equiv y (mod\ [m_1, m_2, \dots, m_r])$

anaghakhiste@iiitp.ac.in

Discrete Structure

Linear Congruence:

- If a and b are any integers and m is a positive integer, then a congruence of the form $ax \equiv b(mod\ m)$, where an integer x is a variable, is called as a linear congruence.
- A solution of the linear congruence $ax \equiv 1(mod\ m)$ is called as an inverse of a (denoted by $\bar{a}$) **mod** m. Furthermore, every integer $y \equiv \bar{a}(mod\ m)$ is also an inverse of a.
- **Theorem**: If $(a, m) = 1$ and $m > 1$, then the congruence $ax \equiv 1(mod\ m)$ has a solution, i.e., there exists $x(= \bar{a})$ such that $ax \equiv 1(mod\ m)$ and any two such x are congruent $(mod\ m)$.
- Ex. 1) Solve the congruence $3x \equiv 1(mod\ 7)$.
- Or Find an inverse of 3 **mod** 7.
- Solution: Here $a = 3$ and $m = 7 > 1$. Since $(3,7) = 1$, $\bar{a}$ exists.

anaghakhiste@iiitp.ac.in

Discrete Structure

- To find $\bar{a}$: $7 = 3(2) + 1$

$\Rightarrow$ $3(-2) + 7(1) = 1$

$\Rightarrow$ $3(-2) \equiv 1(mod\ 7)$

$\Rightarrow$ $\bar{3} = -2$

$\Rightarrow$ $\bar{a} = \{y \in Z : y \equiv -2(mod\ 7)\}$

$= \{y = -2 + 7k : k \in Z\}$

$= \{\ldots, -9, -2, 5, 12, \ldots\}$

Ex. 2) Find an inverse of 101 modulo 4620.

Solution: Here $a = 101$ and $m = 4620$

Using Eclidean Algorithm, we get

$1 = (101, 4620) = 4620(-35) + 101\ (1601).$

Thus $\overline{101} = 1601.$

Discrete Structure

Linear Congruence:

Theorem: Let a and b be any integers and let m be a positive integer.

- The congruence $ax \equiv b(mod\ m)$ has solution iff $g|b$, where $g = (a, m)$ and the number of solutions are $g(mod\ m)$.
- If $g \nmid b$, then $ax \equiv b(mod\ m)$ has no integral solution modulo m.

Ex. 1) Solve $15x \equiv 9(mod\ 35)$

Solution: Here $a = 15,\ b = 9$ and $m = 35$. Since $(15, 35) = 5$ and $5 \nmid 9$, hence it has no integral solutions.

Ex. 2) Solve $15x \equiv 25(mod\ 35)$, …..(1)

i.e., Find the value of x such that $15x - 35y = 25$

anaghakhiste@iiitp.ac.in

Discrete Structure

Linear Congruence:

Solution: Here $a = 15,\ b = 25$ and $m = 35$. Since $(15, 35) = 5$ and $5|25$, hence it has 5 solutions modulo 35.

Using Eclidean Algorithm, we get

$$5 = (15, 35) = 15(-2) + 35\ (1)$$

Thereore $25 = 15(-10) + 35\ (5)$

Hence $x_0 = -10$ and $y_0 = 5$.

Since $x = x_0 + \frac{k}{g}m$ and y $= y_0 - \frac{k}{g}a$, where k is an integer, we have $x = -10 + 7k$ and y $= 5 - 3k$.

Solution set of (1) $= \{-10 + 7k : k \in Z\}$

Solution set of (1) **mod** 35 $= \{-10 + 7k : k = 0,1,2,3,4\}$

$= \{-10, -3, 4, 11, 18\}$

$= \{4, 11, 18, 25, 32\}$

anaghakhiste@iiitp.ac.in

Discrete Structure

Linear Congruence:

Ex 3) What are the solutions of the linear congruence $3x \equiv 4 \ (mod\ 7)$?

