Tutorial-1

1. We have $b^2 \equiv 0 \pmod{a^3}$ as $a^3 | b^2$ is given.

So, we can say $a^3 | b^2$ & $a | a^3$

So, $a | b^2 \Rightarrow b^2 \equiv 0 \pmod{a}$ - (1)

Also, $a^2 \equiv a^2 \pmod{a}$ - (2)

Now, (1) - (2) $b^2 - a^2 \equiv -a^2 \pmod{a}$

$$\left(\frac{b}{a} - 1\right)\left(\frac{b}{a} + 1\right) \equiv 0 \pmod{a}$$

$$\left(\frac{b}{a} - 1\right) \equiv 0 \bmod a$$

$$\frac{b}{a} \equiv 1 \bmod a \quad - (iii)$$

Also $a \equiv a \pmod{a}$ - (iv)

Multiplying (iii) & (iv), $b \equiv a \bmod a$

So $a | b$ Proved

2. Given, $q | 2^p - 1$

$2^p \equiv 1 \bmod q$ (1)

We know from, Fermat's theorem, $a^{p-1} \equiv 1 \bmod p$ for prime p

So $2^{q-1} \equiv 1 \bmod q$ (2)

From (1) & (2) $2^{q-1-p} \equiv 1 \bmod q$

Now $q - 1 - p \geq 0$

$\Rightarrow p < q$ Proved

3

Given, $n > 1$ is an odd integer

To prove $\phi(2n) = \phi(n)$

We know $\phi(pq) = \phi(p)\phi(q)$ if $\gcd(p,q) = 1$

Here $p = 2$ & $q = n$ & n is odd & $\gcd(2,n) = 1$

$$\phi(2n) = \phi(2)\,\phi(n)$$

$$\phi(2n) = \phi(n)$$ Proved

4 Given, $a^2 + 2 \equiv 0 \bmod (2a-1)$

Multiplying by 4, So $4a^2 + 8 \equiv 0 \bmod (2a-1)$

$$4a^2 - 1 + 9 \equiv 0 \bmod (2a-1)$$

$$(2a-1)(2a+1) + 9 \equiv 0 \bmod (2a-1)$$

$$\Rightarrow 9 \equiv 0 \bmod (2a-1)$$

So $(2a-1) \mid 9$

Now $(2a-1)x \equiv 9$ where a & x are integers

$$2a-1 \leq 9$$

Now, $2a-1 \equiv 1 \Rightarrow a = 1$ & $a = 0$

$2a-1 = \pm 3 \Rightarrow a = \pm 3$

$a = 2$ & $a = -1$

$\Rightarrow 2a-1 = \pm 9 \Rightarrow a = 5$ & $a = -4$

So, $\boxed{a = -4, -1, 0, 1, 2, 5}$

(5)

Given, $n>0$ & $a>1$.

To prove, $\gcd\left(\frac{a^n-1}{a-1}, a-1\right) = \gcd(a-1, n)$

$\gcd((a^n-1/a-1, a-1)) = \gcd(a^{n-1}+a^{n-2}+a^{n-3}+\dots a+1, a-1)$

$\gcd[(a^{n-1}-1)+(a^{n-2}-1)\dots+(a^2-1)+(a-1)+1](n+1), a-1)$

$= \gcd((a^{n-1}-1)+(a^{n-2}-1)\dots+(a^2-1)+(a-1)+n, a-1)$

$= \gcd(a-1, ((a^{n-1}-1)+(a^{n-2}-1)\dots+(a^2-1)+(a+1)+n) \bmod (a-1)$

$= \gcd(a-1, n)$ Proved

b) Given, p is prime

To prove, $\sqrt{p}$ is irrational.

Let's prove by contradiction, Let $\sqrt{p}$ be a rational no.

