NUMBER THEORY ASSIGNMENT

SUBMITTED BY
NAME :- AMAN BHARDWAJ
E. No. :- 2019 SIY 7580

Q1. Prove that if $\gcd(a,b)=1$ and $a \mid bc$, then $a \mid c$

Sol^n Given :- (i) $\gcd(a,b)=1$

(ii) $a \mid bc$

To Prove :- $a \mid c$

Proof :- given $\gcd(a,b)=1$

$\Rightarrow$ This can be written as

$$aX + bY = 1 \quad \text{—— (I)}$$

multiply both sides by c

$$acX + bcY = c \quad \text{—— (II)}$$

take mod a both sides.

$$acX \bmod a + bcY \bmod a = c \bmod a$$

now $a \mid ac$ also given $a \mid bc$

$\Rightarrow$ $0 + 0 = c \bmod a$

$\Rightarrow$ $c \bmod a = 0$

$\Rightarrow$ $a \mid c$ Hence Proved

Q2. Prove that if a number is relatively prime to two numbers, then it is relatively prime to their product.

Sol^n :- Given - ~~g gcd (a~~

Let a be the number relatively Prime to b and c

$\gcd(a,b)=1$ and $\gcd(a,c)=1$

To Prove - a is relatively Prime to $b \cdot c$

$\Rightarrow \gcd(a,bc)=1$

Proof on next Page

Proof - as given $\gcd(a,b)=1$ & $\gcd(a,c)=1$

$\therefore$ these can be expressed as

$$aX + bY = 1 \quad \text{— (I)}$$

$$aP + cQ = 1 \quad \text{— (II)}$$

By Multiplying both terms (I) & (II)

we get $(aX+bY)(aP+cQ) = 1$ — (III)

Solving (III)

$$a^2(XP) + ac(XQ) + ab(YP) + bc(YQ) = 1$$

taking mod a both sides.

$\Rightarrow a^2(XP) \bmod a + ac(XQ) \bmod a + ab(YP) \bmod a + bc(YQ) \bmod a = 1$

$\Rightarrow \quad 0 + 0 + 0 + bc^{(YQ)} \bmod a = 1$

(as $a \mid a^2$, $a \mid ac$, $a \mid ab$)

$\Rightarrow (YQ)bc \equiv 1 \bmod a$

$\Rightarrow \gcd(a, bc) = 1$

$\Rightarrow$ a is relatively prime to bc

Q3 on Next Page

Q3 Prove $\gcd(2^m-1, 2^n-1) = 2^{\gcd(m,n)}$

Sol^n $\gcd(2^m-1, 2^n-1) = g$

$\Rightarrow 2^m - 1 = 0 \bmod g$

$\Rightarrow 2^m = 1 \bmod g$ — ①

similarly $2^n = 1 \bmod g$ — ⑪

now $\gcd(m,n) = am + bn$

in eq^n ① Power a both sides & eq ⑪ power b both side

$2^{am} \equiv 1 \bmod g$ $2^{bn} \equiv 1 \bmod g$

Multiply.

$2^{am+bn} \equiv 1 \bmod g$

$\Rightarrow 2^{am+bn} - 1 \equiv 0 \bmod g.$

$\Rightarrow g \mid 2^{am+bn} - 1 \Rightarrow g \mid 2^{\gcd(m,n)} - 1$ —— (111)

also g divides $2^m - 1$
and g divides $2^n - 1$ as g is gcd of both

$\Rightarrow$ Now we have to prove $2^{\gcd(m,n)} - 1 \mid g$ for both of them to be equal.

Q4 Prove $\gcd(a^2+m^2, (a-1)^2+m^2)=1$ if $\gcd((2a-1), 4m^2+1)=1$

Sol^n. Given - $\gcd[(2a-1), (4m^2+1)] = 1$ — ①

Proof - from eq ①

$(2a-1)x + (4m^2+1)y = 1$ where x, y integers

add $4a^2y$ both sides

$\Rightarrow (2a-1)x + (4(a^2+m^2)y) + y = 1 + 4a^2y$

$\Rightarrow (2a-1)x + 4y(a^2+m^2) = 1 + y(4a^2-1)$ $\because a^2-b^2 = (a+b)\times(a-b)$

$= 1 + y(2a+1)(2a-1)$

by solving.

