MODULAR ARITHMETIC AND ITS APPLICATIONS

By
Dr. N Bhaskar, M.Sc.,.PGDCA,Ph.D.,
Professor & Head
VVCE, Mysuru

Prerequisite

- Basic Number theory(Natural and Integers)
- Prime and Composite Numbers
- Greatest Common Divisor
- Relatively Prime
- Euclidian Algorithm
- Inverse in Congruent

Greatest Common Divisor(gcd)

d is the **greatest common divisor** of integers *a* and*b* if *d* is the largest integer which is a common divisor of both *a* and *b*.

Notation: $d = \gcd(a, b)$

Example: 2, 7, and 14 are the only integers that are common divisors of both 42 and 56.
Since 14 is the largest, $\gcd(42, 56) = 14$.

Example: gcd(81,153) = 9

RELATIVE PRIME

- Definition:

pair of integers are said to be relatively prime if gcd is 1

If a and b are relatively prime then d=gcd(a,b)=1

Example: 42 and 75 as gcd(42,75)=1

59 and 97 as gcd(59,97)=1

The Division Algorithm and Euclidian Algorithm

.

DIVISION ALGORITHM

For integers a and b, with $a > 0$,

there exist integers q and r such that

$$b = qa + r \quad \text{and} \quad 0 \leq r < a$$

Euclidian Algorithm

a method of finding the greatest common divisor of two numbers by dividing the larger by the smaller, the smaller by the remainder, the first remainder by the second remainder, and so on until exact division is obtained whence the greatest common divisor is the exact divisor

Steps to find gcd using Euclidian Algorithm
For any two integers a and b with a>b

- Step 1: Let a, b be the two numbers.
- Step 2: a mod b = R.
- Step 3: Let a = b and b = R.
- Step 4: Repeat Steps 2 and 3 until a mod b is greater than 0.

The Euclidean Algorithm

- For example, find the gcd of 25520 and 19314:
  - $25520 = 1 \cdot 19314 + 6206$
  - $19314 = 3 \cdot 6206 + 696$
  - $6206 = 8 \cdot 696 + 638$
  - $696 = 1 \cdot 638 + 58$
  - $638 = 11 \cdot 58$
- Thus, $\gcd(25520, 19314) = 58$.

The Euclidean Algorithm

- We may present this in the form of a table:

a	b	q	r
25520	19314	1	6206
19314	6206	3	696
6206	696	8	638
696	638	1	58
638	58	11	0

Euclidean Algorithm contd……

- Now use the Euclidean Algorithm to write gcd(486, 434) as a linear combination of 486 and 434.

b	a	q	r	r = b-aq
486	434	1	52	52= 486-1X434
434	52	8	18	18= 434-8X52
52	18	2	16	16= 52-18X2
18	16	1	2	2=18-1X16
8	2	4	0	

- 2= 18-1X16→2= 3X18 – 1X52→2 = 3 X 434 – 9 X 52

  →2 = 12 X 434 – 9 X 486 →2= 12 X 434 + (-9) X 486

2= gcd(486, 434) =486x + 434 y, with x = 12 and y= -9

TRY WITH SOME EXAMPLES

- GCD(2322,654)
- GCD(450,741)

CONGRUENCY

- Let a and b be any two integer with m being positive integer

then,

a is said to be congruent mod m

if m/(a-b) or a-b = m X k, where k is some integer

And it is denoted by

$a \equiv b \pmod{m}$

with $0 \leq |b| < m$

Example: $155 \equiv 5 \pmod{10}$

$155 \not\equiv 4 \pmod{10}$

PROPERTIES OF CONGRUENCE

Modular Arithmetic

For $n \geq 1$,

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n}$ implies $b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ imply $a \equiv c \pmod{n}$
4. $a \equiv b \pmod{n}$ implies $a + c \equiv b + c \pmod{n}$
5. $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$
6. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $a + c \equiv b + d \pmod{n}$
7. $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ imply $ac \equiv bd \pmod{n}$

PROPERTIES contd....

