CS 70 Discrete Mathematics and Probability Theory
Fall 2024 Rao, Hug

# DIS 3B

## 1 Modular Basics

Note 6

For the first two parts, select all options that are equivalent to the given statement:

(a) $a \equiv b \pmod{m}$

i. $a$ and $b$ have the same remainder when divided by $m$

ii. $m \mid a+b$

iii. $a = b - km$ for some integer $k$.

(b) $a^k \equiv b^k \pmod{m}$

i. $(a \mod m)^k \equiv (b \mod m)^k \pmod{m}$

ii. $a^{k \bmod m} \equiv b^{k \bmod m} \pmod{m}$

For the remainder, compute the last digit(s) of each given number:

(c) $11^{3142}$

(d) $9^{9999}$

(e) $3^{641}$

## 2 Modular Potpourri

Note 6

Prove or disprove the following statements:

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

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

(c) $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{6}$.

# 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?

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

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

(d) Does 4 have an inverse modulo 8?

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

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