Solution: Here $a = 3,\ b = 4$ and $m = 7$. Since $(3, 7) = 1$ and $1|4$, hence it has 1 solution modulo 7.

Using Eclidean Algorithm, we get

$$1 = (3, 7) = 3(-2) + 7\ (1)$$

Thereore $4 = 3(-8) + 7\ (4)$

Hence $x_0 = -8$ and $y_0 = 4$.

Thus $x = -8 + 7k$ where k is an integer

Solution set of (1) $= \{-8 + 7k : k \in Z\}$

Solution set of (1) **mod** $7 = \{-8 + 7k : k = 0\}$

$= \{-8\}$

$= \{6\}$

anaghakhiste@iiitp.ac.in

Discrete Structure

Chinese Remainder Thm: for solving systems of linear congruences

- A Chinese Mathematician asked in the first century:
- There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5 the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?
- This puzzle is asking for the solution of the following system of congruences:

  $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.
- The Chinese Remainder Theorem establishes that when the moduli are pairwise relatively prime, we can solve such as system of linear congruences uniquely module the product of the moduli.

anaghakhiste@iiitp.ac.in

Discrete Structure

Chinese Remainder Theorem:

Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_r$ be arbitrary integers.

Then, the system:

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1), \\ x &\equiv a_2 \ (mod\ m_2), \\ &\vdots \\ x &\equiv a_r \ (mod\ m_r), \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \ldots m_r$.

(That is, there is a solution x_0 with $0 \leq x_0 < m$, and all other solutions are congruent modulo m to this solution, i.e., all other solutions x are in the form $x_0 + mk$, for some integer k.)

anaghakhiste@iiitp.ac.in

Discrete Structure

Pf of C.R.Thm :-

Let $m = m_1 m_2 m_3 \cdots m_r$

& let $M_i = \frac{m}{m_i} = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_r$, $\forall\ 1 \le i \le r$.

clearly $(M_i, m_i) = 1$, $\forall\ 1 \le i \le r$

$\Rightarrow$ The congruence $M_i x \equiv 1 \pmod{m_i}$ has sol^n say $\bar{M}_i$ $\forall\ 1 \le i \le r$.

i.e. $M_i \bar{M}_i \equiv 1 \pmod{m_i}$, $\forall\ i$

$\Rightarrow a_i M_i \bar{M}_i \equiv a_i \pmod{m_i}$, $\forall\ i$ — (1)