The letters a, b, c, d, k represent integers. The letters m, n represent positive integers. The notation $a \equiv b \pmod{m}$ means that m divides $a - b$. We then say that a is congruent to b modulo m.

1.(Reflexive Property): $a \equiv a \pmod{m}$

2.(Symmetric Property): If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

3.(Transitive Property): If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$,

then $a \equiv c \pmod{m}$.

Contd….

4.If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$ and $a - c \equiv b - d \pmod{m}$.

5.If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

6. Assume that $a \equiv b \pmod{m}$. Let $k \geq 1$. Then $a^k \equiv b^k \pmod{m}$.

contd….

6.Suppose that $P(x)$ is any polynomial with coefficients in $\mathbf{Z}$. Assume that $a \equiv b \pmod{m}$. Then $P(a) \equiv P(b) \pmod{m}$.

7.Assume that $a \equiv b \pmod{m}$. Then $gcd(a, m) = gcd(b, m)$.

8.If $a \equiv b \pmod{m}$ and $n \mid m$, then $a \equiv b \pmod{n}$.

9. Assume that $gcd(m, n) = 1$. Assume that $a \equiv b \pmod{m}$ and that $a \equiv b \pmod{n}$, Then $a \equiv b \pmod{mn}$.

Properties of Modular Arithmetic

Define the set Z_n as the set of nonnegative integers less than n:

$$Z_n = \{0, 1, \ldots, (n-1)\}$$

This set is referred to as the set of **residues**, or **residue classes** (mod n). That is, each integer in Zn represents a residue class.

Properties of Modular Arithmetic

We can label the residue classes (mod n) as:

[0],[1],[2],...,[n-1], where

$[r] = \{a: a \text{ is an integer}, a \equiv r \pmod{n}\}$.

E.g.: The residue classes (mod 4) are

[0] = {..., -16,-12,-8,-4,0,4,8,12,16, ...}

[1] = {..., -15,-11,-7,-3,1,5,9,13,17, ...}

[2] = {..., -14,-10,-6,-2,2,6,10,14,18, ...}

[3] = {..., -13,-9,-5,-1,3,7,11,15,19, ...}

Exponentiation

- Exponentiation is done by repeated multiplication, as in ordinary arithmetic.

To find $(11^7 \bmod 13)$ *do the followings*

$$11^2 = 121 \equiv 4 (\bmod 13)$$

$$11^4 (11^2)^2 \equiv 4^2 \equiv 3 (\bmod 13)$$

$$11^7 \equiv 11 \times 4 \times 3 \equiv 132 \equiv 2 (\bmod 13)$$

Few more example:

- Example:

- Find the value of $11^{153} \pmod{12}$

  $11^2 \equiv 1 \pmod{12}$

  Using division algorithm, we have 153 = 2x75 + 3

  $11^{153} = 11^{(2x75+3)} \equiv (11^2)^{75} X 11^3 \pmod{12} \equiv (11)^{2+1} \pmod{12}$

  $\equiv 11 \pmod{12}$

  - Ans= 11

- Example:

last digit of 3^{1963}

To find x so that $3^{1963} \equiv x \pmod{10}$

$3^2 \equiv (-1) \pmod{10}$ But 1963 = 196 X 10 + 3

Hence $3^{196 \text{ X } 10 + 3} \equiv (-1)^{196 \text{ X } 10 + 3} \pmod{10} \equiv (-1)^3 \pmod{10} \equiv (-1) \pmod{10} \equiv 9 \pmod{10}$

