CS 70 Discrete Mathematics and Probability Theory
Summer 2025 Tate

DIS 1C

Modular Arithmetic Intro I

Note 6

Modular arithmetic: working number "mod m": restrict to only $\{0, 1, \ldots, m-1\}$; other numbers are *equivalent* to some number in this set.

Think of a clock; "13-o'clock" is the same as "1-o'clock"; $2m$ is the same as m, which is the same as 0. We can go the other way too; 0 is the same as $-m$, etc.

Saying $a \equiv b \pmod{m}$ means:

- a, b have same remainder when divided by m
- $a = b + km$ for some integer k
- $m \mid (a-b)$

Operations: Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.

Addition/subtraction: $a \pm c \equiv b \pm d \pmod{m}$

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

Exponentiation: $a^k \equiv b^k \pmod{m}$. You *cannot* apply the mod to the exponent.

There is no division; there are multiplicative inverses though: $x^{-1} \equiv a \pmod{m}$ means $ax \equiv 1 \pmod{m}$.

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}.

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

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

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

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

(c) 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 14?

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

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

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

(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, since $4x - 1$ is odd (and thus cannot be divisible by 8 either).

(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 Wilson's Theorem

Note 6

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

(a) Prove that $(p-1)! \equiv -1 \pmod{p}$ if p is prime. As a hint, consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

(b) Prove that $(p-1)! \equiv -1 \pmod{p}$ only if p is prime. As a hint, if p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

Solution:

(a) For the integers $1, \cdots, p-1$, every number has an inverse. However, it is not possible to pair a number off with its inverse when it is its own inverse. This happens when $x^2 \equiv 1 \pmod{p}$, or when $p \mid x^2 - 1 = (x-1)(x+1)$. Thus, $p \mid x-1$ or $p \mid x+1$, so $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. Thus, the only integers from 1 to $p-1$ inclusive whose inverse is the same as itself are 1 and $p-1$.

We reconsider the product $(p-1)! = 1 \cdot 2 \cdots p-1$. The product consists of 1, $p-1$, and pairs of numbers with their inverse, of which there are $\frac{p-1-2}{2} = \frac{p-3}{2}$. The product of the pairs is 1 (since the product of a number with its inverse is 1), so the product $(p-1)! \equiv 1 \cdot (p-1) \cdot 1 \equiv -1 \pmod{p}$, as desired.

(b) "$(p-1)! \equiv -1 \pmod{p}$ only if p is prime" is the same as "if $(p-1)! \equiv -1 \pmod{p}$, then p is prime." We'll prove this implication by contradiction.

Suppose for contradiction that $(p-1)! \equiv -1 \pmod{p}$ and p isn't prime. Because $(p-1)! \equiv -1 \pmod{p}$, we can write $(p-1)!$ as $p \cdot k - 1$ for some integer k.

Since p isn't prime, it has some prime factor q where $2 \leq q \leq n-2$, and we can write $p = q \cdot r$. Plug this into the expression for $(p-1)!$ above, yielding us $(p-1)! = (q \cdot r)k - 1 = q(rk) - 1 \implies (p-1)! \equiv -1 \pmod{q}$. However, we know q is a term in $(p-1)!$, so $(p-1)! \equiv 0 \pmod{q}$. Since $0 \not\equiv -1 \pmod{q}$, we have reached our contradiction.