Intro to Algorithms - Homework 3

Q1.

$x \equiv y \pmod{N}$

$\downarrow$

N divides $(x-y)$

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

First, we need to check whether the $(4^{1536} - 9^{4824})$ is the multiple of 35 according to the modular arithmetic

35 is the multiple of 5 and 7, so I can split them into two parts to check whether $4^{1536} - 9^{4824}$ is divisible 5 and 7.

$$4^{1536} \equiv ? \pmod{5}$$
$$4^2 \equiv 1 \pmod{5}$$
$$(4^2)^{768} \equiv [1 \pmod{5}]^{768}$$
$$4^{1536} \equiv 1 \pmod{5}$$

$$9^{4824} \equiv ? \pmod{5}$$
$$9^2 \equiv 1 \pmod{5}$$
$$(9^2)^{2412} \equiv [1 \pmod{5}]^{2412}$$
$$9^{4824} \equiv 1 \pmod{5}$$

$$4^{1536} \equiv ? \pmod{7}$$
$$4^3 \equiv 1 \pmod{7}$$
$$(4^3)^{512} \equiv [1 \pmod{7}]^{512}$$
$$4^{1536} \equiv 1 \pmod{7}$$

$$9^{4824} \equiv ? \pmod{7}$$
$$9^2 \equiv 4 \pmod{7}$$
$$(9^2)^{2412} \equiv [4 \pmod{7}]^{2412}$$
$$\downarrow$$
$$4^{2412} \equiv ? \pmod{7}$$
$$4^3 \equiv 1 \pmod{7}$$
$$(4^3)^{804} \equiv [1 \pmod{7}]^{804}$$

$$9^{4824} = [4 \pmod{7}]^{2412} = (4^3)^{804}$$
$$= 1 \pmod{7}$$

Hence, $4^{1536} - 9^{4824} \pmod{5} = 1 - 1 = 0$

$4^{1536} - 9^{4824} \pmod{7} = 1 - 1 = 0$

Therefore, $4^{1536} \equiv 9^{4824} \pmod{35}$ is correct.

Q2.

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

By Fermat's Little Theorem, $x^{28} \equiv 1 \pmod{29}$

Thus $x^{86} \equiv x^2 \bmod 29$ [Because $(28 \times 3) + 2 = 86$.]

Solve $x^2 \equiv 6 \pmod{29}$

$29 \times 2 + 6 = 64 \longrightarrow \sqrt{64} = 8$

Therefore : $x = 8$.

which is $8^{86} \equiv 6 \pmod{29}$

Q3: $\gcd(F_{n+1}, F_n) = 1$, for $n \geq 1$

Prove by induction.

Base case: $n = 1$

$\gcd(2, 1) = 1$ which is correct.

$n = 2$

$\gcd(3, 2) = 1$ which is also true.

Induction step: Assume $\gcd(F_{n+1}, F_n) = 1$ is true,

then Prove that $\gcd(F_{n+1+1}, F_{n+1}) = 1$ also True for all $n \geq 1$

$$\gcd(F_{n+2}, F_{n+1}) = \gcd(F_{n+1}, \text{rem}(F_{n+2}, F_{n+1}))$$
$$= \gcd(F_{n+1}, F_n) = 1$$

Since the induction hypothesis is true, and the (F_{n+1}, F_n) number are next to each other, because F_n is the n-th Fibonacci number they only have 1 gcd, which is 1.

Hence, the $\gcd(F_{n+2}, F_{n+1})$ will be $\gcd(F_{n+1}, 1)$ and this will result as $\gcd(F_{n+1}, F_n) = 1$.

Therefore, Based on the Induction proof, the $\gcd(F_{n+1}, F_n) = 1$ for $n \geq 1$ is True.