Modular Arithmetic

Shef Scholars Winter Math Camp

January 2025

Introduction to Modular Arithmetic

Modular arithmetic is often referred to as "clock arithmetic" because it shares similarities with how time works on a standard 12-hour clock. For example, consider the following scenario:

If it's 10 o'clock and you add 5 hours, you end up at 3 o'clock. This happens because $10+5 = 15$, but on a 12-hour clock, $15 \mod 12 = 3$. In modular arithmetic, this is expressed as:

$$15 \equiv 3 \pmod{12}.$$

This system allows us to work with remainders instead of large numbers, simplifying many problems in number theory. Modular arithmetic also has some powerful properties that make it useful for solving congruences and other mathematical challenges.

Key Concepts and Properties

- **Definition of Congruence:** Two integers a and b are said to be congruent modulo m, written $a \equiv b \pmod{m}$, if $m \mid (a - b)$, meaning that m divides $a - b$ exactly.
- **Arithmetic Operations:** Congruences behave much like regular equations:
  - **Addition:** If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.
  - **Subtraction:** If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$.
  - **Multiplication:** If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \cdot c \equiv b \cdot d \pmod{m}$.
- **Division Caution:** Division is more subtle in modular arithmetic. You cannot simply divide both sides of a congruence unless the divisor and the modulus are coprime. For example, $4x \equiv 8 \pmod{12}$ cannot be divided by 4 without further considerations.
- **Patterns in Powers:** When we take powers of a number, the possible remainders (or congruences) can sometimes reduce to a smaller set. For example:

  $$x \pmod 3 \text{ can be } 0, 1, \text{ or } 2, \quad \text{but } x^2 \pmod 3 \text{ can only be } 0 \text{ or } 1.$$

  This happens because squaring x eliminates some of the possible remainders. Understanding these patterns helps simplify many modular arithmetic problems.
- **Powers and Patterns:** Powers often exhibit repeating patterns in modular arithmetic. Recognizing these patterns can simplify calculations. For example, powers of $2 \mod 7$ follow the sequence:

  $$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 1, \quad 2^4 \equiv 2 \pmod{7}.$$

  Notice the pattern repeats every three terms.

Let's apply these concepts to some problems.

Problems

1. Find the remainder when 2^{2019} is divided by 7.
2. Determine all natural numbers n for which $10^n + 5$ is divisible by 15.
3. What remainder does the number $2017^{2017^{2017}}$ leave when divided by 11?
4. Determine the last three digits of the number A, if

$$A = 9 \cdot 99 \cdot 999 \cdot \ldots \cdot 99\ldots9,$$

   and if the last number written contains 9999 nines.
5. Find all natural numbers a and b for which $2^a - 3^b = 1$.
6. Find all natural numbers a and b for which $3^a - 2^b = 1$.
7. Given natural numbers a, b, c such that $a^2 + b^2 = c^2$:
   a) Prove that the number abc is divisible by 30.
   b) Prove that the number abc is divisible by 60.
8. For each non-negative integer n, define $A_n = 2^{3n} + 3^{6n+2} + 5^{6n+2}$. Determine the greatest common divisor of the numbers $A_0, A_1, A_2, \ldots, A_{2020}$.
9. Prove that the number $19 \cdot 8^n + 17$ is composite for any natural number n.