$\sqrt{p} = \frac{a}{b} \Rightarrow p = \frac{a^2}{b^2} \Rightarrow a^2 = pb^2 \Rightarrow p$ divides a^2

So p divides a, let $a = pk$ — (1)

$(pk)^2 = pb^2 \Rightarrow p^2k^2 = pb^2$

$\Rightarrow b^2 = pk^2$, Therefore, p divides b^2. But $b^2 = b \cdot b$

So p divides b.

Thus proved by contradiction.

(7)

$42x \equiv 12 \pmod{90}$

gcd(42, 12) = 6 so 6 sol's exists

Reducing the eq^n, we get, $7x \equiv 2 \pmod{15}$

Using extended Euclidean Algorithm

for $x = 11$, we get $= 2 \bmod 15$

for $x = 26$, we get $12 \bmod 90$

for $x = 41$, we get $12 \bmod 90$

for $x = 56$ we get $12 \bmod 90$

for $x = 71$, we get $12 \bmod 90$

for $x = 86$ we get $12 \bmod 90$

So, $x \equiv 11, 26, 41, 56, 71, 86$ Ans

(8) $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$ where $n \in \mathbb{R}$

$$\frac{y+x}{xy} = \frac{1}{n}$$

$$nx + ny = xy$$

$$\Rightarrow x(n-y) - n(n-y) = n^2$$

$$(n-x)(n-y) = n^2$$

So $n^2 = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_n}$

So the no. of solutions $(a_1+1)(a_2+1) \cdots (a_n+1)$

(9)

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{84}$$

$$\frac{x+y}{xy}=\frac{1}{84}$$

$$xy-84(x+y)=0$$

$$(x-84)(y-84)=(84)^2$$

So $A \times B = (84)^2$

Factors of $(84)^2 = 2^4 \times 3^2 \times 7^2$

So possible pairs $= (4+1)(2+1)(2+1)$

$= 45$ Ans

(10)

$x \equiv 3 \bmod 7$

$x \equiv 11 \bmod 18$

$x \equiv 5 \bmod 24$

$x \equiv 11 \bmod 18 \Rightarrow x \equiv 11 \bmod 9$

$x \equiv 11 \bmod 2$

$x \equiv 5 \bmod 24 \Rightarrow x \equiv 5 \bmod 3$

$x \equiv 5 \bmod 8$

$\Rightarrow x \equiv 2 \bmod 3$

$x \equiv 5 \bmod 8$

Thus we have

$x \equiv 2 \bmod 9$

$x \equiv 5 \bmod 8$

$x \equiv 3 \bmod 7$

By chinese Remainder theorem,

$N = 9 \times 8 \times 7 = 504$

$N_1 = 56 \quad N_2 = 63 \quad N_3 = 72$

So, $x = 2 \times 56 \times 56^{-1} \bmod 9 + 5 \times 63 \times 63^{-1} \bmod 8 + 3 \times 72 \times 72^{-1} \bmod 7 \bmod 504$

$= 101 \bmod 504$ Ans

(11) Given, $a^{n-1} \equiv 1 \pmod{n}$ $\forall$ a relatively prime to n

To prove, n is carmichael no. iff $\lambda(n) \mid (n-1)$

$$a^{n-1} \equiv 1 \bmod n$$

Let $n-1 = m$, so $a^m \equiv 1 \bmod n$

proof by contradiction

Let $\lambda(n) = x \cdot m + y$

$$a^y = a^{0} \cdot 1$$

We know,

$$a^y = \left[a^{\lambda(n)}\right]^x \cdot a^y$$

$$= a^m$$

Hence $\lambda(n) \mid (n-1)$ proved by contradiction

(13) To prove, for any prime $p = 4k+1$,

$(2k)!$ is a square root of -1 modulo p.

Using Wilson Theorem, $(p-1)! \equiv -1 \bmod p$

If p is prime, $(4k+1-1)! \equiv -1 \bmod p$

$(4k)! \equiv -1 \bmod p$

Let $x = 2k$

$(2x)! \equiv -1 \bmod p$

$1 \cdot 2 \cdot 3 \cdots x(x+1)(x+2)\cdots(2x-2)(2x-1)(2x) \equiv -1 \bmod p$.