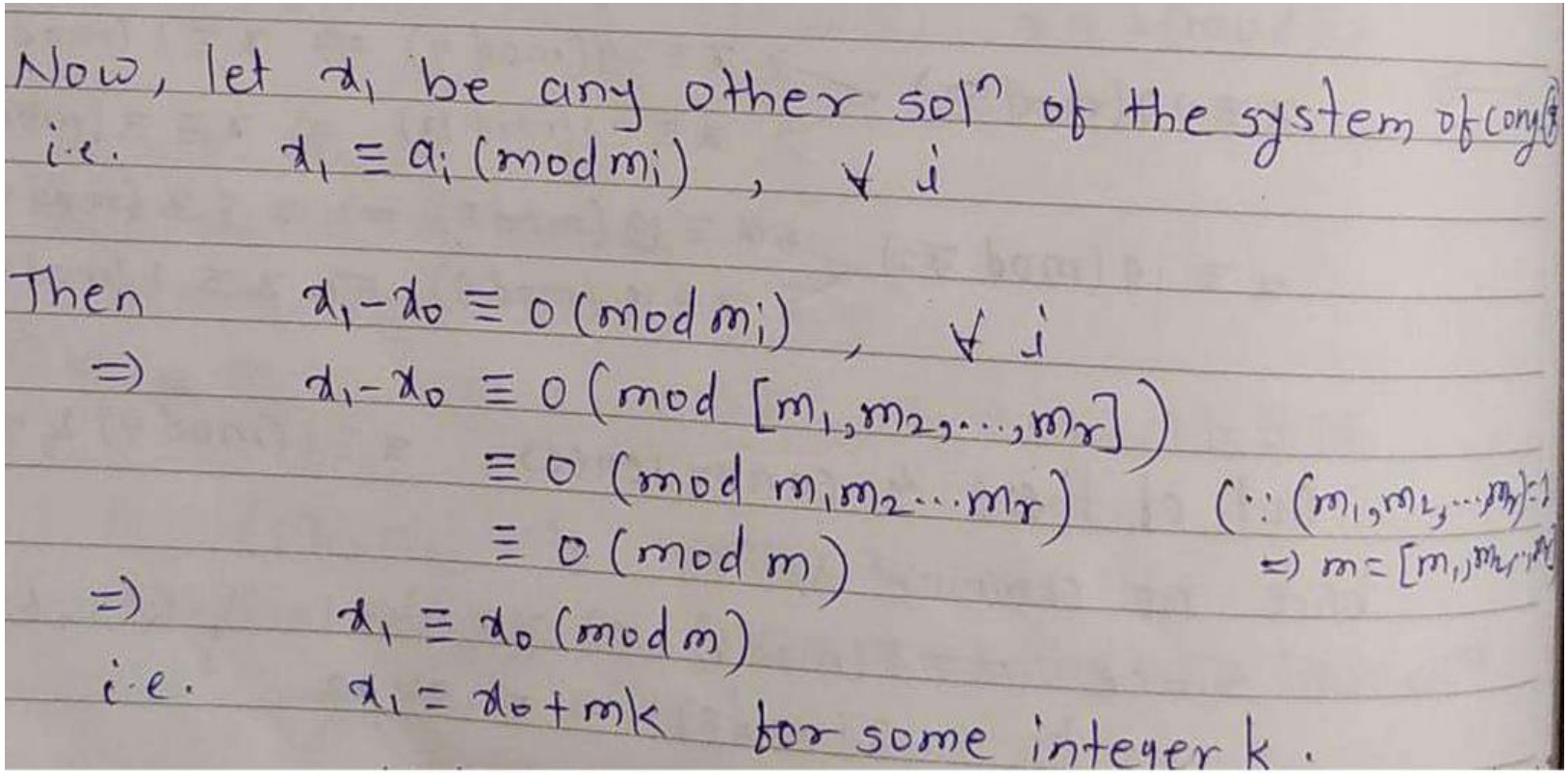
Further we have $M_j \bar{M}_j \equiv 0 \pmod{m_i}$, $\forall\ 1 \le i \ne j \le r$.

$\Rightarrow a_j M_j \bar{M}_j \equiv 0 \pmod{m_i}$, $\forall\ 1 \le i \ne j \le r$.

Thus $\sum_{k=1}^{r} a_k M_k \bar{M}_k \equiv a_i \pmod{m_i}$, $\forall\ 1 \le i \le r$

Hence $x_0 = \sum_{k=1}^{r} a_k M_k \bar{M}_k$ is a sol^n of the system of cong^{ces}

