SMC IMONST Workshop 2024 (Day 2: Number Theory)

Vong Jun Yi · Phua Yufan

September 2024

Contents

Before You Begin...

This handout was written specifically for a two-day workshop to prepare members of Sunway Mathematics Club for IMONST1 2024.

As of 2023, each IMONST1 test lasts for 2 1/2 hours and consists of 30 questions: first 10 questions are worth 1 point, next 10 questions are worth 3, and the last 10 questions are worth 6. The maximum score attainable is 100 points.

A typical IMONST1 test may cover the following topics as mentioned on their official website:

- **Number Theory:** Properties of Integers, Primes, Divisibility, Modulo Arithmetic.
- **Algebra:** Algebraic Expressions, Factorization, Equations, Polynomials, Inequalities, Sequences, Functions.
- **Combinatorics (Counting):** Basic Counting, Pigeonhole Principle, Permutations and Combinations.
- **Geometry:** Measurements (Angles, Lengths, Areas, Volumes), Circles, Triangles, Quadrilaterals, Polygons, Similar Figures, Geometric Transformation.

In this handout, we have included actual questions from IMONST1 so that you can gauge how the difficulty of the questions has varied throughout the years. All credits for IMONST1 problems go to IMO Committee Malaysia. In addition, we have also included problems from other contests of similar style and format to supplement some of the topics covered in this handout.

Abbreviations:
PX - Problem #X from Primary category
JY - Problem #Y from Junior category
SZ - Problem #Z from Senior category

§1 Prime Numbers

Prime numbers are integers greater than 1 that have no positive divisors other than 1 and themselves. The study of prime numbers includes various theorems and properties.

§1.1 The Fundamental Theorem of Arithmetic

The Fundamental Theorem of Arithmetic states that every integer greater than 1 can be uniquely factored into prime numbers. This factorization is unique except for the order of the factors. Formally, if n is a positive integer greater than 1, then:

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where $p_1, p_2, \ldots, p_k$ are distinct prime numbers and $e_1, e_2, \ldots, e_k$ are positive integers.

§1.2 Finding the Number of Factors

If a number n has a prime factorization given by:

$$n = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_k^{e_k}$$

where $p_1, p_2, \ldots, p_k$ are distinct prime numbers and $e_1, e_2, \ldots, e_k$ are their respective powers, then the number of positive factors of n is given by:

$$\text{Number of positive factors of } n = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

Example 1.1

How many positive divisors does 84 have?

Solution. We can perform the prime factorisation of 84:

$$84 = 2^2 \times 3 \times 7$$

To find the number of factors:

- The exponent of 2 is 2, so it contributes $2 + 1 = 3$ factors.
- The exponent of 3 is 1, so it contributes $1 + 1 = 2$ factors.
- The exponent of 7 is 1, so it contributes $1 + 1 = 2$ factors.

Thus, the number of positive factors of 84 is $3 \times 2 \times 2 = \boxed{12}$. □

Exercise 1.2

Find the number of negative divisors of 84. Hence, deduce the number of divisors of 84.

Exercise 1.3

(2022, S18) Find the number of positive integers smaller than 128^{49} that have exactly 2022 positive divisors.

§2 Congruences

Congruences are used to express the equivalence of integers with respect to a modulus. If a and b are integers and n is a positive integer, we say a is congruent to b modulo n if:

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

if and only if $a - b$ is divisible by n. This is written as:

$$a - b = kn$$

for some integer k.

Lemma 2.1 (Addition Properties in Modular Arithmetic)

- If $a + b = c$, then $a \pmod{N} + b \pmod{N} \equiv c \pmod{N}$.
- If $a \equiv b \pmod{N}$, then $a + k \equiv b + k \pmod{N}$ for any integer k.
- If $a \equiv b \pmod{N}$ and $c \equiv d \pmod{N}$, then $a + c \equiv b + d \pmod{N}$.
- If $a \equiv b \pmod{N}$, then $-a \equiv -b \pmod{N}$.

Example 2.2 (Time Calculation Using Modular Arithmetic)

It is currently 7:00 PM. What time (in AM or PM) will it be in 1000 hours?

Solution. Since time "repeats" every 24 hours, we work modulo 24. We calculate:

$$1000 \bmod 24 = 16 \quad \text{since} \quad 1000 = 16 + (24 \times 41)$$

Thus, 1000 hours later is equivalent to 16 hours from now. Since 7:00 PM + 16 hours = 11:00 AM, the time in 1000 hours will be 11:00 AM. □

Example 2.3

Find the sum of 31 and 148 in modulo 24.

Solution. To find the sum of 31 and 148 modulo 24, we first reduce each number modulo 24.

$$31 \bmod 24 = 7$$

$$148 \bmod 24 = 4$$

So,

$$31 + 148 \equiv 7 + 4 \equiv 11 \pmod{24}$$

Therefore, the sum of 31 and 148 in modulo 24 is $\boxed{11}$. □

Example 2.4 (Sum of Multiple Numbers Modulo 3)
Find the remainder when $123 + 234 + 32 + 56 + 22 + 12 + 78$ is divided by 3.

