Modular Arithmetic

And Exciting Card Tricks!

Judy Li

Maths Soc Presentation

October 1 2024

1. Definitions
2. Card trick
3. The magic (maths) behind the trick

New notation

- What do we mean by remainder?
- What does it mean for one number to be divisible by another?

Definition (Congruence)

For a positive integer n and integers a, b, $a \equiv b \pmod{n}$ if a and b leave the same remainder when divided by n.

Examples

Definition (Congruence)

For a positive integer n and integers a, b, $a \equiv b \pmod{n}$ if a and b leave the same remainder when divided by n.

- Clocks

Example

$$
\begin{aligned}
5 &\equiv 2 \pmod{3} \\
-1 &\equiv 3 \pmod{4} \\
100 &\equiv 2 \pmod{7} \\
100 &\equiv 30 \pmod{7} \\
100 &\equiv -5 \pmod{7}
\end{aligned}
$$

Laws of Modular Arithmetic

- Addition: if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$.
- Multiplication: if $a \equiv b \pmod{n}$, then $ak \equiv bk \pmod{n}$.
- Exponentiation: if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

Rules

- 2 stacks of cards: A, 2, 3, 4 and 4, 3, 2, A.
- Shuffle: putting the top card to the bottom of each stack
- I'll give you a magic word: for each letter, you tell me which stack I should shuffle
- After shuffling with all the letters, I'll remove the top card from each stack and shuffle the remaining cards using the word again...

...abracadabra!

Magic words:

- abracadabra
- mathematics

Clockwork configurations

Shuffle: going counterclockwise around a clock of 4 cards.

Chinese Remainder Theorem

- Can we always find a (positive) number N such that $N \equiv -1 \mod m, m-1, \ldots, 3, 2$?

Theorem (Chinese Remainder Theorem: Weaker Version)

Given two sequences of numbers $A = [a_1, a_2, \ldots, a_n]$ and $M = [m_1, m_2, \ldots, m_n]$, where all elements of M are pairwise coprime, there always exists a unique solution for x mod L, where $L = m_1 m_2 \cdots m_n$, such that x satisfies the following:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem: Stronger Version)

Given two sequences of numbers $A = [a_1, a_2, \ldots, a_n]$ *and* $M = [m_1, m_2, \ldots, m_n]$, *let* $g = gcd(m_1, \ldots, m_n)$ *and* $h = lcm(m_1, \ldots, m_n)$. *If* $a_1 \equiv a_2 \equiv \ldots \equiv a_n \pmod{g}$, *then there is a unique solution for* x *mod* h *such that*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

Card Trick

- For the card trick, we have $a_1 = a_2 = \cdots = a_n = -1$, so we can always find a magic word regardless of how many cards we use.
- But the words will get pretty long!

Example Problem

Example

Find all integers x such that

$$x \equiv 3 \pmod{4}$$
$$x \equiv 5 \pmod{9}$$

Thank you!