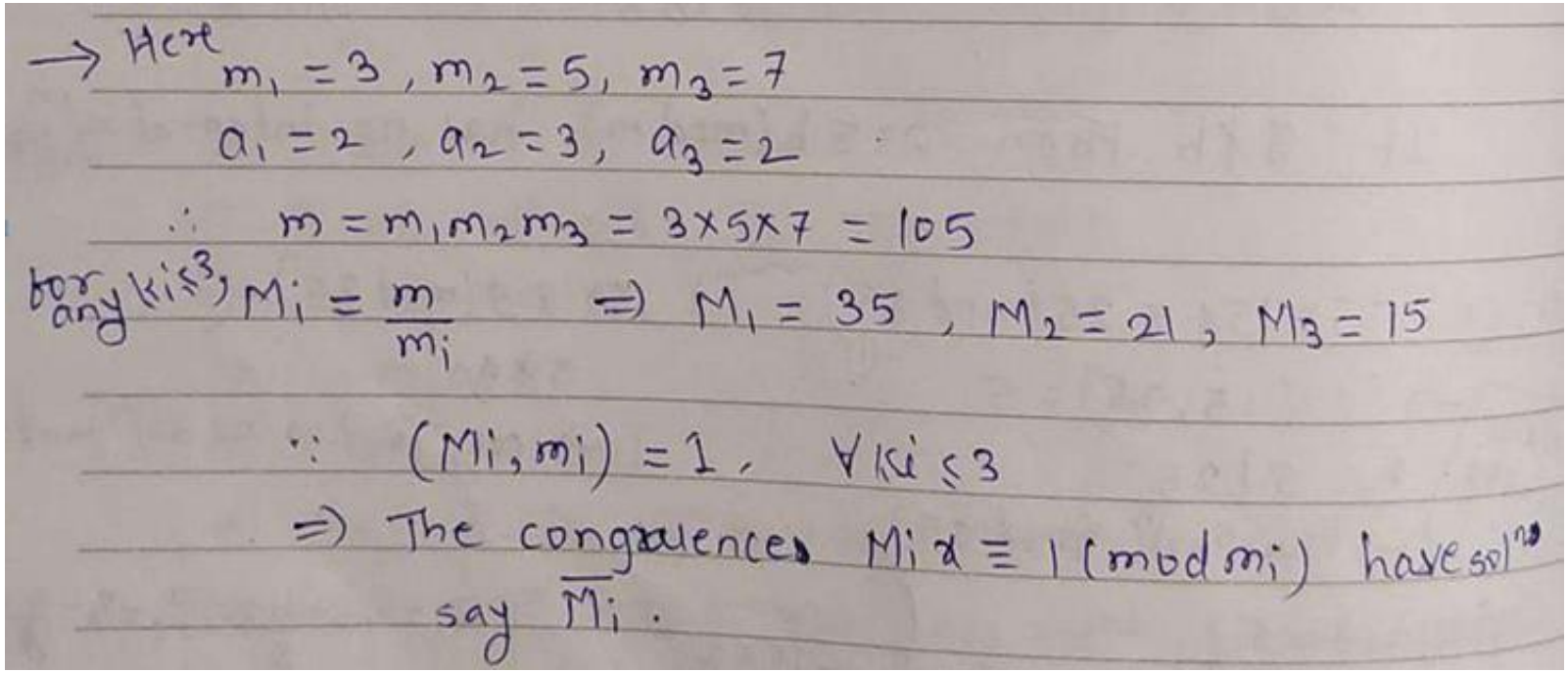
Discrete Structure



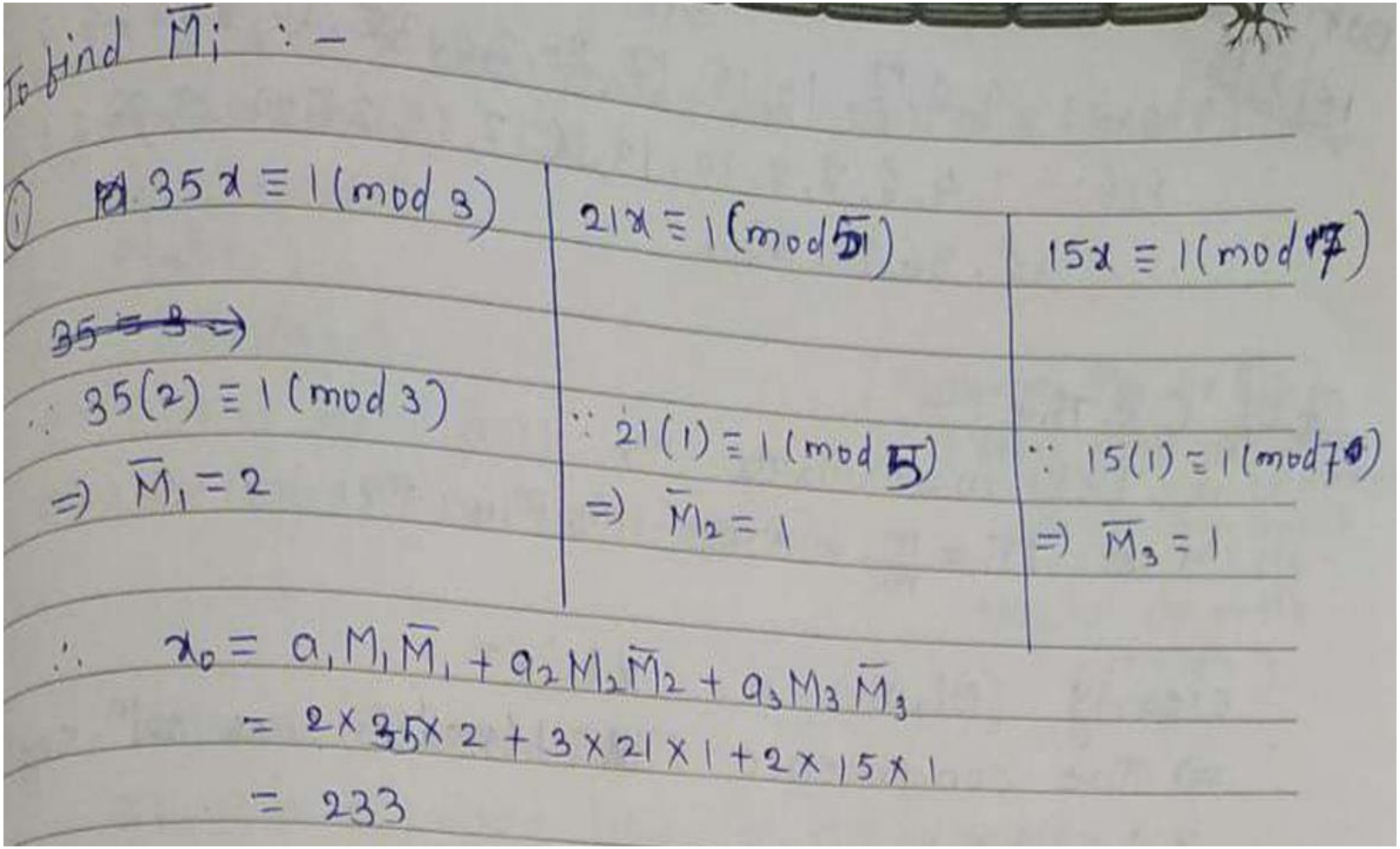
anaghakhiste@iiitp.ac.in

Discrete Structure

Ex. 1) Find the least positive integer x such that
$x \equiv 2\ (mod\ 3),\ x \equiv 3\ (mod\ 5), x \equiv 2\ (mod\ 7)$