Last digit = 9

Example

- Find $14^{100} \bmod 27$.
- $14^{100} = 14^{64} \cdot 14^{32} \cdot 14^{4}$.
- Compute
  - $14^{2} \bmod 27 = 7$.
  - $14^{4} \bmod 27 = 7^{2} \bmod 49 = 22$
  - $14^{8} \bmod 27 = 22^{2} \bmod 27 = (-5)^{2} \bmod 27 = 25$
  - $14^{16} \bmod 27 = 25^{2} \bmod 27 = (-2)^{2} \bmod 27 = 4$
  - $14^{32} \bmod 27 = 4^{2} \bmod 27 = 16$
  - $14^{64} \bmod 27 = 16^{2} \bmod 27 = 13$

Modular Inverses

- Then consider corresponding congruence modulo m:

$$as + mt \equiv 1 \pmod{m}$$

$$as \equiv 1 \pmod{m}$$

- Thus, s is the inverse of a, modulo m.

INVERSE UNDER MODULO

- b is said to be inverse of a(mod n) if

$$ab \equiv 1 \pmod{n}$$

To find the inverse of a(mod n) we apply Euclidian Algorithm for

a and n so that , ax +n y =1 ,

then inverse of a(mod n) = b = x,

with

$$0 < x < n$$

- Find the inverse of 27 (mod 392)
- Apply Euclidian algorithm for 27 and 392

a	b	q	r	r = a- b q
392	27	14	14	14 = 392 – 14 X 27
27	14	1	13	13 = 27 – 1 X 14
14	13	1	1	1 = 14 – 1 X 13

Now, Expressing 1 as linear combination of 392 and 27

We have 1 = 2 X 392 + 363 X 27

Hence inverse of 27(mod 392) is 363

Prob contd.....

- Find the inverse of 15(mod 26)

  to find so that $15x \equiv 1 \pmod{26}$

We apply Euclidian algorithm for 15 and 26

a	b	q	r	r = a- b q
26	15	1	11	11 = 26 -1X 15
15	11	1	4	4 = 15 – 1 X 11
11	4	2	3	3 = 11 – 2 X 4
4	3	1	1	1 = 4 – 1X3

- By expressing linear combination of 15 and 26
- 15 x + 26 y = 1 , with 7 and -4 hence inverse of 15(mod26)
- Alternative method:
- Inverse of 15(mod26) we need to solve $15x \equiv 1 \pmod{26}$
- i,e., X = $\frac{26k+1}{15}$ to find k so that x is positive integer
- For k = 4 we get x = 7 which is the inverse of 15(mod26)

Inverse contd……

- Find

  inverse of 20(mod 97)

  inverse of 37 (mod 123)

Example

- Find the inverse of 10, modulo 27.
  - Apply the extended Euclidean algorithm to get $s = -8$ and $t = 3$, implying that
    $$10(-8) + 27(3) = 1.$$
  - Thus, $10(-8) \equiv 1 \pmod{27}$.
  - So, $10(19) \equiv 1 \pmod{27}$.
- Therefore, for example,
  $$5/10 \equiv 5(19) \equiv 95 \equiv 14 \pmod{27}.$$

DIOPHANTINE EQUATIONS

- an equation involving two or more variables in which the coefficients of the variables and solutions to the problem are integers

Examples of Diophantine Equations

$ax + by = 1$ (Linear Diophantine Equation)

$x^n + y^n = z^n$ (If $n = 2$, there are an infinite amount of solutions for x, y, and z, the Pythagorean Triples. For larger values of n, Fermat's Last Theorem states that there are no positive integer solutions for x, y, and z satisfying this equation)

$x^2 - ny^2 = \pm 1$ (Pell's equation)

$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ (The Erdös-Straus conjecture, states that for every positive integer $n \geq 2$, there is a solution for x, y, and z as positive integers.)

