ORMC AMC Group: Week 2
AMC Basics

October 2, 2022

1 Divisibility

Let X have digits $x_n, \dots, x_1, x_0$. That is,

$$X = 10^n x_n + \cdots + 10x_1 + x_0; \quad x_0, x_1, \dots, x_n \in \{0, 1, 2, \dots, 9\}.$$

For simplicity, we will allow $\overline{x_n \cdots x_1 x_0}$ to denote such a number X.

Some (less-known/less-intuitive) divisibility tests:

- X is divisible by 7 when 2 times its last digit, subtracted from the rest of the number, yields a number divisible by 7. That is, $\overline{x_n \dots x_1} - 2x_0$ is divisible by 7.
- X is divisible by 9 when the sum of its digits is divisible by 9.
- X is divisible by 11 when the alternating sum of its digits is divisible by 11.
  That is, $x_0 - x_1 + x_2 - x_3 + \cdots + (-1)^n x_n$ is divisible by 11.

Other things to know and remember when factoring numbers:

- Remember the factorizations from last week!
  - $2071 = 1728 + 343 = 12^3 + 7^3 = (12 + 7)(12^2 - 12 \cdot 7 + 7^2) = 19 \cdot 109$
  - $2021 = 2025 - 4 = 45^2 - 2^2 = (45 - 2)(45 + 2) = 43 \cdot 47$
- A number is prime precisely when it is not divisible by all primes less than or equal to its square root
  - Proof: Exercise [Hint: use contradiction. Suppose a composite number was not divisible by any prime $\leq$ its square root. Would this cause any problems?]

1.1 Problems

1. The 7-digit numbers $74A52B1$ and $326AB4C$ are each multiples of 3. What is the sum of all possible values of C?.

2. What is the prime factorization of 2023?

3. Which members of the sequence $101, 10101, 1010101, \dots$ are prime?

2 Basic Modular Arithmetic

In modular arithmetic, we consider only integers, and we focus on some **modulus**, m. The main difference between modular arithmetic and regular integer arithmetic is that two numbers are considered **congruent**, or equal "mod m" if their difference is divisible by m. We denote that two expressions are congruent mod m by writing: $a \equiv b \pmod{m}$. For example, if we take $m = 12$, then we would have: $-7 \equiv 5 \equiv 17 \pmod{12}$.

2.1 Modular Arithmetic Operations

Similar to regular integer arithmetic, you may add, subtract, or multiply both sides of a congruence mod m by the same thing:

- $a \equiv b, c \equiv d \pmod{m} \implies a \pm c \equiv b \pm d \pmod{m}$, because if $b - a$ and $d - c$ are both divisible by m, then so is $(b - a) \pm (d - c) = (b + d) - (a + c)$.
- $a \equiv b, c \equiv d \pmod{m} \implies ac \equiv bd \pmod{m}$, because because if $b - a$ and $d - c$ are both divisible by m, then so is: $b(d - c) + c(b - a) = bd - bc + bc - ca = bd - ca$

Unfortunately, we cannot do division. For example, consider $7 \equiv 12 \pmod{5}$. 12 is usually divisible by 2, but what would we do with the 7? Instead of dividing, we use **inverses**. The inverse of $n \mod m$ is some number, written n^{-1}, such that $n^{-1}n \equiv nn^{-1} \equiv 1 \pmod{m}$. The inverse of $n \mod m$ exists precisely when $\gcd(m, n) = 1$.

2.2 Problems

1. Suppose $\overline{x_n \cdots x_1 x_0} \equiv 0 \pmod{13}$. For what values k is it true that $\overline{x_n \cdots x_1} - kx_0 \equiv 0 \pmod{13}$?

2. Find the remainder when $1 + 2 + \cdots + 2022$ is divided by 1000.

3. Let S be a subset of $\{1, 2, 3, \ldots, 50\}$ such that no pair of distinct elements in S has a sum divisible by 7. What is the maximum number of elements in S?

4. In year N, the 300^{th} day of the year is a Tuesday. In year $N + 1$, the 200^{th} day is also a Tuesday. On what day of the week did the 100^{th} day of year $N - 1$ occur?

