Krithikha Balamurugan

U19CS076

Krithikha

Tutorial - 6
Number Theory

① Let $a = 11, p = 17$ pta then fermat's theorem

$$a^{p-1} \equiv 1 \pmod p$$
$$11^{17-1} \equiv 1 \pmod{17}$$

but $104 = 6 \cdot 16 + 8$

$$11^{104} = 11^{6 \cdot 16 + 8} = ((11)^{16})^6 \, 11^8 \pmod{17}$$
$$= 1^6 (11^2)^4 \pmod{17}$$
$$= 2^4 \pmod{17}$$
$$= 16 \pmod{17}$$
$$11^{104} \equiv -1 \pmod{17}$$

So $11^{104} + 1 \equiv 0 \pmod{17}$

i.e $17 \mid 11^{104} + 1$

②a) Since $\gcd(4, 35) = 1$ then $\gcd(4, 5) = \gcd(a, 7) = 1$
Then by fermate theorem

$a^{p-1} \equiv 1 \pmod p$ and $a^6 \equiv 1 \pmod 7$
$a^4 \equiv 1 \pmod 5$ $\quad a^6 \equiv 1 \pmod 7$

$(a^4)^3 \equiv 1 \pmod 5$ and $(a^6)^2 \equiv 1 \pmod 7$
Thus $a^{12} \equiv 1 \pmod{35}$ since $\gcd(5, 7) = 1$

b) Since $42 = 7 \cdot 3 \cdot 2$, $\gcd(a, 42) = 1$, then
$\gcd(3, 2) = 1$

Thus by fermat theorem $a^6 \equiv 1 \pmod 7$.
$a^2 \equiv 1 \pmod 3$, and $a \equiv 1 \pmod 2 \Rightarrow a^6 \equiv 1 \pmod 3$
and $a^6 \equiv 1 \pmod 2$
Since $\gcd(9, 42) = 1$ then a is odd.

U19CS076

So $a^2 \equiv 1 \pmod 8$

$\Rightarrow a^6 \equiv 1 \pmod 8$

Therefore $a^6 \equiv 1 \pmod{\text{lcm}(3,7,8)}$

$a^6 \equiv 1 \pmod{168}$

3) a). $15 = 3 \times 5$ by format theorem

$a^3 \equiv a \pmod 3$ & $a^5 \equiv a \pmod 5$

$\Rightarrow (a^3)^7 = a^7 \pmod 3 \Rightarrow a^{21} = (a^3)^2 a \bmod 3$

$\Rightarrow a^{21} \equiv a \pmod 3$ and $a^{21} = (a^5)^4 . a = a^5 \equiv a \pmod 5$

Thus $a^{21} \equiv a \pmod{\text{lcm}(5,3)}$

$\Rightarrow a^{21} \equiv a \pmod{15}$

b) Using format theorem

$a^9 = (a^3)^3 = a^3 \equiv a \pmod 3$

$a^9 \equiv a^5 . a^4 \equiv a^5 \equiv a \pmod 5$

$a^9 = (a^2)^4 . a = a^5 \equiv a^3 \equiv a^2 \equiv a \pmod 2$

Therefore, $a^9 \equiv a \pmod{3 \times 5 \times 2}$

$a^9 \equiv a \pmod{30}$

4) Proof :- Since $\gcd(a, 30) = 1 \Rightarrow \gcd(a,5) = 1$

So $a^{5-1} \equiv 1 \pmod 5$

$a^4 \equiv 1 \pmod 5$

Thus $a^4 + 59 \equiv 0 \pmod 5$

Also $\gcd(a,3) = \gcd(a,2) = 1$ then

$a^{3-1} \equiv 1 \pmod 3 \Rightarrow a^2 \equiv 1 \pmod 3$

So $a^4 \equiv 1 \pmod 3 \Rightarrow a^4 + 59 \equiv 0 \pmod 3$

Since $\gcd(a, 30) = 1$ then a is odd

So $a \equiv 1 \pmod 4$, $a \equiv 3 \pmod 4$

Then $a^4 \equiv 1 \pmod 4$ or $a^4 = 3^4 \equiv 1 \pmod 4$

So in both cases

$a^4 \equiv 1 \pmod 4 \Rightarrow a^4 + 59 \equiv 0 \pmod 4$

Therefore 1, 2, 3 we have

$a^4 + 59 \equiv 0 \pmod{3 \cdot 4 \cdot 5 = 60}$

So $\boxed{60 \mid a^4 + 59}$

(5). We want to find the units digit at 3^{100} by using fermat theorem

Since gcd(3, 5) = 1 and gcd(3, 2) = 1 then we can use fermat theorem

$3^4 \equiv 1 \pmod 5$

so $(3^4)^{25} \equiv 3^{100} \equiv 1^{25} \equiv 1 \pmod{25}$

$3^{2-1} \equiv 3 \equiv 1 \pmod 3$

$3^{100} \equiv 1^{100} \equiv 1 \pmod 2$

Thus, $3^{100} \equiv 1 \pmod{10}$

Therefore the units digit of 3^{100} is $\boxed{1}$

(6). According to fermat theorem if p is a prime and a is an integer and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod p$.