LINEAR DIOPHANTINE EQUATION

- If a,b,c are any positive integers with d=gcd(a,b) then

linear Diophantine equation ax + by = c as solution only if d/c

And if

x_0 and y_0 represents primitive solution then

general solution is

$x = x_0 + (b/d)t$, $y = y_0 + (a/d)t$, for t is positive integer

where d = gcd(a,b)

example

- Solve $7x + 18y = 208$

  $a=7$, $b=18$, $c = 108$ with $d=1$ and d/c

By Euclidian algorithm we have

$$1 = 7x\text{-}5 + 18 \times 2 \text{ (multiply by 208)}$$

$$208 = 7x\text{-}1040 + 18 \times 416$$

with $x_{0} = -1040$ $y_{0} = 416$

And solutions is $x = -1040 + (18/1)t$ and $y = 416 + (7/1)t$

Example contd….

- Solve $56x + 72y = 40$

  d= 8 and d/c it has solution

By Euclidian algorithm,

$$8 = 56 \times 4 + 72 \times -3 \quad \text{(multiply by 5)}$$

$$40 = 56 \times 20 + 72 \times -15$$

With solution $x = 20 + (72/8)t$ and $y = -15 + (56/8)t$

- Solve $172x + 20y = 1000$

Contnd….

Application problem

- A customer bought dozen quantity of apple and orange for rs.132 with cost of apple is rs. 3 more than orange. Find number of fruits he brought.
- x→ no. of apple y→ no. of orange then x+y = 12

  and if z is cost of orange the

  $(z+3)x + zy = 132 \rightarrow 3x + 12z = 132$

Solving we get

1. no. of apples 8 and no. of orange 4
2. No. of apples 12 and no. of orange 0

- Suppose a man went to a bank to get some cash. The cash amount consists of some 100 Rs and some 50 Rs and the bank had only an infinite supply of 100 Rs and 50 Rs there when he went to the cashier to take his money. By mistake the cashier exchanged the number of 100Rs with the number 50Rs. But he did not count the total amount of money in the bank cashier. Then he moved to the market to buy some things there he spent 5 50Rs. After buying the things he counted his money in his pocket, and he found that the total money in his pocket is twice his initial money. Now how to calculate the total amount of his initial money.
-

• Let suppose initially he had x amount of 100 Rs and y amount of 50 Rs. So, according to the problem$100y+ x – 5 = 2 (100x+ y)$

Or,

$-199x + 98y = 5$

The above equation is an example of Diophantine equation as it has two unknowns and also gcd(199,98) =1 divides 5 so solution exists for this linear

$X = 8k – 165$

and $y = 199k – 335$

$X = 31$ and $y = 63$ is he solution for $k = 2$.

Problem for practice

- If item A is 5 coins , B is 3 coins and thrice C is 1 coin. How many tems of A , B , C totally 100 to be purchased for rs. 100

This Lecture

In this lecture we will study the Chinese remainder theorem, which is a method to solve equations about remainders.

- One equation
- Ancient application
- Two equations and three equations
- Chinese Remainder theorem

One equation

- $ax \equiv b \pmod{n}$

  has no solution if $d \nmid b$

  has solution if d/b , where d = gcd(a,n)

  1. if d/b then it has d congruent solutions
  2. if d=1 the it has only one congruent solution

Example:

- $2x \equiv 3 \pmod 7$

  gcd(2,7) = 1 , hence it has unique congruent solution and

  then, $x = \frac{7k+3}{2}$ for k =1 , x = 5

  solution IS x = [5] = {5, 12,…}

- $5x \equiv 6 \pmod 9$

  gcd(5,9) = 1, hence it has unique congruent solution and

  solution IS x = [3] = {3, 12,….}

- $4x \equiv 2 \pmod 6$

  gcd(4,6) = 2 and 2/6, hence it has two congruent solutions and

  solutions are [2] = {2, 8,…..}

  [5]= {5, 11,…}

- $3x \equiv 1 \pmod 6$

  gcd(3,6) = 3 and 3∤ 1, hence no solution

One Equation: Exercise

$87x \equiv 3 \pmod{15}$	Replace 87 by 87 mod 15
$12x \equiv 3 \pmod{15}$	Divide both sides by gcd(12,15) = 3
$4x \equiv 1 \pmod{5}$	Compute the multiplicative inverse of 4 modulo 5
$x \equiv 4 + 5k$	
$114x \equiv 5 \pmod{22}$	Replace 114 by 114 mod 22
$4x \equiv 5 \pmod{22}$	Divide both sides by gcd(4,22) = 2
no solutions	Because 2 does not divide 5.

