Modular Arithmetic

Serena An–8/17/19

1 Definitions

Theorem 1.1: Residue Definition

The **residues** $\pmod{m}$ are the integers $\{0, 1, 2, \ldots, m-1\}$, the possible remainders upon division by m.

Theorem 1.2: Congruence Definition

$a \equiv b \pmod{m} \Longleftrightarrow m$ divides $a - b$

2 Arithmetic

There are no restrictions on addition and subtraction. It's just like what we're used to.

Theorem 2.1: Addition

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

Theorem 2.2: Subtraction

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$.

Theorem 2.3: Multiplication

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Theorem 2.4: Exponents

If $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$ for all positive integers k.

This follows from the multiplication theorem.

Theorem 2.5: Inverse

For all a **relatively prime** to m, the inverse of a, denoted a^{-1}, is the number such that $a \cdot a^{-1} \equiv 1 \pmod{m}$.

Problem 2.1

Why does a have to be relatively prime to m for an inverse to exist?

Problem 2.2

Find the inverses of 1, 2, 3, 4, 5, and 6 $\pmod 7$.

Theorem 2.6: Division

If $a \equiv b \pmod m$ and $c \equiv d \pmod m$ with c, d relatively prime to m, then $\frac{a}{c} \equiv \frac{b}{d} \pmod m$.

Note that dividing by r is the same as multiplying by r^{-1}.

Theorem 2.7

The equation $ax \equiv b \pmod m$ always has a solution when $\gcd(a, m) = 1$.

Proof. Set $x \equiv a^{-1}b \pmod m$. ■

3 Euler Totient Function (φ)

Theorem 3.1: Euler totient function

The Euler totient function, or phi function, represented by $\varphi(n)$ or $\phi(n)$, counts the number of positive integers at most than n and relatively prime to n. We define $\varphi(1) = 1$. If the prime factorization of $n > 1$ is $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, then

$$\begin{aligned} \varphi(n) &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_m}\right) \\ &= p_1^{\alpha_1 - 1}(p_1 - 1)p_2^{\alpha_2 - 1}(p_2 - 1)\dots p_k^{\alpha_k - 1}(p_k - 1). \end{aligned}$$

Problem 3.1: (AMSP)

Find the values of $\varphi(n)$ for:

1. $n = 6$
2. $n = 100$
3. $n = 1000$
4. $n = p^\alpha$, p a prime

4 Euler's Totient Theorem and Fermat's Little Theorem

Theorem 4.1: Euler's Totient Theorem

For a relatively prime to m, we have $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Theorem 4.2: Fermat's Little Theorem

For a relatively prime to a prime p, we have $a^{p-1} \equiv 1 \pmod{p}$.

Since $\varphi(p) = p - 1$ for prime p, Fermat's Little Theorem is just a special case of Euler's Totient Theorem.

Problem 4.1

Find the remainder when 2^{100} is divided by 27.

Problem 4.2

Find the remainder when 193^{193} is divided by 13.

Problem 4.3

Find the remainder when $1^{18} + 2^{18} + 3^{18} + \cdots + 18^{18}$ is divided by 19.

5 Chinese Remainder Theorem

Theorem 5.1: Chinese Remainder Theorem

The system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{b_1} \\ x &\equiv a_2 \pmod{b_2} \\ &\dots \\ x &\equiv a_n \pmod{b_n} \end{aligned}$$

where $b_1, b_2, \dots, b_n$ are pairwise relatively prime has one distinct solution for x modulo $b_1 b_2 \dots b_n$.

This is a theorem that you will end up using without really thinking that you are using it.

Exercise 5.1

Solve the following system of congruences.

$$x \equiv 3 \pmod{5}$$
$$x \equiv 2 \pmod{17}$$

Solution 5.1: We can write $x = 5m + 3 = 17n + 2$ for integers m and n. Taking $5m + 3 = 17n + 2$ modulo 5, we get $3 \equiv 2n + 2 \pmod{5}$, or $2n \equiv 1 \pmod{5}$. Solving, we get $n \equiv 3 \pmod{5}$, so we can write $n = 5k + 3$ for some integer k. Then $x = 17n + 2 = 17(5k + 3) + 2 = 85k + 53$, so $x \equiv 53 \pmod{85}$.

Exercise 5.2: (MATHCOUNTS 2019 School Sprint Round #30)

Chloe charged for admission to her play on three different nights. Each night, a different number of people were in attendance, but remarkably, Chloe collected $541 each night. If the admission charges for each child and each adult were $9 and $17, respectively, how many people in total came to the three showings?

Solution 5.2: Let c and a be the number of children and adults who attended on any of the days. We have the equation $9c + 17a = 541$. Taking this equation $\pmod{9}$, We get that $17a \equiv 8a \equiv 1 \pmod{9}$, so $a \equiv 8 \pmod{9}$. Now we try some values for a. If $a = 8$, then $c = 45$. If $a = 17$, then $c = 28$. If $a = 26$, then $c = 11$. These must be the three combinations of adults and children for the three nights, so the total number of people is $8 + 45 + 17 + 28 + 26 + 11 = \boxed{135}$.

