

(Q1) is $4^{1536} \equiv 9^{4824} \pmod{35}$

Q1 is $4^{1536} \equiv 9^{4824} \pmod{35}$

We can analyze the question by calculating the value of $4^{1536} \pmod{35}$ and checking if it is the same as $9^{4824} \pmod{35}$. We begin by solving $4^{1536} \pmod{35}$.

$$(nq+r)^k \pmod{n} \equiv r^k \pmod{n}$$

$$\begin{aligned} 4^{2 \cdot 768} &\Rightarrow 16^{768} \pmod{35} \\ 16^{2 \cdot 384} &\Rightarrow 256^{384} \pmod{35} \\ &\Rightarrow (7 \cdot 35 + 11)^{384} \pmod{35} \\ &\Rightarrow 11^{384} \pmod{35} \\ 11^{2 \cdot 192} &\Rightarrow 121^{192} \pmod{35} \\ &\Rightarrow (3 \cdot 35 + 16)^{192} \pmod{35} \\ 16^{2 \cdot 96} &\Rightarrow 256^{96} \pmod{35} \\ &\Rightarrow (3 \cdot 35 + 11)^{96} \pmod{35} \\ 11^{2 \cdot 48} &\Rightarrow 121^{48} \pmod{35} \\ &\Rightarrow (3 \cdot 35 + 16)^{48} \pmod{35} \\ 16^{2 \cdot 24} &\Rightarrow 256^{24} \pmod{35} \\ &\Rightarrow (7 \cdot 35 + 11)^{24} \pmod{35} \\ 11^{2 \cdot 12} &\Rightarrow 121^{12} \pmod{35} \\ &\Rightarrow (3 \cdot 35 + 16)^{12} \pmod{35} \\ 16^{2 \cdot 6} &\Rightarrow 256^6 \pmod{35} \\ &\Rightarrow (3 \cdot 35 + 11)^6 \pmod{35} \\ 11^{2 \cdot 3} &\Rightarrow 121^3 \pmod{35} \\ &\Rightarrow (3 \cdot 35 + 16)^3 \pmod{35} \\ 16^2 \cdot 16^1 &\Rightarrow 256 \cdot 16 \pmod{35} \\ &\Rightarrow (7 \cdot 35 + 11) \cdot 16 \pmod{35} \\ &\Rightarrow 11 \cdot 16 \pmod{35} \end{aligned}$$

$$\begin{aligned} 176 \pmod{35} &= 1 \\ \therefore 4^{1536} \pmod{35} &= 1 \end{aligned}$$

We know $4^{1536} \pmod{35} = 1$, we can use Fermat's little theorem to solve whether or not $9^{4824} \pmod{35} = 1$, where $9^{4824} \equiv 1 \pmod{35}$.

By Fermat's prime factorization by n , we get $35 = 5 \cdot 7$.

① $a^{n-1} \equiv 1 \pmod{n}$ for $n=5$
 $a^4 \equiv 1 \pmod{5}$

② $a^{n-1} \equiv 1 \pmod{n}$ for $n=7$
 $a^6 \equiv 1 \pmod{7}$

combine ① ② yields

$$a^{4 \cdot 6} \equiv 1 \pmod{5 \cdot 7}$$

$$a^{24} \equiv 1 \pmod{35}$$

Solve for a by $\frac{4824}{24} = 201$

$$a = 9^{201}$$

by fermat's we have found a value that satisfy his theorem.

$$\therefore 9^{4824} \pmod{35} = 1$$

Both the left hand side and right hand side are congruent, therefore the statement is true. ■

Q2 Solve $x^{86} \equiv 6 \pmod{29}$

Q3 Prove that $\gcd(F_{n+1}, F_n) = 1$, for $n \geq 1$, where F_n is the n -th Fibonacci element.

Solution:

When the \gcd of two numbers is 1, that means that the numbers are relatively prime, meaning that there is no number $n \neq 1$ that divides both of the numbers. We can prove the following statement by induction.

Base case:

For $n = 0$, we check the $\gcd(F_0, F_1)$, which are $\gcd(1, 1)$, these two numbers satisfy as $\gcd(1, 1) = 1 \checkmark$

Induction step:

For our induction hypothesis, we assume that $\gcd(F_n, F_{n+1}) = 1$. We must prove that the statement is true as well for $n = k + 1$ and prove $\gcd(F_{k+1}, F_{k+2}) = z$, for $z = 1$

By the equation, we know that $z \mid F_{k+1}$, $z \mid F_{k+2}$ and $z \mid F_k + F_{k+1}$ since $F_x = F_{x-2} + F_{x-1}$ for $x \in \mathbb{N}$. $z \mid F_k + F_{k+1}$ tells us that $z \mid F_k$ and $z \mid F_{k+1}$, we can derive Euclid's GCD by stating $\gcd(F_k, F_{k+1}) = z$. From our induction hypothesis, we know that $\gcd(F_n, F_{n+1}) = 1$, therefore, z is also 1. We prove the following claim by a direct proof via induction. ■