Modular Arithmetic

Meeting #7

Justin Hua

McRoberts Math Circle

March 4, 2021

Outline

Warm-Up Problems

Problem

It is 7 p.m right now. What will the time be in 1000 hours?

- Try using modular arithmetic.

Problem

Find $4!$ *(mod 5)*

Warm-Up Problems

Problem

It is 7 p.m right now. What will the time be in 1000 hours?

- Try using modular arithmetic.
- The idea is to take modulo 24 since the time repeats in cycles of 24.

Problem

Find $4!$ *(mod 5)*

Warm-Up Problems

Problem

It is 7 p.m right now. What will the time be in 1000 hours?

- Try using modular arithmetic.
- The idea is to take modulo 24 since the time repeats in cycles of 24.
- We compute $1000 \equiv 16 \pmod{24}$

Problem

Find $4!$ *(mod 5)*

Warm-Up Problems

Problem

It is 7 p.m right now. What will the time be in 1000 hours?

- Try using modular arithmetic.
- The idea is to take modulo 24 since the time repeats in cycles of 24.
- We compute $1000 \equiv 16 \pmod{24}$
- We conclude that the time will be 7p.m $+16$ hours, which is 11 a.m

Problem

Find $4!$ *(mod 5)*

Review

Remember that last time, we introduced the idea of modular arithmetic.

Definition (Congruence)

We say

$$a \equiv b \pmod{n}$$

if and only if $a - b$ is divisible by n. That is, $\frac{a-b}{n} \in \mathbb{Z}$

Another way to think of this is that a is congruent to b modulo n if they have the same remainders when divided by n.

Example

$$12 \equiv 8 \equiv 4 \equiv 0 (\text{mod } 4)$$

$$31 \equiv 1 \equiv 4 (\text{mod } 3)$$

Typical Modular Arithmetic Problems

Problem

Find the remainder when 3^{16} is divided by 4.

- Don't actually compute 3^{16}

Typical Modular Arithmetic Problems

Problem

Find the remainder when 3^{16} is divided by 4.

- Don't actually compute 3^{16}
- What is 3 congruent to modulo 4?

Typical Modular Arithmetic Problems

Problem

Find the remainder when 3^{16} is divided by 4.

- Don't actually compute 3^{16}
- What is 3 congruent to modulo 4?
- We compute $3 \equiv -1 \pmod 4$

Typical Modular Arithmetic Problems

Problem

Find the remainder when 3^{16} is divided by 4.

- Don't actually compute 3^{16}
- What is 3 congruent to modulo 4?
- We compute $3 \equiv -1 \pmod 4$
- $3^{16} \equiv (-1)^{16} \equiv 1 \pmod 4$

Problems

Problem

Find the last digit of 7^{100}

- Don't actually compute 7^{100}

Problems

Problem

Find the last digit of 7^{100}

- Don't actually compute 7^{100}
- Take modulo 10?

Problems

Problem

Find the last digit of 7^{100}

- Don't actually compute 7^{100}
- Take modulo 10?
- We compute $7 \equiv -3 \pmod{10}$. However, this would still give a huge number

Problems

Problem

Find the last digit of 7^{100}

- Don't actually compute 7^{100}
- Take modulo 10?
- We compute $7 \equiv -3 \pmod{10}$. However, this would still give a huge number
- $7^2 \equiv -1 \pmod{10}$

Problems

Problem

Find the last digit of 7^{100}

- Don't actually compute 7^{100}
- Take modulo 10?
- We compute $7 \equiv -3 \pmod{10}$. However, this would still give a huge number
- $7^2 \equiv -1 \pmod{10}$
- $7^{100} \equiv (7^2)^{50} \equiv (-1)^{50} \equiv 1 \pmod{10}$

More Modular Arithmetic Problems

Problem (AoPS)

What is the remainder when 11^{2021} *is divided by* 12*?*

- Similar idea to many other problems. Don't compute

More Modular Arithmetic Problems

Problem (AoPS)

What is the remainder when 11^{2021} *is divided by* 12*?*

- Similar idea to many other problems. Don't compute
- What is something nice that 11 is congruent to modulo 12?