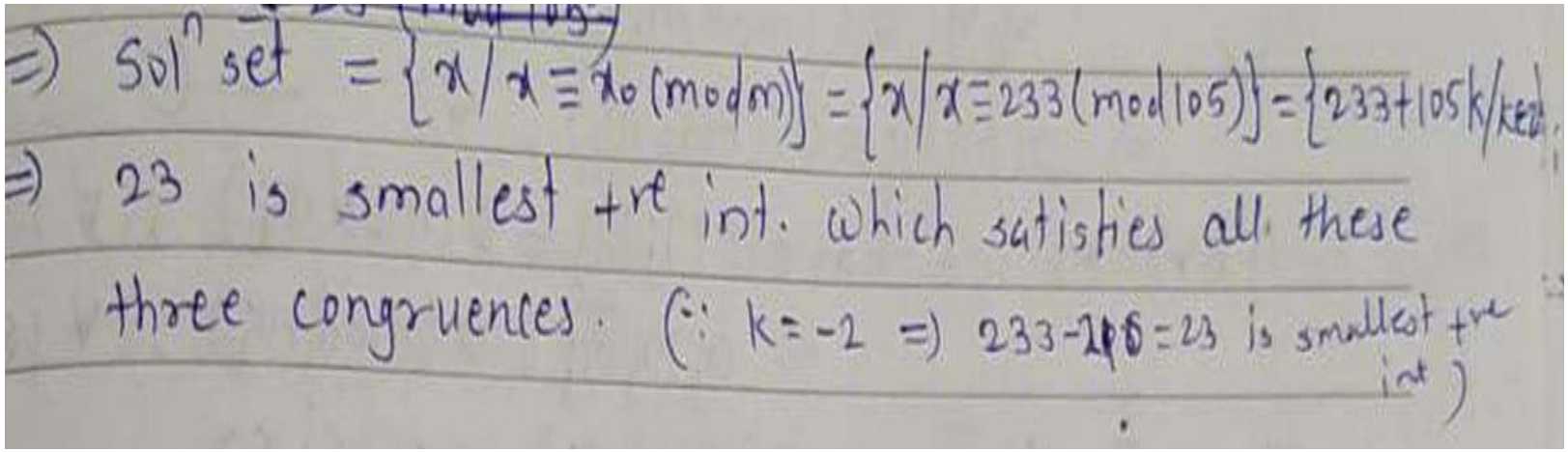


Discrete Structure



anaghakhiste@iiitp.ac.in

Discrete Structure



Discrete Structure

Ex. Solve the the following system of congruences;

2) $x \equiv 4\ (mod\ 5), x \equiv 2\ (mod\ 7), x \equiv 9 (mod\ 11)$.

3) $x \equiv 5\ (mod\ 7), x \equiv 7\ (mod\ 11), x \equiv 3 (mod\ 13)$.

4) Show that the following congruences has no common solutions; $x \equiv 29\ (mod\ 52), x \equiv 19\ (mod\ 72)$.

anaghakhiste@iiitp.ac.in

Discrete Structure

Quadratic residue modulo m:

- If m is a positive integer, the integer a is a quadratic residue of m if $\gcd(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution.
- In other words, a quadratic residue of m is an integer relatively prime to m that is a perfect square modulo m.
- If a is not a quadratic residue of m and $\gcd(a, m) = 1$, we say that it is a quadratic nonresidue of m.

Remarks:

1. If p is an odd prime and a is an integer not divisible by p, then the congruence $x^2 \equiv a \pmod{p}$ has either no solutions or exactly two incongruent solutions modulo p.

2. If p is an odd prime, then there are exactly $\frac{p+1}{2}$ quadratic residues of p among the integers $0, 1, 2, \ldots, p-1$.

anaghakhiste@iiitp.ac.in

Discrete Structure

For example,

- Is 2 a quadratic residue of 7?

Solution: Yes, because $\gcd(2, 7) = 1$ and $3^2 \equiv 2 \ (mod\ 7)$.

- Is 3 a quadratic residue of 7?

Solution: No, because $\gcd(3, 7) = 1$ but $x^2 \equiv 3 \ (mod\ 7)$ has no solution.

Discrete Structure

Applications of Congruences

1. In hash function:

- Suppose that a customer identification number is ten digits long. To retrieve customer files quickly, we do not want to assign a memory location to a customer record using the ten-digit identification number. Instead, we want to use a smaller integer associated to the identification number. This can be done using what is known as a hashing function.
- A hashing function h assigns memory location $h(k)$ to the record that has k as its key.

anaghakhiste@iiitp.ac.in

Discrete Structure

Applications of Congruences

- In practice, many different hashing functions are used. One of the most common is the function

$$h(k) = k \bmod m$$

where m is the number of available memory locations.

- To find $h(k)$, we need only compute the remainder when k is divided by m.
- Furthermore, the hashing function should be onto, so that all memory locations are possible.

