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

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

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

$(nq+r)^k \bmod n \equiv r^x \bmod n$

$4^{2 \cdot 768} \Rightarrow 16^{768} \bmod 35$

$16^{2 \cdot 384} \Rightarrow 256^{384} \bmod 35$

$\Rightarrow (7 \cdot 35 + 11)^{384} \bmod 35$

$\Rightarrow 11^{384} \bmod 35$

$11^{2 \cdot 192} \Rightarrow 121^{192} \bmod 35$

$\Rightarrow (3 \cdot 35 + 16)^{192} \bmod 35$

$16^{2 \cdot 96} \Rightarrow 256^{96} \bmod 35$

$\Rightarrow (35 \cdot 7 + 11)^{96} \bmod 35$

$11^{2 \cdot 48} \Rightarrow 121^{48} \bmod 35$

$\Rightarrow (3 \cdot 35 + 16)^{48} \bmod 35$

$16^{2 \cdot 24} \Rightarrow 256^{24} \bmod 35$

$\Rightarrow (7 \cdot 35 + 11)^{24} \bmod 35$

$11^{2 \cdot 12} \Rightarrow 121^{12} \bmod 25$

$\Rightarrow (3 \cdot 35 + 16)^{12} \bmod 35$

$16^{2 \cdot 6} \Rightarrow 256^{6} \bmod 35$

$\Rightarrow (35 \cdot 7 + 11)^{6} \bmod 35$

$11^{2 \cdot 3} \Rightarrow 121^{3} \bmod 35$

$\Rightarrow (3 \cdot 35 + 16)^{3} \bmod 35$

$16^2 16^1 \Rightarrow 256 \cdot 16 \bmod 35$

$\Rightarrow (7 \cdot 35 + 11) \cdot 16 \bmod 35$

$\Rightarrow 11 \cdot 16 \bmod 35$

$176 \bmod 35 = 1$

$\therefore 4^{1536} \bmod 35 = 1$

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

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

① $a^{n-1} = 1 \bmod n$ for $n = 5$

$a^4 = 1 \bmod 5$

② $a^{n-1} = 1 \bmod n$ for $n = 7$

$a^6 = 1 \bmod 7$

combine ① ② yields

$a^{4 \cdot 6} \equiv 1 \bmod (5 \cdot 7)$

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

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

$a = 9^{201}$

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

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

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

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

Q2. solve $x^{86} \equiv 6 \mod 29$

Fermat says we can use his formula $a^{N-1} \equiv 1 \mod N$ if N is prime.

In our case, N is a prime number 29. we can derive the following equation

$x^{28} \equiv 1 \mod 29$ ①

prime factorization of 28 ②

$x^{2 \cdot 7} \equiv 1 \mod 29$ ③

$x^2 \equiv 1 \mod 29$ ④

$x^7 \equiv 1 \mod 29$ ⑤

for ④: we try to solve the equation $x^2 \bmod 29 = 6$:

find the multiples of 29
29, 58

$x^2 = 29n + 6$
$x^2 = 58 + 6$
$x^2 = 64$
$x = 8 \mod 29$

for ⑤: we try to solve the equation $x^7 \bmod 29 = 6$:

we will try different values for

x	x^7	$\lvert 29 \cdot \lfloor x^7/29 \rfloor - x^2 \rvert$ ← to calculate the remainder
2	128	12
3	2187	12
4	16356	28
5	78125	28
6	279936	28
7	823543	1
8	2097152	17

we just have to solve for the smallest x value and this already exceeds it, therefore it is unimportant. Our previous solution remains.

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 $gcd(1, 1) = 1$ ✓

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 $x \in \mathbb{N}$. $z \mid F_k + Fk + 1$ 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. ■