$\Rightarrow (2a-1)(x + y(2a+1)) + 4y(a^2+m^2) = 1$

Let $(x+y(2a+1)) = P$ & $4y = Q$ P & $Q \in$ integers

$\Rightarrow (2a-1)P + (a^2+m^2)Q = 1$ [From this add & sub $(a^2+m^2)(P)$]

we get $\Rightarrow (-2a+1)(-P) + (a^2+m^2)(-P) + (a^2+m^2)(Q+P) = 1$

$\Rightarrow (a^2-2a+1+m^2)(-P) + (a^2+m^2)(Q+P) = 1$ — ⑪

now let $-P = P'$
and $(Q+P) = Q'$ $\Big\}$ - ⑪⑪ Put in ⑪

$\Rightarrow (a^2-2a+1+m^2)P' + (a^2+m^2)(Q') = 1$

$\Rightarrow ((a-1)^2+m^2)P' + (a^2+m^2)Q' = 1$

where P' and Q' are integers

$\Rightarrow \gcd[(a-1)^2+m^2, a^2+m^2] = 1$

Hence Proved

Scanned by CamScanner

Q5 Prove that for some positive integer n if $2^n - 1$ is prime then n is also prime.

Soln given :- $2^n - 1$ is prime.

Let there exist two positive integers r and s such that $n = rs$.

$\Rightarrow 2^n - 1 = 2^{rs} - 1$

$= (2^s)^r - 1$

This can be expressed as $(2^s - 1)$ times polynomial

$(x^s)^r - 1 = (x^s - 1)(x^{s(r-1)} + x^{s(r-2)} \cdots + x^2 + 1)$ — (I)

$x = 2$.

$\Rightarrow (2^s)^r - 1 = (2^s - 1)(2^{s(r-1)} + 2^{s(r-2)} + \cdots 2^2 + 1)$

$= (2^n - 1)$ — (II) if n is composite then $(2^n - 1)$ is also composite as it is divisible by $(2^s - 1)$

if given $(2^n - 1)$ is prime.

$\therefore s = 1$ and $r = n$ — (III)

$\because (x-1)$ divides $(x^n - 1)$ $\therefore$ for $(x^n - 1)$ to be prime $(x-1)$ should be prime.

$\therefore$ from (III) we can say n is also prime

Q6 $P \mid a^2+b^2$ then $P \mid a$ and $P \mid b$ for $P = 4K+3$ and not for $4K+1$

Soln Given $P \mid a^2+b^2$

To Prove - $P \mid a$ and $P \mid b$ for $P = 4K+3$

Proof $P \mid a^2+b^2 \Rightarrow a^2+b^2 = KP$ take mod P

$\Rightarrow a^2+b^2 = 0 \mod P$ — (I)

Let $P \nmid a \Rightarrow a^{-1}$ modulo P exists

$\Rightarrow a a^{-1} = 1 \mod P$ — (II)

in eq (I) multiply $(a^{-1})^2$ both sides

$\Rightarrow (a^{-1}a)^2 + (a^{-1}b)^2 = 0 \mod P$

$\Rightarrow 1 + (a^{-1}b)^2 = 0 \mod P$

$\Rightarrow \underbrace{(a^{-1}b)}^2 \equiv -1 \mod P$

$t^2 \equiv -1 \mod P$ — (III)

As mentioned in class notes while calculating square root modulo P.

Case I → $P = 3 \mod 4$ This will never occur

$\therefore$ for $P = 3 \mod 4$ our assumption fails.

$\Rightarrow P \mid a$ similarly $P \mid b$ Hence Proved

Case II → $P = 1 \mod 4$ $t^2 \equiv -1 \mod P$ may or may not be true as it can be ± 1 both modulo P

$\therefore$ For $P = 4K+1$ this does not hold true

Case III For $P=2$ $\therefore$ inequality $a^2+b^2 \geq 2$ holds true

$P \mid a^2+b^2$ $\therefore$ let $a^2+b^2 = 2$ $\therefore a = b = 1$

here $2 \mid a^2+b^2$ but $2 \nmid a$ or $2 \nmid b$

$\therefore$ not true for ~~also~~ $P=2$

Q7 Find 3 consecutive numbers which are square free.

