CS4042D – Introduction to Information Security.

Assignment - 1.

Bhukya Vasanth Kumar
B180441CS.

Answers:

1). $\gcd(241, 743) = 743x + 241y$.

$\Rightarrow \gcd(241, 743) \Rightarrow 743 = 3 \cdot 241 + 20$ — (1).

$\gcd(20, 241) \Rightarrow 241 = 20 \cdot 12 + 1$ — (2).

$\boxed{\gcd(1, 20) = 1}$ — (3).

From (3)

So, $\gcd(241, 743) = 1$.

as (2)

$241 - 12 \cdot 20 = 1$

$241 - 12(743 - 3 \cdot 241) = 1$.

$-12 \cdot 743 + 37 \cdot 241 = 1$.

$\{x = -12\}$
$\{y = 37\}$.

(2) $(a, 4) = 2 \rightarrow 2 \mid a, \ 4 \nmid a$.

$(b, 4) = 2 \rightarrow 2 \mid b, \ 4 \nmid b$.

So, we can write.

$a = 2(2n+1) \quad b = 2(2m+1)$

$a + b = 2(2n+1 + 2m+1)$

$a + b = 4(m+n+1)$

$4 \mid a+b \quad 4 \mid a \Rightarrow \gcd(a+b, 4) = 4$

$\therefore$ Hence proved.

(3) If $n \to$ odd

It can be represented in form like:

$$n = 2t + 1$$

$$n^2 = (2t+1)^2$$

$$n^2 = 4t^2 + 4t + 1$$

$$n^2 - 1 = 4t^2 + 4t$$

$$n^2 - 1 = 4(t^2 + t)$$

$\therefore$ Here, $t^2 + t \to$ even always whether $t \to$ even or $t \to$ odd

$$n^2 - 1 = 4(2x)$$

$$n^2 - 1 = 8x$$

$\therefore 8 \mid n^2 - 1$, Hence proved

(4) Using FTA,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

Suppose that the primes $(p_1 p_2 \cdots p_r)$ in the factorization of n^2 occur to an even power are $(p_1 p_2 \cdots p_r)$.

and

let power of p_i in the factorization be $2b_i$

and

Suppose that the primes that occur to our odd power are $q_1 q_2 \cdots q_s$ and let the power of q_j in the factorization be $2c_j + 1$

then

$$n = \left(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k} q_1^{c_1} q_2^{c_2} \cdots q_l^{c_l}\right)^2 (q_1 \cdots q_s)$$

That is the factorization of n^2 is to square and a square free integer.

(6) If $n \to 5q+1$, for $\forall q$ is +ve int

$\Rightarrow n = 5q+1$

$n^2 = (5q+1)^2$

$\Rightarrow 25q^2 + 10q + 1 = n^2$

let $5q^2 + 2q \to m$

$n^2 \Rightarrow 5m+1 \to \{$ where m is same integer $\}$

Hence n & n^2 are of same form

(9) The only even prime number $\Rightarrow 2$.

$2 \neq 3K+1$

Thus any prime of the form $3K+1$ must be odd.

$\Rightarrow 3K$ must be even

$\Rightarrow K$ must be even.

$\Rightarrow K = 2m$

Then $3K+1 = 3(2m)+1$

$\to 6m+1$

So, any prime of form $3K+1$ is also of form $6m+1$.

(10) $a^2 \equiv b^2 (p)$

$p \mid a^2 - b^2$

$\Rightarrow p \mid (a+b)(a-b)$ — (1)

Using theorem $p \mid ab \Rightarrow p \mid a$ or $p \mid b$ in (1)

$p \mid (a+b)$ or $p \mid (a-b)$.

(10). Since $n \rightarrow$ composite

we know that $n = ab \quad 1 < a, b < n$.

If $a \neq b$ then

a, b appears separate terms in $(n-1)!$.

$\therefore n \mid (n-1)!$ {as $ab \mid (n-1)!$}.

If $a = b$

So, $n = a^2$ a is term in $(n-1)!$.

Since $n > 4$, $a > 2$

$\Rightarrow a^2 > 2a$

$\Rightarrow n > 2a$

$\Rightarrow 2a$ is also a term in $(n-1)!$

Hence $(n-1)!$ is divisibly by $(2a)(a)$

$2a^2 \mid (n-1)!$

$2n \mid (n-1)!$.

$\hookrightarrow \Rightarrow n \mid (n-1)!$ Hence proved.

(11) Say

$p - r \equiv -r \pmod p \quad \Rightarrow r \equiv -(p-r)$

For uniqueness

$r \leq p - r$ or $2r \leq p$

$\Rightarrow r \leq p/2$.

So, $1 \leq r \leq \frac{p-1}{2}$ as p is odd

Putting $r = 1, 2, 3 \cdots \frac{p-3}{2}, \frac{p-1}{2}$ we get.

$1 \equiv -(p-1)$

$2 \equiv -(p-2)$

$\frac{p-3}{2} \equiv \frac{p+3}{2} \cdots \frac{p-1}{2} \equiv \left(\frac{p+1}{2}\right)$

So there are $(p-1)$ pairs so,

$$(p-1)\,1 = (-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2}\right)!\right)^2$$

Using Wilson's theorem

$$(-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}$$

If $p \equiv 3 \pmod 4$.