Hence using above thm, we get that

$a^{7-1} \equiv 1 \pmod 7$

$a^6 \equiv 1 \pmod 7$

$a^6 - 1 = 7k$ where k is integer

Since k is integer $(a^3 - 1)$ or $(a^3 + 1)$ is divisible by 7.

(7) a) Suppose a and b are integers not divisible by prime p.

U19CS076

Then by fermat theorem, we know that $a^{p-1} \equiv 1 (\bmod p)$ & $b^{p-1} \equiv 1 (\bmod p)$

Multiplying a an either sides of first congruence, b on either sides of second congruence and subtracting we get

$$a^p - b^p \equiv (a-b) (\bmod p)$$

Using hypothesis that $a^p \equiv b^p (\bmod p)$ or $a^p - b^p \equiv a \bmod p$ we get

$$0 \equiv a - b (\bmod p)$$

$$a \equiv b (\bmod p)$$

(8) b) If $a^p \equiv b^p (\bmod p)$ then $a^p \equiv b^p (\bmod p^2)$

By fermat theorem

$$p \mid a-b \rightarrow a \equiv b \text{ in modulo } p$$

$$\frac{a^p - b^p}{a-b} = (a^{p-1} + b a^{p-2} + \dots b^{p-2} a + b^{p-1})$$

$$= (b^{p-1} + b b^{p-2} b + \dots + b^{p-2} b + b^{p-1})$$

$$= p b^{p-1} \equiv 0 \text{ in modulo } p$$

Since $\frac{a^p - b^p}{a-b}$ and $a-b$ are divisible by p

The product $a^p - b^p$ is divisibly by p^2.

(8) Use Fermat's Theorem to prove that if p is an odd prime then

a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \dots (p-1)^{p-1} \equiv -1 (\bmod p)$

as $\forall i \in \{1, 2, \dots (p-1)\}$

$\gcd(i, p) = 1$ i.e. $p \nmid i$

we can fermat theorem.

U19CS076

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

$= 1 \bmod p + 1 \bmod p \; \cdots \; 1 \bmod p$ (p-1 times)

$= (p-1)(1 \bmod p)$

$= (p-1)(1 \bmod p)$

$\therefore 1^{p-1} + 2^{p-1} + 3^{p-1} \cdots (p-1)^{p-1} = (p-1) \bmod p$

$= -1 \bmod p$

$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots (p-1)^{p-1} \equiv -1 \bmod p$

b) $1^p + 2^p + 3^p + \cdots (p-1)^p = 0 \pmod p$

Since $\forall i \in \{1, 2, 3, \ldots p-1\}$

$\gcd(i, p) = 1$

we can use Fermat theorem

$a^p \equiv a \bmod p$ ($\because$ p is odd prime)

$LHS = 1^p + 2^p + 3^p + \cdots (p-1)^p$

$= 1 \bmod p + 2 \bmod p + 3 \bmod p + \cdots (p-1) \bmod p$

$= \frac{p(p-1)}{2} \bmod p$

$(p-1)$ is divisible by 2 ($\because$ p is odd prime)

$\Rightarrow \frac{p(p-1)}{2} \bmod p = 0 \bmod p$

LHS = RHS → Hence proved.

Q9 Confirm the following integers are absolute pseudo primes.

a) $1105 - 5 \cdot 13 \cdot 17$

Note that $1105 = 5 \times 13 \times 17$

If $1105 | a$ then $1105 | a^{1105} \Rightarrow 1105 | a^{1105}$ -

$a^{1105} = a \pmod{1105}$

Scanned with CamScanner

If $1105 \nmid a$ then $5 \nmid a$, $13 \nmid a$, $17 \nmid a$ then by Fermat theorem

$$a^4 \equiv 1 \pmod 5, \quad a^{12} \equiv 1 \pmod{13}, \quad a^{16} \equiv 1 \pmod{17}$$

$$a^{1104} = (a^4)^{276} \equiv 1 \pmod 5$$
$$a^{1104} = (a^{12})^{92} \equiv 1 \pmod{13}$$
$$a^{1104} \equiv (a^{16})^{69} \equiv 1 \pmod{17}$$
$$\therefore a^{1104} \equiv 1 \pmod{5 \times 13 \times 17}$$
$$a^{1105} \equiv a \pmod{1105} \quad \text{—(2)}$$