Solⁿ By using Chinese Remainder Theorem.

if $n = a_1 \bmod m_1$ $m_1\ m_2\ m_3$ are coprime

$n = a_2 \bmod m_2$

$n = a_3 \bmod m_3$

$$n = \sum_{i=1}^{3} a_i N_i Z_i \bmod N$$

where $N = m_1 \cdot m_2 \cdot m_3$

$N_i = \frac{N}{m_i}$ $Z_i = N_i^{-1} \bmod m_i$ — (I)

For our case $m_1\ m_2\ m_3$ have to be coprime squares

the smallest coprime Sq. are 4, 9, 25

$\therefore$ let $m_1 = 4$ $m_2 = 9$ $m_3 = 25$ — (II)

3 consecutive numbers be $(n-2)\ (n-1)\ (n)$, we have taken this sequence to simplify the calculations.

$$\Rightarrow \left.\begin{aligned} n-2 &= 0 \bmod 4 \\ n-1 &= 0 \bmod 9 \\ n &= 0 \bmod 25 \end{aligned}\right\} \text{— (III)}$$

for numbers to be not sq. free.

$$\Rightarrow \left.\begin{aligned} n &= 2 \bmod 4 \\ n &= 1 \bmod 9 \\ n &= 0 \bmod 25 \end{aligned}\right\} \text{now apply CRT}$$

$a_1 = 2$ $a_2 = 1$ $a_3 = 0$

$m_1 = 4$ $m_2 = 9$ $m_3 = 25$

$N = m_1 \cdot m_2 \cdot m_3 = 4 \times 9 \times 25 = 900$

$N_1 = 225$ $N_2 = 100$ $N_3 = 36$

$Z_1 = 225^{-1} \bmod 4$

$= 1^{-1} \bmod 4$

$Z_1 = 1 \bmod 4$

PTO

$Z_2 = 100^{-1} \bmod 9$

$\equiv 1^{-1} \bmod 9$

$\equiv 1 \bmod 9$

$Z_3 = 36^{-1} \bmod 25$

$\equiv 11^{-1} \bmod 25$

$\equiv 16 \bmod 25$

Now $n = \sum_{i=1}^{3} a_i N_i Z_i$

$= 2 \cdot 225 \cdot 1 + 1 \cdot 100 \cdot 1 + 0 \cdot 36 \cdot 16$

$n = 550$

$\Rightarrow$ three consecutive numbers

$$\left.\begin{aligned} n-2 &= 550-2 = 548 \\ n-1 &= 550-1 = 549 \\ n &= 550 \end{aligned}\right\} \text{Ans}$$

Q 8 Find a Premitive root of 13

Sol^n For a +ve integer $a \in \phi(n)$ is a premitive root modulo n if multiplicative order of a is $= \phi(n) \Rightarrow a^{\phi(n)} = 1 \bmod n$

For 13 $\quad \phi(n) = 12$

Check for $a = 2$

~~$2^1 \bmod 13$~~

$2^1 = 2 \bmod 13$

$2^2 = 4 \bmod 13$

$2^3 = 8 \bmod 13$

$2^4 = 16 = 3 \bmod 13$

$2^5 = 3 \cdot 2 \bmod 13 = 6$

$2^6 = 3 \cdot 2^2 = 12 \bmod 13$

$2^7 = 3 \cdot 2^3 = 11 \bmod 13$

$2^8 = 11 \cdot 2 = 9 \bmod 13$

$2^9 = 9 \cdot 2 = 5 \bmod 13$

$2^{10} = 5 \cdot 2 = 10 \bmod 13$

$2^{11} = 10 \cdot 2 = 7 \bmod 13$

$2^{12} = 7 \cdot 2 = 1 \bmod 13$

$\Rightarrow 2^{\phi(n)} = 1$ & 12 is multiplicative order of 2 modulo 13

$\Rightarrow$ 2 is a Premitive root of 13

Scanned by CamScanner

Q9 Least non negative residue of $19! + (13!)^{44} \bmod 23$

Sol^n Let us calculate residue individually for each term.

(i) $19! \bmod 23$

23 is Prime

$\therefore$ by wilson's theorem $(P-1)! \bmod P = -1 \bmod P$.