Important: to be familiar with the extended Euclidean algorithm to compute gcd and to compute multiplicative inverse.

Chinese Remainder Theorem

Theorem: If $n_1, n_2, \ldots, n_k$ are relatively prime and $a_1, a_2, \ldots, a_k$ are integers, then

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_k \pmod{n_k}$$

have a simultaneous solution x that is **unique** modulo n, where $n = n_1 n_2 \ldots n_k$.

We will give a proof when k=3, but it can be extended easily to any k.

Contd….

- Procedure to apply Chinese remainder theorem
- If m_i, i=1,2,3 are relatively prime
- Then the solution of $x_i \equiv b_i \pmod{m_i}$, i=1,2,3
- Is x = $\sum_1^3 b_i M_i y_i$
- Where, $M_i = M / m_i$ with $M = \prod_1^3 m_i$
- And y_i such that $M_i y_i \equiv 1 \pmod{m_i}$ that is y_i *is inverse of* M_i under mod m_i

Contd on CRT….

- Problem
- Solve x≡ 1(mod3), x≡ 2(mod5) and x≡ 3(mod7)
- M= 3X5X7=105
- b1=1 b2=2 b3=3
- m1 = 3 m2= 5 m3= 7
- M1= M/m1 =35 M2= M/m2 =21 M3=M/m3 =15
- M1Y1≡ 1(modm1)→ y1=2
- M2Y2≡ 1(modm2)→y2=1
- M3Y3≡ 1(modm3)→y3=1
- X=$\sum_1^3 biXMiXyi$ = 52(mod105)

Contd…..

INTERESTING APPLICATION OF CRT

CRT is to solve system of linear congruences.

To find a number which when divided by 3, 4, and 5 leave a remainder equal to 1, 2 and 3

Now, problem is modeled to three linear congruences.

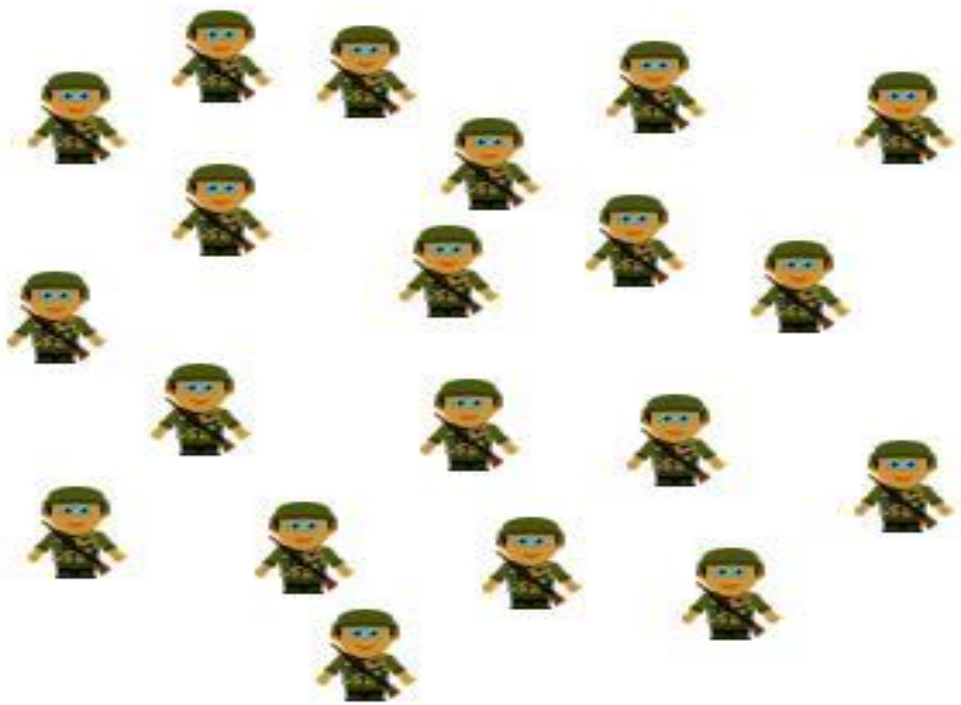
$x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $x \equiv 3 \pmod 5$