From (1), (2). we conclude that 1105 is absolute pseudo prime.

b) $2465 = 5 \cdot 17 \cdot 29$

Note that $2465 = 5 \times 17 \times 29$

If $2465 \mid a$ then $2465 \mid a^{2465}$

$\Rightarrow 2465 \mid a^{2467} - a$

$\Rightarrow a^{2465} \equiv a \pmod{2465}$

If $2465 \nmid a$ then $5 \nmid a$, $17 \nmid a$, $29 \nmid a$ then by Fermat theorem.

$$a^4 \equiv 1 \pmod 5, \quad a^{16} \equiv 1 \pmod{17}, \quad a^{28} \equiv 1 \pmod{29}$$

$$a^{2464} = (a^4)^{616} \equiv 1 \pmod 5$$
$$a^{2464} = (a^{16})^{154} \equiv 1 \pmod{17}$$
$$a^{2464} = (a^{28})^{88} \equiv 1 \pmod{29}$$
$$a^{2464} = 1 \pmod{17 \times 29}$$
$$a^{2465} = a \pmod{2465}$$

From (1), (2) we conclude that 2465 is absolute pseudo prime.

(10). Find the remainder when 45! is divided by 17.

U19CS076

Using willison theorem which states that every prime p divides $(p-1)!+1$

$$(p-1)! \equiv -1 \pmod p$$

As 17 is a prime.

$$16! = -1 \pmod{17}$$
$$16(15)! = -1 \pmod{17}$$
$$(17-1)(15)! = -1 \pmod{17}$$
$$17(15)! - 15! = -1 \pmod{17}$$

We get $17(15!) \equiv 0 \pmod{17}$

So, $-15! \equiv -1 \pmod{17}$

$$15! \equiv 1 \pmod{17}$$

The remainder when 15! is divided by 17 is $\underline{\underline{1}}$.

(11). Arrange the integers 2, 3, 4 .... 21 in pairs a and b that satisfy $ab \equiv 1 \pmod{23}$

$p = 23$ i.e the prime number than its possible to divide the integers 2, 3, 4 ... 21 into $\frac{p-1}{2} = \frac{23-1}{2} = 10$

Pairs each ~~band~~ product of which is congruent to 1 modulo 23.

$$21 = (2\times12)\cdot(3\times8)\cdot(4\times6)\cdot(5\times14)\cdot(7\times10)$$
$$(13\times16)\cdot(9\times18)\cdot(17\times19)\cdot(15\times20)\cdot(11\times21)$$

$$= (1)^{10} \bmod 23$$

U19CS076

The integers are arranged in paired a & b,

$ab \equiv 1 \pmod{23}$

(12). Show that $18! \equiv -1 \pmod{437}$

Using fermat's theorem :-

$(p-1)! \equiv -1 \pmod{p}$

as $437 = 19 \times 23$

We apply above theorem seperrately

$(19-1)! \equiv -1 \bmod 19$

$18! \equiv -1 \bmod 19$

$(23-1)! \equiv -1 \bmod 23$

$22! \equiv -1 \bmod 23$

$22! = 22 \times 21 \times 20 \times 19 \times 18! \equiv (-1)(-2)(-3)(-4)$

$\equiv 24$

$\equiv 1 \bmod 23$

Since 23 and 19 are coprimes

$18! \equiv -1 \bmod (19 \times 23)$

$18! \equiv -1 \bmod 437$

Q13 Given a prime number p, establish the congruence

$(p-1)! \equiv (p-1) \pmod{1+2+\dots(p-1)}$

Proof by Wilson's theorem

$(p-1)! \equiv -1 \equiv p-1 \pmod{p}$ — ①

Scanned with CamScanner

U19CS076

$p \mid (p-1)! - (p-1)$

Now using the identify

$$1+2+\dots\dots+n = \frac{n(n-1)}{2}$$

$$\therefore 1+2+\dots\dots p-1 = \frac{p(p-1)}{2}$$

Since p is odd prime then $(p-1)$ is even,
So $\frac{p-1}{2}$ is integer.

But, $(p-1) \mid (p-1)! - (p-1)$

$$\therefore \left(\frac{p-1}{2}\right) \Big| (p-1)! - (p-1) \quad — ②$$

Since p is prime then

$\gcd\left(\frac{p-1}{2}, p-1\right) = 1$ from ① & ②

We have

$$\frac{p(p-1)}{2} \Big| (p-1)! - (p-1) \Rightarrow (p-1)! \equiv (p-1) \bmod \left(\frac{p(p-1)}{2}\right)$$