CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair **DIS 3A**

1 Party Tricks

Note 6

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}.

$(11)^{3142} \bmod 10 = (1)^{3142} \bmod 10 = 1$

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

$(9^{9999}) \bmod 10 = (-1)^{9999} = -1 \bmod 10$
$= 9$

(c) Find the last digit of 3^{641}.

$(3^{641}) \bmod 10$
$= (9^{320} \cdot 3) \bmod 10$
$= (-1)^{320} \cdot 3 \bmod 10 = 3$

2 Modular Potpourri

Note 6

Prove or disprove the following statements:

X (a) There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod{6}$.

$x = 3 + 16 \cdot c$, $x = 4 + 6 \cdot d$
$x \bmod 2 = 1$ $x \bmod 2 = 0$
Thus. impossible.

X (b) $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$.

$x \equiv 2 \Rightarrow 2x \equiv 4$ obvious
$2x \equiv 4 \Rightarrow 2x = 4 + 12 \cdot d$
$x = 2 + 6 \cdot d$ any d even

(c) $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{6}$. Thus $2x = 16, x = 8$ violate. not the

Yes by above

3 Modular Inverses

Note 6

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

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

Yes

(c) For all $n \in \mathbb{N}$, is $3 + 14n$ an inverse of 5 modulo 14?

Yes

(d) Does 4 have an inverse modulo 8?

No, as $GCD(4,8) \neq 1$

(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. Suppose $xa \equiv ax' \equiv 1 \bmod m$

$x'a \equiv xax'$

$\equiv x \cdot 1 \equiv 1 \cdot x' \equiv x \equiv x' \bmod m$

4 Fibonacci GCD

Note 6

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

Yes as gcd algorithm works by calculating $F_n \bmod F_{n-1}$ recursively, thus as F_n strictly increases, the subtract back down to F_2 and F_1 which returns 1.