5. Determine the smallest positive integer m such that $m^2 + 7m + 89$ is a multiple of 77.

3 Modular Arithmetic Applications and Tools

Some important theorems that involve and/or are derived using modular arithmetic:

1. Wilson's Theorem: for a prime p, $(p-1)! \equiv -1 \pmod{p}$.
   (a) Each number in the set $\{2, \ldots, p-2\}$ has a unique inverse, which is also in the set. So the product of all these is congruent to 1, leaving us with $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$.
2. Fermat's Little Theorem: for an odd prime p and any integer a, $a^p \equiv a \pmod{p}$.
   (a) This is usually proved by induction, and involves the fact that the binomial coefficient $\binom{p}{k}$ is divisible by p for $0 < k < p$. We have $1^p \equiv 1$ and via induction, $(a+1)^p \equiv a^p + 1 \equiv a + 1$.
3. Euler's Totient Theorem: Let $\phi(n)$ be the number of integers $0 < k < n$ such that $\gcd(k, n) = 1$. Then, $a^{\phi(n)} \equiv 1 \pmod{n}$ for any a relatively prime to n.
   (a) Note that $\{k \mid 0 < k < n, \gcd(k, n) = 1\} = \{ak \mid 0 < k < n, \gcd(k, n) = 1\}$. Letting P denote the product of all the elements in the first set, we have $P \equiv a^{\phi(n)} P \implies a^{\phi(n)} \equiv 1$.
4. Chinese Remainder Theorem (CRT): The system of equations $x = a_1 \pmod{m_1}, \ldots, x = a_k \pmod{m_k}$ has exactly one integer solution $0 \leq x < m_1 m_2 \cdots m_k$.

3.1 Problems

1. For what values of $0 < n \leq 25$ is $\frac{(n-1)!}{n}$ an integer?

2. What is the value of $3^{2022} \pmod{223}$?

3. Let $a_n = 6^n + 8^n$. Determine the remainder upon dividing a_{83} by 49.

4. Find the smallest solution to this system of congruences:

$$\begin{aligned} x &\equiv 1 \mod 2 \\ x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 5 \\ x &\equiv 4 \mod 7 \end{aligned}$$

4 Using Modular Arithmetic

Advice for using modular arithmetic:

- For modular exponentiation:
  - Use Euler's Theorem and Fermat's Little Theorem to reduce large exponents
  - When not checking for a pattern, use repeated squaring. i.e. $7^8 \equiv 9^4 \equiv 1^2 \equiv 1 \pmod{10}$, as opposed to $7 \cdot 7 \equiv 9, 9 \cdot 7 \equiv 3, \ldots$.
- When to use modular arithmetic as a tool:
  - Checking when some expression is an integer
  - Checking for divisibility, or when something is (almost) equally divided
  - Solving an equation for integer solutions (isolate a prime p, then work $\bmod p$)
- General Advice
  - In general, things that seem "large" in modular arithmetic can be simplified down to something smaller, or involve some repeated pattern.
  - You can break down a very large modulus by its prime factors, then use the CRT to find the solution. For example, instead of working directly $\bmod 52$, work $\bmod 4$ and $\bmod 13$ first.

4.1 Problems

1. Let $a_1, a_2, \ldots, a_{2018}$ be a strictly increasing sequence of positive integers such that

$$a_1 + a_2 + \cdots + a_{2018} = 2018^{2018}.$$

   What is the remainder when $a_1^3 + a_2^3 + \cdots + a_{2018}^3$ is divided by 6?

2. Let $N = 123456789101112\ldots4344$ be the 79-digit number that is formed by writing the integers from 1 to 44 in order, one after the other. What is the remainder when N is divided by 45?

3. There is a pile of eggs. Joan counted the eggs, but her count was off by 1 in the 1's place. Tom's count was off by 1 in the 10's place. Raoul was off by 1 in the 100's place. Sasha, Jose, Peter, and Morris all counted the eggs and got the correct count. When these seven people added their counts together, the sum was 3162. How many eggs were in the pile?

4. Find the least positive integer n for which $2^n + 5^n - n$ is a multiple of 1000.