Modular Arithmetic

Meeting #6

Justin Hua

McRoberts Math Circle

February 19, 2021

Outline

Warm-Up

Problem (AMC 12B 2021 # 7)

Let $N = 34 \cdot 34 \cdot 63 \cdot 270$. What is the ratio of the sum of the odd divisors of N to the sum of the even divisors of N?

Hint: Prime factorize N and think about a single odd divisor; does it have a exponent of 2? What happens when we take an odd divisor and multiply it by 2?

Division Algorithm

Theorem (Division Algorithm)

Given an integer k, we can express any integer n in a unique way with some q and r such that:

$$n = kq + r$$

where $0 \leq r < k$. We call k the remainder when n is divided by k and call q the quotient.

Example

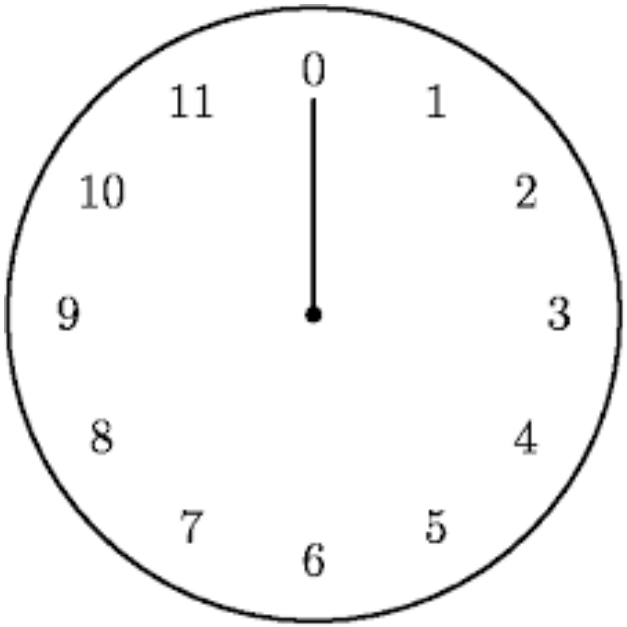
Let us take $k = 3$ and $n = 23$ Then notice that

$$23 = (3 \cdot 7) + 2$$

Here, 2 is the remainder and 7 is the quotient.

Clock Example

A perfect example of modular arithmetic in the world is the usage of clocks.



For example, lets say that the world was created on January 1st. At the end of the fourth day, would we call the time 96 hours? Sounds like a pretty terrible idea.
So, in real life, we take the time of the day in cycles of **24 hours**.
We call this taking the time *modulo 24*

Modular Congruences

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

$$8 \equiv 6 \equiv 2 \equiv 0 (\text{mod } 2\ )$$

$$23 \equiv 2 \equiv 5 (\text{mod } 3\ )$$

Residues

It is often useful to denote the smallest positive integer congruent to some number a.

Definition (Modular Residue)

We call a nonnegative integer b the *residue* of an integer a modulo n if b satisfies:

1. $a \equiv b \mod n$
2. $0 \leq b < n$

Example

The residue of 47 modulo 9 is 2 because:

1. $47 \equiv 2 \mod 9$
2. $0 \leq 2 < 9$

Problem

What is the residue of 6 modulo 5?

Modular Operations

Modular arithmetic has various nice operations like addition, subtraction, multiplication and exponentiation.

Example (Addition)

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a + c \equiv b + d \pmod{n}$$

Example (Subtraction)

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a - c \equiv b - d \pmod{n}$$

Modular Operations

Example (Multiplication)

If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$a \cdot c \equiv b \cdot d \pmod{n}$$

Example (Exponentiation)

If $a \equiv b \pmod{n}$, then

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

for any integer k

Problem Solving

Why is this useful?

Problem

Find the units digit of $1453212 + 123504 + 98043$.

Problem (AMC 12B # 5 2016)

The War of 1812 *started with a declaration of war on Thursday, June* 18, 1812. *The peace treaty to end the war was signed* 919 *days later, on December* 24, 1814. *On what day of the week was the treaty signed?*

Problem (AoPS)

What is the remainder when 11^{2020} *is divided by* 12*?*

Resources

Art of Problem Solving-artofproblemsolving.com

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