More Modular Arithmetic Problems

Problem (AoPS)

What is the remainder when 11^{2021} *is divided by* 12*?*

- Similar idea to many other problems. Don't compute
- What is something nice that 11 is congruent to modulo 12?
- $11 \equiv -1 \pmod{12}$

More Modular Arithmetic Problems

Problem (AoPS)

What is the remainder when 11^{2021} *is divided by* 12*?*

- Similar idea to many other problems. Don't compute
- What is something nice that 11 is congruent to modulo 12?
- $11 \equiv -1 \pmod{12}$
- $11^{2021} \equiv (-1)^{2021} \equiv -1 \pmod{12}$

Problem

What is the remainder when 2015^{2015} *is divided by 2014?*

- This one is easier. Once again, that would take years to compute.

Problem

What is the remainder when 2015^{2015} *is divided by 2014?*

- This one is easier. Once again, that would take years to compute.
- $2015 \equiv 1 \pmod{2014}$

Problem

What is the remainder when 2015^{2015} is divided by 2014?

- This one is easier. Once again, that would take years to compute.
- $2015 \equiv 1 \pmod{2014}$
- $2015^{2015} \equiv 1^{2015} \equiv 1 \pmod{2014}$

Modular Inverses

What about division in modular arithmetic?
We introduce the concept of a modular inverse.

Definition

We call a^{-1} the *modular inverse* of a modulo m if

$$a \cdot a^{-1} \equiv 1 \pmod{m}$$

Example

Let us take modulo 5. The inverse of 1,2,3,4 are 1,3,2,4 respectively.

$$\begin{cases} 1 \cdot 1 \equiv 1 \pmod{5} \\ 2 \cdot 3 \equiv 1 \pmod{5} \\ 3 \cdot 2 \equiv 1 \pmod{5} \\ 4 \cdot 4 \equiv 1 \pmod{5} \end{cases}$$

Inverse Problems

Problem

Solve $3x \equiv 2$ *(mod 5)*

- Find a solution that works. Try $\{0, 1, 2, 3, 4\}$.

Inverse Problems

Problem

Solve $3x \equiv 2$ *(mod 5)*

- Find a solution that works. Try $\{0, 1, 2, 3, 4\}$.
- Multiply both sides by 3^{-1}

Inverse Problems

Problem

Solve $3x \equiv 2$ *(mod 5)*

- Find a solution that works. Try $\{0, 1, 2, 3, 4\}$.
- Multiply both sides by 3^{-1}
- Our equation becomes $3^{-1} \cdot 3x \equiv 2 \cdot 3^{-1} \pmod 5$

Inverse Problems

Problem

Solve $3x \equiv 2$ *(mod 5)*

- Find a solution that works. Try $\{0, 1, 2, 3, 4\}$.
- Multiply both sides by 3^{-1}
- Our equation becomes $3^{-1} \cdot 3x \equiv 2 \cdot 3^{-1} \pmod 5$
- Notice that on the LHS, $3 \cdot 3^{-1} \equiv 1 \pmod 5$. Find the modular inverse of 3.

Inverse Problems

Problem

Solve $3x \equiv 2$ *(mod 5)*

- Find a solution that works. Try $\{0, 1, 2, 3, 4\}$.
- Multiply both sides by 3^{-1}
- Our equation becomes $3^{-1} \cdot 3x \equiv 2 \cdot 3^{-1} \pmod 5$
- Notice that on the LHS, $3 \cdot 3^{-1} \equiv 1 \pmod 5$. Find the modular inverse of 3.
- The modular inverse of 3 is 2. Thus, the solutions to this equation are all x such that $x \equiv 4 \pmod 5$. Notice that $x = 4$ works.

Resources

Art of Problem Solving-artofproblemsolving.com

1. Problems
2. Alcumus Game
3. Problem Solving Books
4. Classes