Discrete Structure

Applications of Congruences

Ex. 1) Find the memory locations assigned by the hashing function $h(k) = k \bmod 111$ to the records of customers with Social Security Numbers 064212848 and 037149212.

Solution: The record of the customer with Social Security number 064212848 is assigned to memory location 14, because

$$h(064212848) = 064212848 \bmod 111 = 14.$$

Similarly, because

$$h(037149212) = 037149212 \bmod 111 = 65,$$

the record of the customer with Social Security number 037149212 is assigned to memory location 65.

Discrete Structure

Applications of Congruences

Note that

- a hashing function is not one-to-one (because there are more possible keys than memory locations), hence more than one file may be assigned to a memory location.
- When this happens, we say that a **collision** occurs.
- One way to resolve a collision is to assign the first free location following the occupied memory location assigned by the hashing function.

Ex. 2) After making the assignments of records to memory locations in Example 1, assign a memory location to the record of the customer with Social Security number 107405723.

Applications of Congruences

Solution: First note that the hashing function $h(k) = k$ **mod** 111 maps the Social Security number 107405723 to location 14, because $h(107405723) = 107405723 \textbf{ mod } 111 = 14$. However, this location is already occupied (by the file of the customer with Social Security number 064212848). But, because memory location 15, the first location following memory location 14, is free, we assign the record of the customer with Social Security number 107405723 to this location.

Discrete Structure

Applications of Congruences

2. To generate pseudorandom numbers:

- Randomly chosen numbers are often needed for computer simulations. Numbers generated by systematic methods are not truly random, they are called pseudorandom numbers.
- The most commonly used procedure for generating pseudorandom numbers is the **linear congruential method**.

Discrete Structure

Applications of Congruences

- We choose four integers: the modulus m, multiplier a, increment c, and seed x_0, with $2 \leq a < m, 0 \leq c < m$, and $0 \leq x_0 < m$.

We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by successively using the recursively defined function

$$x_{n+1} = (ax_n + c) \bmod m.$$

anaghakhiste@iiitp.ac.in

Discrete Structure

Ex. Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.

Solution: We compute the terms of this sequence by successively using the recursively defined function $x_{n+1} = (7x_n + 4) \bmod 9$, beginning by inserting the seed $x_0 = 3$ to find x_1. We find that

$$x_1 = (7x_0 + 4) \bmod 9 = (7 \times 3 + 4) \bmod 9 = 25 \bmod 9 = 7,$$
$$x_2 = (7x_1 + 4) \bmod 9 = (7 \times 7 + 4) \bmod 9 = 53 \bmod 9 = 8,$$
$$x_3 = (7x_2 + 4) \bmod 9 = (7 \times 8 + 4) \bmod 9 = 60 \bmod 9 = 6,$$
$$x_4 = (7x_3 + 4) \bmod 9 = (7 \times 6 + 4) \bmod 9 = 46 \bmod 9 = 1,$$
$$x_5 = (7x_4 + 4) \bmod 9 = (7 \times 1 + 4) \bmod 9 = 11 \bmod 9 = 2,$$
$$x_6 = (7x_5 + 4) \bmod 9 = (7 \times 2 + 4) \bmod 9 = 18 \bmod 9 = 0,$$
$$x_7 = (7x_6 + 4) \bmod 9 = (7 \times 0 + 4) \bmod 9 = 4 \bmod 9 = 4,$$
$$x_8 = (7x_7 + 4) \bmod 9 = (7 \times 4 + 4) \bmod 9 = 32 \bmod 9 = 5,$$
$$x_9 = (7x_8 + 4) \bmod 9 = (7 \times 5 + 4) \bmod 9 = 39 \bmod 9 = 3.$$

Discrete Structure

Because $x_9 = x_0$ and because each term depends only on the previous term, we see that the sequence

$$3, 7, 8, 6, 1, 2, 0, 4, 5, 3, 7, 8, 6, 1, 2, 0, 4, 5, 3, \ldots$$

is generated. This sequence contains nine different numbers before repeating.