CS 70 Discrete Mathematics and Probability Theory
Spring 2022 Koushik Sen and Satish Rao **DIS 3A**

1 Party Tricks

You are at a party celebrating your completion of the CS 70 midterm. Show off your modular arithmetic skills and impress your friends by quickly figuring out the last digit(s) of each of the following numbers:

(a) Find the last digit of 11^{3142}.

(b) Find the last digit of 9^{9999}.

Solution:

(a) First, we notice that $11 \equiv 1 \pmod{10}$. So $11^{3142} \equiv 1^{3142} \equiv 1 \pmod{10}$, so the last digit is a 1.

(b) 9 is its own multiplicative inverse mod 10, so $9^2 \equiv 1 \pmod{10}$. Then

$$9^{9999} = 9^{2(4999)} \cdot 9 \equiv 1^{4999} \cdot 9 \equiv 9 \pmod{10},$$

so the last digit is a 9.

Another solution: We know $9 \equiv -1 \pmod{10}$, so

$$9^{9999} \equiv (-1)^{9999} \equiv -1 \equiv 9 \pmod{10}.$$

You could have also used this to say

$$9^{9999} \equiv (-1)^{9998} \cdot 9 \equiv 9 \pmod{10}.$$

2 Modular Potpourri

(a) Evaluate $4^{96} \pmod{5}$.

(b) Prove or Disprove: There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod{6}$.

(c) Prove or Disprove: $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$.

Solution:

(a) One way: $4 \equiv -1 \pmod 5$, and $(-1)^{96} \equiv 1$.

Another: $4^2 \equiv 1 \pmod 5$, so $4^{96} = (4^2)^{48} \equiv 1 \pmod 5$.

Mention that it is **invalid** to "apply the mod to the exponent": $4^{96} \not\equiv 4^1 \pmod 5$.

(b) Impossible.

Suppose there exists an x satisfying both equations.

From $x \equiv 3 \pmod{16}$, we have $x = 3 + 16k$ for some integer k. This implies $x \equiv 1 \pmod 2$.

From $x \equiv 4 \pmod 6$, we have $x = 4 + 6l$ for some integer l. This implies $x \equiv 0 \pmod 2$.

Now we have $x \equiv 1 \pmod 2$ and $x \equiv 0 \pmod 2$. Contradiction.

(c) False, consider $x \equiv 8 \pmod{12}$.

The reason we can't eliminate the 2 in the first equation to get the second equation is because 2 does not have a multiplicative inverse modulo 12, as 2 and 12 are not coprime.

3 Modular Inverses

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod m$, then we say x is an **inverse of a modulo m**.

Now, we will investigate the existence and uniqueness of inverses.

(a) Is 3 an inverse of 5 modulo 10?

(b) Is 3 an inverse of 5 modulo 14?

(c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?

(d) Does 4 have inverse modulo 8?

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod m$?

Solution:

(a) No, because $3 \cdot 5 = 15 \equiv 5 \pmod{10}$.

(b) Yes, because $3 \cdot 5 = 15 \equiv 1 \pmod{14}$.

(c) Yes, because $(3 + 14n) \cdot 5 = 15 + 14 \cdot 5n \equiv 15 \equiv 1 \pmod{14}$.

(d) No. For contradiction, assume $x \in \mathbb{Z}$ is an inverse of 4 modulo 8. Then $4x \equiv 1 \pmod 8$. Then $8 \mid 4x - 1$, which is impossible.

(e) No. We have $xa \equiv x'a \equiv 1 \pmod{m}$. So

$$xa - x'a = a(x - x') \equiv 0 \pmod{m}.$$

Multiply both sides by x, we get

$$xa(x - x') \equiv 0 \cdot x \pmod{m}$$

$$\implies x - x' \equiv 0 \pmod{m}.$$

$$\implies x \equiv x' \pmod{m}$$

4 Fibonacci GCD

The Fibonacci sequence is given by $F_n = F_{n-1} + F_{n-2}$, where $F_0 = 0$ and $F_1 = 1$. Prove that, for all $n \geq 1$, $\gcd(F_n, F_{n-1}) = 1$.

Solution:

Proceed by induction.

Base Case: We have $\gcd(F_1, F_0) = \gcd(1, 0) = 1$, which is true.

Inductive Hypothesis: Assume we have $\gcd(F_k, F_{k-1}) = 1$ for some $k \geq 1$.

Inductive Step: Now we need to show that $\gcd(F_{k+1}, F_k) = 1$ as well.

We can show that:

$$\gcd(F_{k+1}, F_k) = \gcd(F_k + F_{k-1}, F_k) = \gcd(F_k, F_{k-1}) = 1.$$

Note that the second expression comes from the definition of Fibonacci numbers. The last expression comes from Euclid's GCD algorithm, in which $\gcd(x, y) = \gcd(y, x \bmod y)$, since

$$F_k + F_{k-1} \equiv F_{k-1} \pmod{F_k}.$$

Therefore the statement is also true for $n = k + 1$.

By the rule of induction, we can conclude that $\gcd(F_n, F_{n-1}) = 1$ for all $n \geq 1$, where $F_0 = 0$ and $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$.