Since 3,4 and 5 are relatively prime we can solve this problem using CRT

Ancient Application of Number Theory

Starting from 1500 soldiers, after a war, about 400-500 soldiers died.

Now we want to know how many soldiers are left.



Form groups of 3 soldiers

韓信

2 soldiers are left

Ancient Application of Number Theory

There are 2 soliders left.

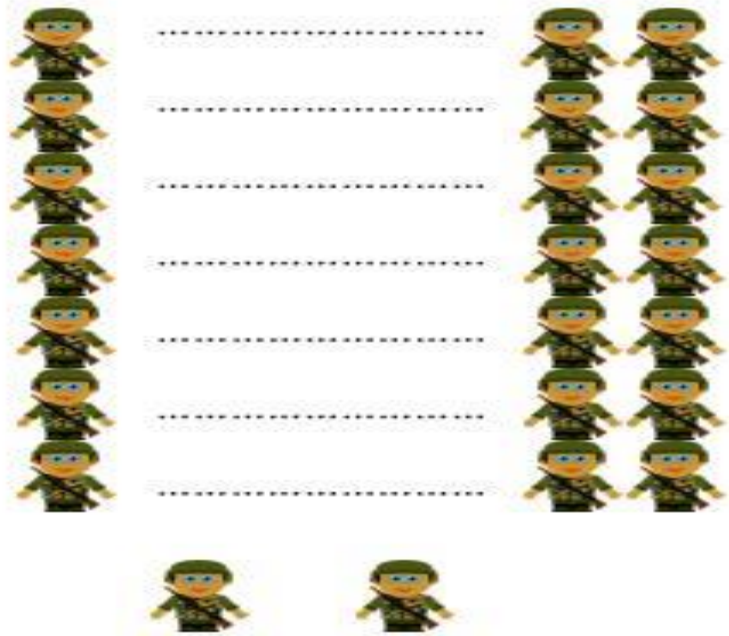
Form groups of 5 soldiers

Ancient Application of Number Theory

There are 3 soliders left.

Form groups of 7 soldiers

Ancient Application of Number Theory



There are 2 soliders left.

We have 1073 soliders.

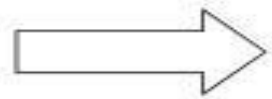
How could he figure it out?!

The Mathematical Question

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

+

$1000 <= x <= 1100$



$x = 1073$

How to solve this system of modular equations?

Very interesting problem ????

- ***Find the last three digits of the 100th powers of the first 100 natural numbers***

(we can solve by using CRT and euler's Φ function….)

- ***Technical application of CRT***
    1. Signal Processing and the Information Security
    2. ***Image compression***
    3. ***RSA decryption in faster sense***

Few more ……

The RSA Cryptosystem

- The RSA cryptosystem was named after Ronald Rivest, Adi Shamir, and Leonard Adleman, who are now quite rich.
- It is a “public-key” cryptosystem.
  - The encryption key can be made public without revealing the decryption key.
  - Thus, anyone can encrypt a message and send it, but only holders of the private decryption key can decrypt them.