$\Rightarrow (23-1)! = 1 \bmod 23$

$\Rightarrow 22! = 1 \bmod 23$

$\Rightarrow 22 \times 21 \times 20 \times 19! = -1 \bmod 23$

$\Rightarrow (-1) \times (-2) \times (-3) \times 19! = -1 \bmod 23$

$\Rightarrow +6 \times 19! = 1 \bmod 23$

$\Rightarrow 19! = 6^{-1} \bmod 23$

$= 4 \bmod 23$ — (I)

$6x = 1 \bmod 23$

$\Rightarrow x = 4 = 6^{-1} \bmod 23$

(ii) $(13!)^{44} \bmod 23 = n$

23 is Prime $\Rightarrow$

$\therefore$ By Fermet's theorem $a^{P-1} = 1 \bmod p$

$\Rightarrow a^{22} = 1 \bmod 23$ — (II)

$\Rightarrow n = (13!)^{44} \bmod 23$

$= [(13!)^2]^{22} \bmod 23$ — (III)

From (II) let $a = (13!)^2$

$\Rightarrow n = 1 \bmod 23$ — (IV)

$\therefore$ Ans = (I) + (IV)

$= 4 + 1 \bmod 23$

$= 5 \bmod 23$

Q10. Find $\phi(125)$. $N = 3^{10!} - 1$ is divisible by 125?

Soln. $125 = 5 \times 5 \times 5 = 5^3$

$$\phi(n) = n\left[1 - \frac{1}{P_1}\right]\left[1 - \frac{1}{P_2}\right] \cdots \left[1 - \frac{1}{P_n}\right]$$ $P_1, P_2 \ldots P_n$ are Prime facto of n

$$\phi(125) = 125 \times \left[1 - \frac{1}{5}\right]$$

$$= 125 \times \frac{4}{5} = 100$$

$$\Rightarrow \boxed{\phi(125) = 100} \quad \text{— (I)}$$

$$N = \underbrace{3^{10!}}_{n} - 1 \quad \text{mod } 125$$

$$n = 3^{10!} \text{ mod} 125$$

By generalization of Fermat's Theorem.

$$a^{\phi(n)} = 1 \text{ mod } n \quad \text{for any number } n \quad \text{— (II)}$$

$$\phi(125) = 100 \qquad \overbrace{9 \times 8 \times 7 \times 6 \times 4 \times 3 \times 1}^{\text{Let this Power be } P}$$

$$n = 3^{10!} = \left[3^{10 \times 5 \times 2}\right] \quad \text{mod} 125$$

$$= \left[3^{100}\right]^P \text{ mod } 125$$

from (II)

$$n = 3^{10!} = [1]^P \text{ mod } 125$$

$$= 1 \text{ mod } 125 \quad \text{— (III)}$$

$\therefore$ $N = 3^{10!} - 1 \text{ mod } 125$

$$= 1 - 1 \text{ mod } 125$$

$$= 0 \text{ mod } 125$$

$\therefore$ Yes 125 divides N

Q11 Q. Premitive root of modulo 29:

(i) How many Premitive roots does 29 has.

Ans Reference :- wikipedia.org/wiki/Primitive_root_modulo_n

Cite Note 11 - https://oeis.org/A010554

States that Number of Premitive root of modulo n

$= \phi(\phi(n))$

where $\phi \rightarrow$ Phi function ~~mod~~ of n

$\Rightarrow \phi(n) = n\left[1-\frac{1}{P_1}\right]\left[1-\frac{1}{P_2}\right]\ldots\left[1-\frac{1}{P_r}\right]$ $P_1, P_2 \ldots P_r$ Prime factor of n

$\Rightarrow \phi(29) = P-1 = 29-1 = 28$

$\phi(\phi(29)) = \phi(28)$

$28 = 2^2 \cdot 7$

$\Rightarrow \phi(28) = 28\left(1-\frac{1}{2}\right)\left(1-\frac{1}{7}\right)$

$= 2 \times 1 \times 6$

$\phi(28) = 12$

* Also calculated in Part (iii) of this Q. on next Page

$\Rightarrow$ no. of Premitive roots of 29 $= \underline{\underline{12}}$ Ans

(ii) Find a Premitive root modulo 29

Check for 2. Powers of 2 mod 29

$2^1 = 2 \mod 29$

$2^2 = 4$ "

$2^3 = 8$ "

$2^4 = 16$ "

$2^5 = 32 = 3$ "

$2^6 = 6$ "

$2^7 = 12$ "

$2^8 = 24$ "

$2^9 = 48 = 19$ "