6 Problems

Problem 6.1:

What is the units digit of 3^{2019}?

Solution 6.1: The units digit of powers of 3 repeats every four: 3, 9, 7, 1, etc. Since $2019 \equiv 3 \pmod{4}$, the units digit of 3^{2019} is $\boxed{7}$.

Problem 6.2: (CMMS)

In the decimal expansion of two-sevenths, what is the hundredth digit to the right of the decimal point?

Solution 6.2: The decimal expansion of two-sevenths is $0.\overline{285714}$, where the bar denotes the repeating block. The digits repeat every 6, and since $100 \equiv 4 \pmod{6}$, the desired digit is $\boxed{7}$.

Problem 6.3: (CMMS)

It is currently 5 o'clock. What time will it be 1000 hours from now?

Solution 6.3: The time repeats every 12 hours (without regard to am/pm). $1000 \equiv 4 \pmod 6$ so it will be $\boxed{\text{9 o'clock}}$.

Problem 6.4: (CMMS)

During her history class, Priyanka writes her name over and over again on a sheet of paper. She completes 955 letters before the paper is taken away by her teacher and she is reminded to pay attention in class. What is the last letter she writes?

Solution 6.4: 'Priyanka' has 8 letters, and $955 \equiv 3 \pmod 8$, so the last letter she writes is $\boxed{\text{i}}$.

Problem 6.5: (Alcumus)

Let $S = 2010 + 2011 + \cdots + 4018$. Compute the residue of S, modulo 2009.

Solution 6.5: We can subtract 2009 from all the terms to get that $S \equiv 1 + 2 + \cdots + 2009 \pmod{2009}$. Then $1 + 2 + \cdots + 2009 = \frac{2009 \cdot 2010}{2} = 2009 \cdot 1005$, which is divisible by 2009. Thus, $\boxed{S \equiv 0 \pmod{2009}}$.

Problem 6.6: (MATHCOUNTS)

What is the remainder when 11^{12} is divided by 13?

Solution 6.6: Fermat's Little Theorem states that $a^{p-1} \equiv 1 \pmod p$ for a relatively prime to p. For this problem, we take $a = 11$ and $p = 13$ to get that $\boxed{11^{12} \equiv 1 \pmod{13}}$.

Problem 6.7:

How many positive integers less than 216 are not divisible by 2, 3, 5, or 7?

Solution 6.7: We see that $2 \cdot 3 \cdot 5 \cdot 7 = 210$, which is close to 216. By the φ function, $\varphi(210) = (2-1)(3-1)(5-1)(7-1) = 48$, so there are 48 numbers less than 210 that are not divisible by 2, 3, 5, or 7. Then considering 211, 212, 213, 214, and 215, only 211 is not divisible by 2, 3, 5, or 7. In all, there are $\boxed{49}$ such numbers.

Problem 6.8: (Alcumus)

Let $A = 111111$ and $B = 142857$. Find a positive integer N with six or fewer digits such that N is the multiplicative inverse of AB modulo 1,000,000.

Solution 6.8: We see that $9A = 999999$ and $7B = 999999$ are both very close to 1000000. In fact, $9A \equiv -1 \pmod{1000000}$ and $7B \equiv -1 \pmod{1000000}$, so $63AB \equiv 1 \pmod{1000000}$, so the inverse of AB is $\boxed{63}$.

Problem 6.9: (Alcumus)

Compute the multiplicative inverse of 201 modulo 299. Express your answer as an integer from 0 to 298.

Solution 6.9: First, $3 \cdot 201 = 603 \equiv 5 \pmod{299}$. Then $5 \cdot 60 = 300 \equiv 1 \pmod{299}$. All together, $3 \cdot 60 = \boxed{180}$ is the multiplicative inverse of $201 \pmod{299}$.

Problem 6.10:

A group of friends distributed some candy amongst themselves. If some people got 15 candies each, there would be 4 candies left over. If some people got 19 candies each, there were 7 candies left over. If there were at least 100 candies, what is the smallest possible number of candies?

Solution 6.10: Let C be the number of candies. From the problem statement, we get the system

$$\begin{cases} C & \equiv 4 \pmod{15} \\ C & \equiv 7 \pmod{19}. \end{cases}$$

To solve, let $C = 15x + 4$ for some integer x. Then $15x + 4 \equiv 7 \pmod{19} \implies 15x \equiv 3 \pmod{19}$. Since 3 is relatively prime to 19, we can divide both sides by 3 to get $5x \equiv 1 \pmod{19}$, so $x \equiv 4 \pmod{19}$. Let $x = 19y + 4$. Substituting this in the equation for C, $C = 15(19y + 4) + 4 = 285y + 64$. Since there are at least 100 candies, the smallest possible number is $285 + 64 = \boxed{349}$.