The RSA Cryptosystem

- The RSA cryptosystem begins with two large primes p and q.
  - "Large" means at least 100 digits long.
- Theorem: Let a be any integer not divisible by p or q. Then

$$a^{(p-1)(q-1)} \equiv 1 \pmod{pq}.$$

The RSA Cryptosystem

- Next, choose an integer e that is relatively prime to $(p-1)(q-1)$. This is the encryption key.
- The *public key* is the pair (pq, e).
- Use the extended Euclidean algorithm to find the inverse of e, modulo $(p-1)(q-1)$. Call it d, the decryption key.

The RSA Cryptosystem

- The decryption procedure is similar.
- Given the ciphertext C, recover M as follows:

$$M = C^d \bmod pq.$$

- Why does this work?
  - Why does this recover M?
  - Why can't the enemy obtain d from e.

The RSA Cryptosystem

- Let M be the *plaintext* message, expressed as an integer between 0 and $pq - 1$.
- For example, ASCII may be used.
- Longer messages are broken into blocks of such integers.
- Encrypt M to the *ciphertext* C as follows:

$$C = M^e \bmod pq.$$

Why RSA Recovers M

- Since e and d are inverses modulo $(p-1)(q-1)$, then $ed = 1 + k(p-1)(q-1)$, for some integer k.
- Thus,

$$\begin{aligned} C^d &\equiv (M^e)^d \equiv M^{ed} \\ &\equiv M^{1 + k(p-1)(q-1)} \\ &\equiv M \cdot (M^k)^{(p-1)(q-1)} \\ &\equiv M \pmod{pq}. \end{aligned}$$

The RSA Cryptosystem

- For example, if $p = 37$ and $q = 41$, then $pq = 1517$ and $(p-1)(q-1) = 1440$.
- Let $a = 7$.
- A simple computation verifies that

$$7^{1440} \equiv 1 \pmod{1517}.$$

- To find the inverse of 7 under (mod1440)

We apply the linear congruence

by taking $7x \equiv 1 \pmod{1440}$

Where x = 823

- for p=37 and q = 41

then pq = 1517 and (p-1)(q-1) = 1440

choose e = 7 with gcd(e, pq) = 1, i,e,. e and pq are relatively prime

compute d = 823,

the inverse of 7(mod144r0)

now the public key is (1517,7)

RSA Example

- Let $p = 37$ and $q = 41$.
- Then $pq = 1517$ and $(p-1)(q-1) = 1440$.
- Choose $e = 7$.
- Compute $d = 823$.
- Publish the key (1517, 7).

ASCII VALUE OF ALPHABET

65	A	71	G	77	M	83	S	89	Y	
66	B	72	H	78	N	84	T	90	Z	
67	C	73	I	79	O	85	U			
68	D	74	J	80	P	86	V			
69	E	75	K	81	Q	87	W			
70	F	76	L	82	R	88	X			

RSA Example

- Alice wants to send Bob the message

  "ATTACK AT DAWN"

- In ASCII, this is the plaintext

  65, 84, 84, 65, 67, 75, 32, 65, 84, 32, 69, 65, 87, 78

- Let's encrypt only 65 for this example.
- Compute $M^e = 65^7 \bmod 1517 = 1094 = C$.
- Transmit 1094.

RSA Example

- Bob receives the ciphertext

  1094, 1194, 1194, 1094, 1483, 926, 870, 1094, 1194, 870, 56, 1094, 143, 918

- Let's decrypt only 1094 for this example.
- A simple calculation shows that

$$C^d = 1094^{823} \bmod 1517 = 65 = \text{'A'}$$

The Security of RSA

- Suppose we were given the numbers 37 . 41 = 1517 and 37 + 41 = 76. How would we find 37 and 41?
- Consider the quadratic equation

$$(x - 37)(x - 41) = x^2 - 76x + 1517 = 0.$$

- We could use the quadratic formula to find the two roots, 37 and 41.

