B.M.S. COLLEGE OF ENGINEERING, BENGALURU
DEPARTMENT OF MATHEMATICS

For the Course Code: 23MA1BSMCS
Course: Mathematical Foundation for Computer Science Stream – 1

Unit 4: Congruence's and its Applications

I. Examples on Application of congruence's in finding remainders:

1. Prove that 11 divides $233^5 - 1$.
2. Prove that 31 divides $15^{10} - 1$.
3. Show that 41 divides $2^{20} - 1$.
4. Find the remainder when 5^{48} is divided by 24.
5. Find the remainder when the sum $1! + 2! + 3! + 4! + \ldots\ldots\ldots\ldots + 1000!$ is divided by 8.
6. Find the number of mangoes remaining if we distribute 2^{67} mangoes equally among 17 fruit stalls.
7. Is it possible to distribute 2^{340} computers among 341 colleges equally? , if no, find the number of computers remaining when we distribute equally.
8. What is the remainder when 11^{35} divided by 13

II. Find the number of solutions exists in each of the following linear congruence

1. $8x \equiv 12 \pmod{20}$
2. $9x \equiv 15 \pmod{27}$
3. $7x \equiv 2 \pmod{37}$

III. Solve the following linear congruence's

1. $7x \equiv 2 \pmod{37}$
2. $11x \equiv 4 \pmod{25}$
3. $5x \equiv 1 \pmod{4}$
4. $3x \equiv 1 \pmod{23}$
5. $12x \equiv 6 \pmod{21}$
6. $8x \equiv 6 \pmod{10}$
7. $21x \equiv 7 \pmod{25}$
8. $7x \equiv 21 \pmod{49}$
9. $28x \equiv 56 \pmod{49}$
10. $3x \equiv 12 \pmod{6}$

IV. Solve the following system of linear congruence's using Chinese Remainder Theorem

1. $x \equiv 3 \pmod{5},\ x \equiv 2 \pmod{6},\ x \equiv 4 \pmod{7}$
2. $x \equiv 2 \pmod{3},\ x \equiv 3 \pmod{5},\ x \equiv 2 \pmod{7}$
3. $x \equiv 1 \pmod{5},\ x \equiv 3 \pmod{6},\ x \equiv 2 \pmod{7}$

For the Course Code: 23MA1BSMCS
Course: Mathematical Foundation for Computer Science Stream – 1

Unit 4: Congruence’s and its Applications

4. $x \equiv 2 \pmod{5},\ x \equiv 3 \pmod{7},\ x \equiv 1 \pmod{8}$
5. $x \equiv 6 \pmod{11},\ x \equiv 13 \pmod{16},\ x \equiv 9 \pmod{21},\ x \equiv 19 \pmod{25}$ 5.

6. Brahmagupta has a basket full of eggs. When he takes the eggs out of the basket 2 at a time, there is 1 egg left over. When he takes them out 3 at a time, there are 2 eggs left over. Likewise, when he takes the eggs out 4, 5, and 6 at a time, he finds remainders of 3, 4, and 5, respectively. However, when he takes the eggs out 7 at a time, there are no eggs left over. What is the least amount of eggs that could be in Brahmagupta's basket?

7. A general counts the number of surviving soldiers of a battle by aligning them successively in rows of certain sizes. Each time, he counts the number of remaining soldiers who failed to fill a row. The general initially had 1200 soldiers before the battle; after the battle, aligning them in rows of 5 soldiers leaves 3 remaining soldiers; aligning them in rows of 6 soldiers leaves 3 remaining soldiers; aligning them in rows of 7 soldiers leaves 1 remaining soldier; aligning them in rows of 11 soldiers leaves 0 remaining soldiers. How many soldiers survived the battle?

8. There are certain things whose number is unknown. When this number is 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 is the number of the things?

V. Find the integer solution of following Diophantine equations.

1. $6x + 11y = 41$
2. $7x + 4y = 59$
3. $12x + 17y = 299$
4. $172x + 20y = 1000$
5. $20x + 16y = 500$
6. When Mrs.Brown cashed her cheque, the absent minded teller gave her as many cents as she should have dollars, and as many dollars as she should have cents. Equally absent minded Mrs, Brown left with the cash without noticing the discrepancy. It was only after she spent 5 cents that she noticed now she had twice as much money as she should. What was the amount of her cheque?

VI. Solve the following polynomial congruence’s

1. $x^3 + 2x + 2 \equiv 0 \pmod{49}$
2. $x^3 + 3x + 5 \equiv 0 \pmod{9}$
3. $x^3 + 5x + 1 \equiv 0 \pmod{27}$

B.M.S. COLLEGE OF ENGINEERING, BENGALURU
DEPARTMENT OF MATHEMATICS

For the Course Code: 23MA1BSMCS
Course: Mathematical Foundation for Computer Science Stream – 1

Unit 4: Congruence's and its Applications

4. $x^3+x+2\equiv 0\pmod{36}$
5. $x^2\equiv 0\pmod{12}$
6. $x^2\equiv 1\pmod{30}$
7. $x^3+x+3\equiv 0\pmod{25}$
8. $x^2\equiv 9\pmod{16}$
9. $x^3+4x\equiv 12\left(\bmod 7^3\right)$

Euler's Theorem: If a and n are co-primes then $a^{\phi(n)}\equiv 1\ (\bmod n)$, where $\phi(n)$ Euler's totient function.

Fermat's Little Theorem: If p is a prime number then for any integer a, $a^p\equiv a\ (\bmod p)$. That is p divides a^p-a.

Wilson's Theorem: The integer $p>1$ is said to be prime number if and only if

$$(p-1)!\equiv -1(\bmod p).$$

VII. Euler's Theorem, Fermat's Little Theorem and Wilson Theorem:

1. Using FLT show that $8^{30}-1$ is divisible by 31
2. Find the remainder when 72^{1000} is divisible by 31
3. Find the remainder when 4^{2414} is divisible by 21
4. Find the remainder when 5^{446} is divisible by 12
5. Find the value of a for which $24^{1947}\equiv a\pmod{17}$
6. Find the value of a for which $2^{2025}\equiv a(\bmod 15)$
7. Show that $2^{340}\equiv 1\pmod{11}$
8. Show that $2^{340}\equiv 1\pmod{31}$
9. Using FLT show 42 divides n^7-n
10. Using Wilson theorem show that 17 is prime
11. Using WT show that $10!+1$ is divisible by 11
12. For prime number 71 show that $63!\equiv -1\pmod{71}$

VIII. Applications of congruence's : RSA Algorithm

1. Generate the public and private keys to encrypt certain message using primes 3 and 11.
2. Encrypt the message STOP using RSA with key $(2537,13)$ using the prime number 43 and 59.
3. Decrypt the message 09810461 using the key $(937,2537)$
4. Encrypt the following messages (i) UPLOAD (ii) ATTACK
5. Decrypt the message 1420061413011694.