EXAMPLES ON MODULAR ARITHMETIC

VARUN S 21PC25

5)Prove that 6 | a(a+1)(2a+1) for every $a \in N$.

- We know that the sum of first n^2 natural numbers is n(n+1)(2n+1)/6. So now we have to prove 6 divides n(n+1)(2n+1) or in this case a(a+1)(2a+1), where n=a.
- Firstly, let us check the number of residue classes for modulo 6. There are 6 residue classes for modulo 6, namely [0],[1],[2],[3],[4],[5].
- Let us assume $f(x) = x(x+1)(2x+1)$ be some polynomial.
- If $f(a) = 0$ for some $a \in N$ then $f(a) = 0 \pmod n$ for every $n \in N$.

$f(0) = 0*1*1 \equiv 0 \pmod 6$

$f(1) = 1*2*3 = 6 \equiv 0 \pmod 6$ as $6 \mid 6 - 0$

$f(2) = 2*3*5 = 30 \equiv 0 \pmod 6$

$f(3) = 3*4*7 = 84 \equiv 0 \pmod 6$

$f(4) = 4*5*9 = 180 \equiv 0 \pmod 6$

$f(5) = 5*6*11 = 330 \equiv 0 \pmod 6$

- Thus, since f(x) takes zero value in all the residue classes under modulo 6 operation, we can conclude that f(x) is divisible by 6 or 6 divides f(x).
- Therefore, 6 | a(a+1)(2a+1).

5)Prove that 6 | a(a+1)(2a+1) for every $a \in \mathbb{N}$.

- In other way, we can say that 6 | k if and only if 2 | k and 3 | k, for some k.
- So, it is enough to check that f(x) = x(x+1)(2x+1) takes zero value on all residue classes under modulo 2 and modulo 3.
- Mod 2 has 2 residue classes [0],[1].

  $f(0) = 0*1*1 \equiv 0 (\mathrm{mod}\ 2)$

  $f(1) = 1*2*3 \equiv 0 (\mathrm{mod}\ 2)$
- Mod 3 has 3 residue classes [0],[1],[2].

  $f(0) = 0*1*1 \equiv 0 (\mathrm{mod}\ 3)$

  $f(1) = 1*2*3 \equiv 0 (\mathrm{mod}\ 3)$

  $f(2) = 2*3*5 \equiv 0 (\mathrm{mod}\ 3)$
- Thus, 6 | f(x) since , 2 | f(x) and 3 | f(x).

7)Prove that $f(x) = x^5 – x^2 + x -3$ has no integer root.

- We know that , if $f(a) = 0$ for some $a \in N$ then $f(a) \equiv 0 \pmod{n}$ for every $n \in N$.
- If there is some n1 in N such that f(a) is not congruent to 0(mod n1) for any a modulo n1,then f(a) is not equal to zero for any $a \in N$.
- To prove f(x) has no integer root, it is enough if we just give a counter example.
- Let us take n1 = 4.

$$f(0) = -3 \equiv 1 \pmod{4}$$

$$f(1) = -2 \equiv 2 \pmod{4}$$

$$f(2) = 32 – 4 + 2 – 3 = 27 \equiv 3 \pmod{4}$$

f(3) :

$$3^5 = 3^2 * 3^2 * 3 \qquad [\, 3^2 = 9 \equiv 1 \pmod{4} \,]$$

$$= 1*1*3 = 3$$

$$f(3) = 3 – 1 + 3 – 3 \equiv 2 \pmod{4}$$

- Thus, since no residue classes have 0 value, we can conclude that f(x) has no integer root.

- If we take n1 = 2,

  $f(1) = 1 – 1 + 1 - 3 = -2 \equiv 0 \pmod{2}$

  Thus, 1 is a root.

- If we take n1 = 3,

  $f(0) = -3 \equiv 0 \pmod{3}$

So , cases n1 = 2 and n1 = 3 will provide us with a root, so it will not disprove the statement.

<u>POINTS:</u>

1) Sometimes, we would have to substitute large value for n1 in order to disprove any given statement.
2) If we get root for any one value of n , do not assume it has roots for all values of n.
3) In some polynomials, all n values might have roots.