Fermat's little theorem

- If p is any prime and p ∤a, then

$a^{p-1} \equiv 1 \pmod{p}$ or $a^{p} \equiv a \pmod{p}$

Problem:

Find the remainder when 24^{1947} divide by 17

To find x so that $24^{1947} \equiv x \pmod{17}$

a=24 and p = 17 and (24,17)=1{relatively prime}

Hence $24^{16} \equiv 1 \pmod{17}$

Now 1947 = 121 x 16 + 11

$24^{121 \text{ x } 16 + 11} = 24^{11}$

Now $24^{2} \equiv -2 \pmod{17} \rightarrow 24^{2X5+1} \equiv (-2)^{5} X24 = -32X24 = 2X24 = 48 \pmod{17}$

Hence $24^{1947} \equiv 48 \pmod{17} = 14 \pmod{17}$

Hence remainder is 14

Contnd….

- Problem:

Find the remainder of 11^{104} $when\ divided\ by$ 15

Problem :

Find the unit digit of 13^{1005}

EULERS Φ-FUNCTION

General Case

- Given *n* and it's prime factorization, can we derive a general formula for *n*?

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$

$$\phi(n) = \phi(p_1^{r_1})\phi(p_2^{r_2})\ldots\phi(p_m^{r_m})$$

In general:

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

.

Euler's totient function (also called the Phi function) counts the number of positive integers less than n that are coprime to n. That is,$\phi(n)$ is the number of m, $m \in \mathbb{N}$ such that $1 \leq m < n$ and $\gcd(m,n)=1$

- Example:

$900 = 2^3 \ X 3^2 \ X 5^2$

$\phi(900)=900(1-21)(1-31)(1-51)=240$

$2000 = 2^4 \ X \ 5^3$

$\phi(2000)= 2000(1-\frac{1}{2})(1-\frac{1}{3})= 800$

Module -4 Modular Arithmetic (CSE branches)

	Topics	Topics to be covered	Hrs
	Introduction to Congruences, Linear Congruences, The Remainder theorem (statement only), Solving Polynomials, Linear Diophantine Equation, System of Linear Congruences	**Articles 4.2, 4.4, 2.5 of textbook 3 (Similar types of problems in the exercise to be discussed)**	2L
	Euler's Theorem(statement only), Wilson's Theorem(statement only) and Fermat's little theorem (statement only).	**Articles 7.2, 7.3, 5.3, 5.2 of textbook 3 (Similar types of problems in the exercise to be discussed)**	2L
	Applications of Congruences-RSA algorithm	**Article 10.1 of textbook 3 (restricted simple problems)**	1L

Module -4 (All branches)

	Topics	Topics to be covered	Hrs
	Tutorials	Involvement of faculty and students in identifying the problems & solutions. **PPT presentations of Engg. Applications- Cryptography, encoding and decoding, RSA applications in public key encryption by the faculty about the module**. Guide the students to self-study topics through illustrative examples.	4T
	Self-study: Centre and Circle of curvature, evolutes and involutes	**Article no. 2.2, 2.3 & 3.1 of textbook 3** **No Question is to be set for SEE** **20% weightage shall be given to CIE from self-study topics**	

Module-4			
Q. 7	a	(a) Find the remainder when 2^{23} is divided by 47 (b) Find the last digit in 7^{118}.	06
	b	Find the solutions of the linear congruence $11x \equiv 4\ (mod\ 25)$.	07
	c	Encrypt the message STOP using RSA with key (2537,13) using the prime numbers 43 and 59	07

Module-4			
Q. 8	a	Using Fermat's little theorem show that $8^{30} - 1$ is divisible by 31.	06
	b	Solve the system of linear congruence $x \cong 3(mod\ 5), x \cong 2\ (mod\ 6), x \cong 4\ (mod\ 7)$ using Chinese remainder theorem	07
	c	(a) Find the remainder when 175×113×53 is divided by 11. (b) Solve $x^3 + 5x + 1 \cong 0(mod\ 27)$.	07