$2^{10} = 9$ "

$2^{11} = 18 \mod 29$

$2^{12} = 7$ " "

$2^{13} = 14$ " "

$2^{14} = 28$ " "

$2^{15} = 56$ " $= 27$ "

$2^{16} = 54$ " $= 25$ "

$2^{17} = 50$ " $= 21$ "

$2^{18} = 2 \times 21 \mod 29 = 13$

$2^{19} = 26 \mod 29$

$2^{20} = 23 \mod 29$

$2^{21} = 46 \mod 29 = 17 \mod 29$

$2^{22} = 34 \mod 29 = 5 \mod 29$

$2^{23} = 10 \mod 29$

$2^{24} = 20$ "

$2^{25} = 11$ "

$2^{26} = 22$ "

$2^{27} = 44$ " $= 15 \mod 29$

$2^{28} = 30 \mod 29$

$\boxed{2^{28} = 1 \mod 29}$

$\Rightarrow$ 2 is a Premitive root of 29

(iii) use g mod 29 to calculate Primitive roots of modulo 29

Sol^n: g is a ~~a~~ primititive root of ~~29~~ modulo 29

$\Rightarrow$ g is a generator of

~~Root~~ Primitive roots g^n $n \in \overset{1\ldots}{}\phi(n)$ and Coprime with $\phi(n)$

if P is Prime then $\phi(n) = P-1$

Our case

$g = 2 \quad P = 29 \quad \phi(29) = 28$

$n \to 1 \le n \le 28$ & coprime with 28

$n = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$

$\Rightarrow$ Primitive roots $= g^n \bmod P$

As calculated in Part (i) of this question on Previous Page

$2^1 = 2 \bmod 29$

$2^3 = 8 \bmod 29$

$2^5 = 3 \bmod 29$

$2^9 = 19 \bmod 29$

$2^{11} = 18 \bmod 29$

$2^{13} = 14 \bmod 29$

$2^{15} = 27 \bmod 29$

$2^{17} = 21 \bmod 29$

$2^{19} = 26 \bmod 29$

$2^{23} = 10 \bmod 29$

$2^{25} = 11 \bmod 29$

$2^{27} = 15 \bmod 29$

$\therefore$ total Primitive roots modulo 29 $= \underline{12}$

$\therefore$ Primitive roots mod 29 are $-$ 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27

(iv) Use g mod 29 to express quadratic residue of modulo 29.

Solⁿ Quadratic residue mod n is a

if $\exists x \in Z^*$ s.t

$x^2 \equiv a \bmod n$

Also. in terms of g Reference * class notes 20 Jan

g^i $i \in (1, 2, \ldots \phi(n))$

if i = even then g^i = Quadratic residue

and i = odd then g^i = Quad. non residue.

$\Rightarrow$ $g = 2$ here

Quad residue

$2^2 \bmod 29$

$2^4 \bmod 29$

$2^6 \bmod 29$

$2^8 \bmod 29$

$2^{10} \bmod 29$ * we will calculate in next Part

$2^{12} \bmod 29$

$2^{14} \bmod 29$

$2^{16} \bmod 29$

$2^{18} \bmod 29$

$2^{20} \bmod 29$

$2^{22} \bmod 29$

$2^{24} \bmod 29$

$2^{26} \bmod 29$

$2^{28} \bmod 29$

(V) Quadratic residue –

$2^2 \bmod 29 = 4 \bmod 29$ As calculated in Part (i) of this Q.

$2^4 = 16 \bmod 29$ $\quad$ $2^{22} = 5 \bmod 29$

$2^6 = 6 \bmod 29$ $\quad$ $2^{24} = 20 \bmod 29$

$2^8 = 24 \bmod 29$ $\quad$ $2^{26} = 22 \bmod 29$

$2^{10} = 9 \bmod 29$ $\quad$ $2^{28} = 1 \bmod 29$

$2^{12} = 7 \bmod 29$

$2^{14} = 28 \bmod 29$

$2^{16} = 25 \bmod 29$

$2^{18} = 13 \bmod 29$

$2^{20} = 23 \bmod 29$

From above

Quadratic Residues $= \{1, 4, 5, 6, 7, 9, 13, 16, 20, 22, 24, 28\}$

Quadratic Nonresidue $= 1 - Q = \bar{Q}$

$\Rightarrow \{2, 3, 8, 10, 11, 12, 14, 15, 17, 18, 19, 21, 23, 25, 26, 27\}$

(vi) Is 5 a quad. residue modulo 29. Is 5 congruent to 4th Power modulo 29.