$p \equiv 4t+3$.

$\frac{p-1}{2} = 2t+1 \rightarrow$ which is odd,

So, $(-1)^{\frac{p-1}{2}} = -1$.

$$\Rightarrow \left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv 1 \pmod p$$

$$\boxed{\left(\left(\frac{p-1}{2}\right)!\right) = \pm 1 \pmod p}$$

$\hookrightarrow$ Hence proved.

(12) 37^{39997}.

for last 3 digits, $37^{39997} \div 1000$

$(37, 1000) = 1$, we can euler's theorem

$\phi(1,000) = (2^3-2^2)(5^3-5^2) = 400$.

$37^{400} \equiv 1 \pmod{1000}$

$\Rightarrow (37^{400})^{99} \equiv 1 \mod 1000$

$37^{399600} \equiv 1 \mod 1000$

$\Rightarrow 37^{100} \cdot 37^{399600} \equiv 37^{100} \cdot 1 \pmod{1000}$

$$\Rightarrow \boxed{37^{399700} \Rightarrow 1 \pmod{1000}}$$

$\{\because 37^{100} \pmod{1000} = 1 \pmod{1000}\}$.

Using ① 37^{200} on both sides

$$37^{399900} \equiv 1 \pmod{1000}$$

multiply 37^{97} both sides,

$$37^{399997} \equiv [37^{97} \pmod{1000}] \cdot [1 \bmod (1000)]$$

$$\equiv 317 \bmod (1000)$$

Hence, last 3 digits of 37^{399997} is 317.

(3) let p be prime and $1 \le K \le (P-1)$

$$\binom{P}{K} = \frac{P!}{K!(P-K)!}.$$

This implies.

$$P! = K!(P-K)! \binom{P}{K}$$

and in particular that p divides $K!(P-K)!\binom{P}{K}$

As p is prime this implies.

$$P \mid K! \cdot P \mid (P-K)! \quad \text{or} \quad P \mid \binom{P}{K} \text{ — ③}$$

But $K < P \Rightarrow P \nmid K!$ — ①.

As $K \ge 1$ we have $(P-K) < P \Rightarrow P \nmid (P-K)!$ — ②

from ①, ② and ③ we conclude that.

$$\boxed{P \mid \binom{P}{K}}$$

Hence proved

(14) Let the number be 'n' with $k=1$, this is just exactly the definition of the ϕ fn.

Now lets assume that this eq. holds for some k and try to prove it for $k+1$.

The no of int $1 \le n \le m(k+1)$ that satisfy $(n,m)=1$ is the sum of following :

$$\#\{1 \le n \le mk \mid (n,m)=1\} \quad \#\{mk+1 \le n \le m(k+1) \mid (n,m)=1\}.$$

By our inductive hypothesis, the first sumn and is $k\phi(m)$.

Now to compute the second summand.

For any n such that $mk+1 \le n \le m(k+1)$

we have that $(n,m) = (n-mk, m)$.

Since any common factor of n and m must divide $n-mk$ and any common factor of $n-mk$ and m must divide $n-mk+mk=n$

$$n \in \{mk+1 \le n \le m(k+1) \mid (n,m)=1\} \iff n-mk \in \{1 \le n \le mk \mid (n,m)=1\}.$$

Since the size of right set is by definition $\phi(m)$, so is the size of the left set.

$\therefore$ above sum is $k\phi(m) + \phi(m) \Rightarrow (k+1)\phi(m)$.

So, it is true for $(k+1)$ implies that it is true $\forall k$.

$\therefore$ Hence proved.

7 (i) Divisibility by 9.

Let $a = a_n, a_{n-1} \cdots a_2 a_1$ be an integer

{ ∵ Here $a_1, a_2 \cdots a_n$ are digits }

$$a = a_1 + (10)^1 a_2 + (10)^2 a_3 + \cdots + (10)^{n-1} a_n.$$

$$= a_1 + 10a_2 + 100a_3 + \cdots$$

$$= a_1 + (a_2 + 9a_2) + (a_3 + 99a_3) + \cdots$$

$$a = (a_1 + a_2 + a_3 + \cdots) + 9(a_2 + 11a_3 + \cdots) \quad -(1)$$

$$a = s + 9(a_2 + 11a_3 + \cdots)$$

$$a - s = 9(a_2 + 11a_3 + \cdots)$$

$$9 \mid (a - s) \quad -(2)$$

Given s (sum of digits) is divisible by 9.

i.e $9 \mid s$ —(3)

from (2) and (3)

$$9 \mid [(a-s) + s]$$

$$\Rightarrow 9 \mid a \rightarrow \text{Integer is divisible by } 9.$$

∴ Hence proved.

(ii) Divisibility by 3.

From (2) → $3 \mid (a-s)$ —(5)

Given - s (Sum of digits) is divisible by 3.

$\Rightarrow 3 \mid 5$ —(4)

From (5) & (4)

$$3 \mid [(a-s) + s]$$

∵ $3 \mid a \rightarrow$ Integer divisible by 3.

∴ Hence proved.