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}

Solution:

(a) i, iii is the answer. Note that for ii, $m \mid a+b$ is equivalent to $a \equiv -b \pmod{m}$.

(b) i is the only answer. For ii, remember that you can't apply the mod to the exponent. Simple counterexample:

$$6^5 \equiv 4^5 \pmod{4} \not\Longrightarrow 6 \equiv 4 \pmod{4}$$

(c) 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.

(d) 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

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

(e) Notice that $3^4 = 9^2$ so using that $9^2 = 81 \equiv 1 \pmod{10}$, we have $3^4 \equiv 1 \pmod{10}$. We also have that $641 = 160 \cdot 4 + 1$, so

$$3^{641} \equiv 3^{4(160)} \cdot 3 \equiv 1^{160} \cdot 3 \equiv 3 \pmod{10},$$

making the last digit a 3.

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

Solution:

(a) 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.

(b) 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.

(c) True. We can write $2x \equiv 4 \pmod{12}$ as $2x = 4 + 12k$ for some $k \in \mathbb{Z}$. Dividing by 2, we have $x = 2 + 6k$ for the same $k \in \mathbb{Z}$. This is equivalent to saying $x \equiv 2 \pmod{6}$.

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 $x \not\equiv x' \pmod{m}$?

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

$$\begin{aligned} xa(x - x') &\equiv 0 \cdot x \pmod{m} \\ \implies x - x' &\equiv 0 \pmod{m}. \\ \implies x &\equiv x' \pmod{m} \end{aligned}$$

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

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 $F_n = F_{n-1} + F_{n-2}$.