Modular Arithmetic

Serena An–3/18/2019

1 Introductory Problems

Problem 1.1

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

Problem 1.2: (CMMS)

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

Problem 1.3: (CMMS)

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

2 Modular Arithmetic Definitions and Notation

Theorem 2.1: Residue Definition

The **residues** $\pmod{m}$ are the integers $\{0, 1, 2, \ldots, m-1\}$, the possible remainders upon division by m. A **residue class** $\pmod{m}$ includes all integers with the same remainder upon division by m.

Theorem 2.2: Modulus, Modulo, Congruent

A **modulus** (noun) is the length of the repeating block. **Modulo** (preposition) means an operator in the modulus. We say two integers a and b are **congruent** modulo m if they leave the same remainder upon division by m.

Theorem 2.3: Notation

We use the word $\bmod$ as a shorthand for modulo and the symbol $\equiv$ to denote congruence.

Theorem 2.4: Congruence Definition

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

To clarify, we would say that $a \equiv b$ modulo m and that m is the modulus. It would be incorrect to say $a \equiv b$ modulus m or that m is the modulo. However, this distinction is not important for just doing the math.

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 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

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

$\varphi(n)$ is an integer for all n, and $\varphi(n) < n$ for all $n > 1$.

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

The Euler totient function is very important in modular arithmetic, and will show up again shortly.

4 Arithmetic

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

Theorem 4.1: Addition

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

Theorem 4.2: Subtraction

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

These two theorems could actually be combined into one (why?).

Theorem 4.3: Multiplication

If $a \equiv b \pmod{m}$, then $ar \equiv br \pmod{m}$ for all integers r.
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$.

Theorem 4.4: 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 4.5: 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 4.1

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

Problem 4.2

How many positive integers $a \leq m$ have an inverse $\pmod{m}$?

Problem 4.3

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

Theorem 4.6: Inverses are unique (part 1)

Let a and m be relatively prime positive integers. Let the set of positive integers relatively prime to m and less than m by $R = \{a_1, a_2, \ldots, a_{\varphi(m)}\}$. Prove that $S = \{aa_1, aa_2, \ldots, aa_{\varphi(m)}\}$ is the same as R when reduced $\pmod{m}$.

Proof. (From *Olympiad Number Theory Through Challenging Problems*)

Every element in S is relatively prime to m. Also, R and S have the same number of elements, so if we can prove that no two elements of S are congruent $\pmod{m}$, we would be done. However $aa_x \equiv aa_y \pmod{m} \implies a(a_x - a_y) \equiv 0 \pmod{m} \implies a_x \equiv a_y \pmod{m}$, which happens only when $x = y$. Therefore, the elements of S are distinct $\pmod{m}$ and we are done. ■

Theorem 4.7: Inverses are unique (part 2)

When $\gcd(a, m) = 1$, a always has a distinct inverse $\pmod{m}$.

Proof. (From *Olympiad Number Theory Through Challenging Problems*)

We know that $1 \in R$, where we define $R = \{a_1, a_2, \ldots, a_{\varphi(m)}\}$ to be the same as above. By Theorem 1, there must be some element in $\{aa_1, aa_2, \ldots, aa_{\varphi(m)}\}$ congruent to $1 \pmod{m}$. Thus, there exists some a_x such that $aa_x \equiv 1 \pmod{m}$. ■

Theorem 4.8: Division

If $a \equiv b \pmod{m}$, then $\frac{a}{r} \equiv \frac{b}{r} \pmod{m}$ for all integers r *relatively prime* to m.
If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ with $\gcd(c, m) = \gcd(d, m) = 1$, then $\frac{a}{c} \equiv \frac{b}{d} \pmod{m}$.

Dividing by r is the same as multiplying by the inverse of r, or r^{-1}.

So, the only thing we need to be careful of is division, since we must make sure that we are dividing by numbers *relatively prime* to the modulus.

Theorem 4.9

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

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

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

Theorem 5.1: Euler's Totient Theorem

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

Proof. From Theorem 4.6, the sets $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ and $\{aa_1, aa_2, \ldots, aa_{\varphi(m)}\}$ are the same $\pmod{m}$. Therefore, the products of each set must be the same $\pmod{m}$, and we get

$$a^{\varphi(m)} a_1 a_2 \ldots a_{\varphi(m)} \equiv a_1 a_2 \ldots a_{\varphi(m)} \implies a^{\varphi(m)} \equiv 1 \pmod{m}$$

. ■

Theorem 5.2: Fermat's Little Theorem

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

Proof. Since $\varphi(p) = p - 1$ for prime p, this follows from Euler's Totient Theorem. ■

Problem 5.1

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

Problem 5.2

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

Problem 5.3

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

6 Chinese Remainder Theorem

Theorem 6.1: 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, ..., 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 6.1

Solve the following system of congruences.

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod{17} \end{aligned}$$

Solution 6.1: 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 6.2: (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 6.2: 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 $8 + 45 + 17 + 28 + 26 + 11 = \boxed{135}$.

Problem 6.1

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?

7 Divisibility Rules

Exercise 7.1

Prove the divisibility rule for 9.

Solution 7.1: Since $10 \equiv 1 \pmod 9$, if $N = a_0 \cdot 10^{a_0} + a_1 \cdot 10^{a_1} + a_2 \cdot 10^{a_2} + \dots a_n \cdot 10^{a_n}$, where the a_i are single digits, then $N \equiv a_0 + a_1 + a_2 + \dots a_n \pmod 9$.

Exercise 7.2

Prove the divisibility rule for 11.

Solution 7.2: Since $10^n \equiv (-1)^n \pmod 11$, $10^n \equiv 1 \pmod{11}$ for even n and $10^n \equiv -1 \pmod{11}$ for odd n. So, if $N = a_0 \cdot 10^{a_0} + a_1 \cdot 10^{a_1} + a_2 \cdot 10^{a_2} + \dots a_n \cdot 10^{a_n}$, where the a_i are single digits, then $N \equiv a_0(-1)^0 + a_1(-1)^1 + a_2(-1)^2 + \dots a_n(-1)^n \equiv a_0 - a_1 + a_2 - a_3 + a_4 - a_5 + \dots + a_n(-1)^n \pmod{11}$.

Exercise 7.3

Prove the divisibility rule for 7.

Solution 7.3: Let N be the number that we want to test. Express N as $10A + B$, where B is a single digit number. Applying the divisibility by 7 rule to N, we end up with $A - 2B$. Consider $10(A - 2B)$. 7 divides $A - 2B$ if and only if 7 divides $10(A - 2B)$. Note that $10(A - 2B) \equiv 10A - 20B \equiv 10A + B \pmod 7$. Thus, 7 divides $A - 2B$ if and only if 7 divides $10A + B$, as desired.

8 Problems

Problem 8.1: (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?

Problem 8.2: (Alcumus)

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

Problem 8.3: (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.

Problem 8.4: (Alcumus)

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

Problem 8.5

Show that the square of any integer is congruent to 0 or $1 \pmod{4}$.

Problem 8.6: (M&IQ 1992)

enote by p_k the kth prime number. Show that $p_1 p_2 \ldots p_n + 1$ cannot be the perfect square of an integer.