Modular Arithmetic

$$a \equiv b \pmod{m} \iff a = b + km \quad \text{for } k \in \mathbb{Z}$$

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

CS 70 Spring 2022 — Discrete Mathematics and Probability Theory — 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}.

a) $11^{3142} \equiv 1^{3142} \pmod{10}$

$\equiv 1 \pmod{10}$

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

$\equiv ((-1)^2)^{4999}(-1)^1$

$\equiv 1^{4999}(-1)^1$

$\equiv -1$

$\equiv 9 \pmod{10}$

2 Modular Potpourri

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

$4^{96} \equiv (-1)^{96} \pmod 5$

$\equiv 1 \pmod 5$

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

False. If $x = 16k+3$ then x is odd,

but $x = 6k+4$ would be even.

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

False. $x = 8$

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? No. $3 \cdot 5 = 15 \equiv 5 \pmod{10}$

(b) Is 3 an inverse of 5 modulo 14? Yes. $3 \cdot 5 = 15 \equiv 1 \pmod{14}$

(c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14? Yes. $5(3+14n) = 15 + 14 \cdot 5n = 1 + 14(1+5n)$

(d) Does 4 have inverse modulo 8? No. $4x \equiv 1 \pmod{8} \Rightarrow 4x - 1 = 8k$

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

No.

$$ax \equiv ax' \pmod{m}$$
$$xax \equiv xax'$$
$$x \equiv x'$$

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 $n \geq 1$, $\gcd(F_n, F_{n-1}) = 1$.

Base Case: $\gcd(F_1, F_0) = \gcd(1, 0) = 1$

Induction Hypothesis: $\gcd(F_k, F_{k-1}) = 1$

Inductive Step:
$$\begin{aligned}\gcd(F_{k+1}, F_k) &= \gcd(F_k + F_{k-1}, F_k) \\ &= \gcd(F_k, (F_k + F_{k-1}) \bmod F_k) \\ &= \gcd(F_k, F_{k-1}) \\ &= 1\end{aligned}$$