CSCI 2300: Introduction to Algorithms
Homework 3

Lucien Brule
brulel@rpi.edu

January 30, 2023

1 Problem 1.1

a. We can show that $4^{1536} \equiv 9^{4824} \pmod{35}$ using Fermat's Little Theorem. Fermat's Little Theorem states that for any prime p and any integer a such that $gcd(a, p) = 1$, we have $a^{p-1} \equiv 1 \pmod{p}$. Since $35 = 5 \cdot 7$ and both 5 and 7 are primes, we can use Fermat's Little Theorem on both 5 and 7 separately:

$$4^4 \equiv 1 \pmod{5} \quad 9^6 \equiv 1 \pmod{7}$$

Now we can use the property of modular exponentiation to simplify 4^{1536} and 9^{4824}

$$4^{1536} \equiv (4^4)^{384} \pmod{35} \equiv 1^{384} \pmod{35} \equiv 1 \pmod{35}$$

$$9^{4824} \equiv (9^6)^{804} \pmod{35} \equiv 1^{804} \pmod{35} \equiv 1 \pmod{35}$$

Finally,

$$4^{1536} \equiv 9^{4824} \equiv 1 \pmod{35}$$

So, $4^{1536} \equiv 9^{4824} \pmod{35}$.

Problem 1.2

Is $4^{1536} \equiv 9^{4824} \pmod{35}$?

Since $35 = 5 \cdot 7$, we can use the Chinese Remainder Theorem to solve the congruence.

$$\begin{aligned} 4^{1536} &\equiv 4^{1536} \bmod 5 \cdot 7 \\ &\equiv 4^{1536} \bmod 5 \cdot 4^{1536} \bmod 7 \\ &\equiv 1 \cdot 1 \\ &\equiv 1 \pmod{35} \end{aligned}$$

$$\begin{aligned} 9^{4824} &\equiv 9^{4824} \bmod 5 \cdot 7 \\ &\equiv 9^{4824} \bmod 5 \cdot 9^{4824} \bmod 7 \\ &\equiv 1 \cdot 1 \\ &\equiv 1 \pmod{35} \end{aligned}$$

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

The Chinese Remainder Theorem is a theorem that states that if we have a system of linear congruences, with moduli that are pairwise relatively prime, then this system has a unique solution modulo the product of the moduli.

Applying this theorem to the problem above, we have:

$$4^{1536} \equiv 1 \pmod 5 \quad 4^{1536} \equiv 1 \pmod 7 \quad 9^{4824} \equiv 1 \pmod 5 \quad 9^{4824} \equiv 1 \pmod 7$$

Since the moduli 5 and 7 are relatively prime, we can find a solution for $4^{1536} \equiv 9^{4824} \pmod{35}$ using the Chinese Remainder Theorem. The unique solution is $4^{1536} \equiv 9^{4824} \equiv 1 \pmod{35}$.

Problem 2

Solve for $x^{86} \pmod{29}$.

Let's start with Fermat's Little Theorem:

$$x^{28} \equiv 1 (\text{mod } 29) \tag{1}$$

Using this, we can simplify x^{86}:

$$x^{86} \equiv x^2 (\text{mod } 29) \tag{2}$$

So, we only need to find $x^2 (\text{mod } 29)$.

$$x^2 \equiv 6 (\text{mod } 29) \tag{3}$$

This is the same as:

$$x^2 \equiv 64 (\text{mod } 29) \tag{4}$$

ergo:

$$x^2 - 64 \equiv (x-8)(x+8) \equiv 0 (\text{mod } 29) \tag{5}$$

Thus,

$$x \equiv 8 (\text{mod } 29) \tag{6}$$

$$x \equiv 21 (\text{mod } 29) \tag{7}$$

Problem 3

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

Base case:

$$\gcd(F_2, F_1) = \gcd(1, 1) = 1$$

By induction...

Assumption:

$$\gcd(F_n, F_{n-1}) = 1 \text{ for some } n \geq 1$$

Calculation:

$$\begin{aligned} \gcd(F_{n+1}, F_n) &= \gcd(F_{n+1}, F_n) + \gcd(F_n, F_{n-1}) \\ &= \gcd(F_n, F_{n-1}) + \gcd(F_{n+1}, F_{n-1}) \\ &= \gcd(F_{n+1}, F_{n-1}) \end{aligned}$$

Conclusion:

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