$(x!)^2 (-1)^x \equiv -1 \bmod p$

Putting $x = 2k$

$(x!)^2 (-1)^{2k} \equiv (-1) \bmod p$

$(2k!)^2 \equiv -1 \bmod p$ Proved

AFFINE:

KEY: A=5,B=8

PLAINTEXT

THEARTOFWRITINGSECRETMESSAGESWHICHISINTELLIGIBLETOTHOSEWHOAREINPOSS
ESSIONOFTHEKEYANDUNINTELLIGIBLETOALLOTHERSTHEUSEFULNESSOFSUCHMESSAG
ESESPECIALLYINTIMEOFWARISOBVIOUS.ONTHEOTHERHANDTHEIRSOLUTIONMAYBEA
MATTEROFGREATIMPORTANCETOTHOSEFROMWHOMTHEKEYISCONCEALED

ENCRYPTED TEXT:
ZRCIPZAHOPWZWVMUCSPCZQCUUIMCUORWSRWUWVZCLLWMWNLCZAZRAUCORAIPC
WVFAUUCUUWAVAHZRCGCYIVXEVWVZCLLWMWNLCZAILLAZRCPUZRCEUCHELVCUU
AHUESRQCUUIMCUCUFCSWILLYWVZWQCAHOIPWUANJWAEURAVZRCAZRCPRIVXZRC
WPUALEZWAVQIYNCIQIZZCPAHMPCIZWQFAPZIVSCZAZRAUCHPAQORAQZRCGCYWUSA
VSCILCX

SIMPLE SUBSTITUTION:

PLAINTEXT:

COLLEGELIFEISAREMARKABLEANDESSENTIALTIMEINAPERSONLIFEANDEVERY
ONESHOULDENJOYIT.COLLEGELIFETEACHESUSMANYTHINGSANDBUILDSOURCO
NFIDENCETOFACETHENEWCHALLENGESANDSTRUGGLESINOURFUTUREINSTEAD
OFJUSTFOCUSSINGONTHESTUDYAPERSONMUSTPARTICIPATEINOTHERACTIVITIE
SANDSOCIALISEASMUCHASPOSSIBLEASALLTHESETHINGSHELPINTHEOVERALLD
EVELOPMENTOFAPERSON

Key: ZEBRACDFGHIJKLMNOPQSTUVWXY

CIPHERTEXT:

BMJJADAJGCAGQZPAKZPIZEJAZLRAQQALSGZJSGKAGLZNAPQMLJGCAZLRAUAP
XMLAQFMTJRALHMXGS.BMJJADAJGCASAZBFAQTQKZLXSFGLDQZLRETGJRQMT
PBMLCGRALBASMCZBASFALAVBFZJJALDAQZLRQSPTDDJAQGLMTPCTSTPAGLQS
AZRMCHTQSCMBTQQGLDMLSFAQSTRXZNAPQMLKTQSNZPSGBGNZSAGLMSFAPZ
BSGUGSGAQZLRQMBGZJGQAZQKTBFZQNMQQGEJAZQZJJSFAQASFGLDQFAJNGL
SFAMUAPZJJRAUAJMNKALSMCZNAPQML

Q12. $n = \prod_{i=1}^{m} p_i$

$$\lambda(n) = \text{lcm}\{\lambda(p_1), \lambda(p_2), \cdots, \lambda(p_m)\}$$

$$= \text{lcm}\{(p_1-1), (p_2-1), \cdots (p_m-1)\}$$

$$= \min\{k_1(p_1-1), k_2(p_2-1), \cdots k_m(p_m-1)\}$$

where $k_1, k_2, \cdots k_m$ are some constants.

$$= \min\{k_1(p_1-1) : k_i(p_i-1) = k_1(p_1-1), i=1,2,\cdots m\}.$$