Solⁿ From Previous Q.

5 is a Quad. Residue of modulo 29.

Calculate 4th Power modulo 29

$1^4 = 1 \bmod 29$

$2^4 = 16 \bmod 29$

$3^4 = 81 \bmod 29 = 23 \bmod 29$

$4^4 = 64 \times 4 \bmod 29 = 24 \bmod 29$

$5^4 = 25 \times 25 \bmod 29 = 16 \bmod 29$

$6^4 = 36 \times 36 \bmod 29 = 20 \bmod 29$

$7^4 = 49 \times 49 \bmod 29 = 23 \bmod 29$

$8^4 = 64 \times 64 = 6 \times 6 \bmod 29 = 7 \bmod 29$

$9^4 = 81 \times 81 \bmod 29 = 23 \times 23 = 36 = 7 \bmod 29$

$10^4 = 100 \times 100 \bmod 29 = 13 \times 13 \bmod 29 = 24 \bmod 29$

$11^4 = 121 \times 121 \bmod 29 = 5 \times 5 \bmod 29 = 25 \bmod 29$

$12^4 = 144 \times 144 \bmod 29 = 28 \times 28 = (-1)(-1) \bmod 29 = 1 \bmod 29$

$13^4 = 169 \times 169 = 24 \times 24 = 5 \times 5 = 25 \bmod 29$

$14^4 = 196 \times 196 = 22 \times 22 = 49 \bmod 29 = 20 \bmod 29$

$\therefore$ 4th Power $= 1, 16, 23, 24, 20, 7, 25$

$\therefore$ 5 is not congruent to 4th Power

(vii) use g modulo 29 to calculate Congruence classes congruent to 4th Power

Solⁿ $g = 2$ ∴ 4K Power of 2

$2^4 \bmod 29 = 16 \bmod 29$

$2^8 \bmod 29 = 64 \times 4 \bmod 29$

$= 6 \times 4 = 24 \bmod 29$

$2^{12} \bmod 29 = 24 \times 16 = 7 \bmod 29$

$2^{16} \bmod 29 = 7 \times 16 = 25 \bmod 29$

$2^{20} \bmod 29 = 25 \times 16 = -64 \bmod 29$

$= 23 \bmod 29$

$2^{24} \bmod 29 = 23 \cdot 16 = 20 \bmod 29$

$2^{28} \bmod 29 = 1 \bmod 29$

∴ Power 4th Congruence classes $= 1, 7, 16, 20, 23, 24, 25$

(viii) $x^4 - 29y^4 = 5$ has no integral Solⁿ

Solⁿ $x^4 - 29y^4 = 5$

take modulo 29 both sides.

~~$x^4 \bmod 29$~~ −

$(x^4 - \underbrace{29y^4}_{=0}) \bmod 29 = 5 \bmod 29$

$\Rightarrow x^4 = 5 \bmod 29$ — (1)

But we have verified in (vi) & (vii) Part of this question 5 doesnot lie in congruence class of Power 4 modulo 29.

⇒ There is no integral solution for the above equation.

Hence Proved

Q12 Simplify 146! mod 149.

Soln $N = 146! \pmod{149}$

$\because$ 149 is a Prime no.

$\therefore$ By wilson's Theorem if P is a Prime no.

then $(P-1)! = -1 \bmod P$

$\Rightarrow$ for 149

$(149-1)! = -1 \bmod P$

$148! = -1 \bmod 149$

$\Rightarrow 148 \times 147 \times 146! = -1 \bmod 149$

$\Rightarrow (-1) \times (-2) \times 146! = -1 \bmod 149$

$\Rightarrow 146! = (-2)^{-1} \bmod 149$ — ①

$2^{-1} \bmod 149$

$\Rightarrow 149 = 74 \times 2 + 1$

$\Rightarrow 149 - 74 \times 2 = 1$

$\Rightarrow 2^{-1} = -74 \bmod 149.$

Put in ①

$\Rightarrow 146! = -(2)^{-1} \bmod 149$

$= -(-74) \bmod 149$

$146! = 74 \bmod 149$ Ans