Solution. We reduce each number modulo 3:

$$123 \equiv 0 \pmod 3, \quad 234 \equiv 0 \pmod 3, \quad 32 \equiv 2 \pmod 3,$$

$$56 \equiv 2 \pmod 3, \quad 22 \equiv 1 \pmod 3, \quad 12 \equiv 0 \pmod 3, \quad 78 \equiv 0 \pmod 3.$$

Thus, the sum modulo 3 is:

$$0 + 0 + 2 + 2 + 1 + 0 + 0 = 5 \equiv 2 \pmod 3.$$

Therefore, the remainder is 2. □

Remark 2.5. The remainder of a number N when divided by 3 can be found by summing its digits and taking the remainder of this sum when divided by 3.

Lemma 2.6 (Multiplication Properties in Modular Arithmetic)

1. If $a \cdot b = c$, then $a \pmod N \cdot b \pmod N \equiv c \pmod N$.
2. If $a \equiv b \pmod N$, then $ka \equiv kb \pmod N$ for any integer k.
3. If $a \equiv b \pmod N$ and $c \equiv d \pmod N$, then $ac \equiv bd \pmod N$.

Example 2.7 (Modular Multiplication Problem)
What is $(8 \times 16) \mod 7$?

Solution. First, reduce both numbers modulo 7:

$$8 \equiv 1 \pmod 7 \quad \text{and} \quad 16 \equiv 2 \pmod 7.$$

Thus,

$$8 \times 16 \equiv 1 \times 2 \equiv 2 \pmod 7.$$

□

Example 2.8 (Product of Multiple Numbers Modulo 3)
Find the remainder when $124 \cdot 134 \cdot 23 \cdot 49 \cdot 235 \cdot 13$ is divided by 3.

Solution. We reduce each number modulo 3:

$$124 \equiv 1 \pmod 3, \quad 134 \equiv 2 \pmod 3, \quad 23 \equiv 2 \pmod 3,$$

$$49 \equiv 1 \pmod 3, \quad 235 \equiv 1 \pmod 3, \quad 13 \equiv 1 \pmod 3.$$

Thus, the product modulo 3 is:

$$1 \cdot 2 \cdot 2 \cdot 1 \cdot 1 \cdot 1 = 4 \equiv 1 \pmod{3}.$$

Therefore, the remainder is 1.

□

Example 2.9

Find the last digit of 7^{2023}.

Solution. The last digit of a number is the remainder when divided by 10, so we need to find:

$$7^{2023} \pmod{10}$$

We begin by calculating the powers of 7 modulo 10:

$$7^1 \equiv 7, \quad 7^2 \equiv 49 \equiv 9, \quad 7^3 \equiv 343 \equiv 3, \quad 7^4 \equiv 2401 \equiv 1$$

Thus, the powers of 7 modulo 10 repeat in a cycle: $7, 9, 3, 1$.

Now, to find $7^{2023} \pmod{10}$, we observe that:

$$2023 \div 4 = 505 \text{ remainder } 3$$

Therefore, $7^{2023} \equiv 7^3 \pmod{10}$. From our calculations, we know:

$$7^3 \equiv 3 \pmod{10}$$

Thus, the last digit of 7^{2023} is $\boxed{3}$.

□

§3 Chinese Remainder Theorem

The Chinese Remainder Theorem (CRT) provides a way to solve systems of simultaneous congruences with pairwise coprime moduli. Suppose we have the following system:

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

where $n_1, n_2, \ldots, n_k$ are pairwise coprime. There exists a unique solution modulo N, where $N = n_1 \cdot n_2 \cdot \ldots \cdot n_k$. The solution can be found using the following steps:

1. Compute $N_i = \frac{N}{n_i}$ for each i.
2. Find M_i such that $N_i M_i \equiv 1 \pmod{n_i}$.
3. The solution is $x \equiv \sum_{i=1}^{k} a_i N_i M_i \pmod{N}$.

Example 3.1 (Three Equations)
Solve the system:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

Solution.
Using the Chinese Remainder Theorem,
We first compute $N = 3 \times 5 \times 7 = 105$.
Next, we compute:

$$N_1 = \frac{105}{3} = 35, \quad N_2 = \frac{105}{5} = 21, \quad N_3 = \frac{105}{7} = 15$$

Now, we find M_1, M_2, and M_3:

$$35M_1 \equiv 1 \pmod{3}$$

By trial, $M_1 = 2$, since $35 \times 2 = 70 \equiv 1 \pmod{3}$.

$$21M_2 \equiv 1 \pmod{5}$$

By trial, $M_2 = 1$, since $21 \times 1 = 21 \equiv 1 \pmod{5}$.

$$15M_3 \equiv 1 \pmod{7}$$

By trial, $M_3 = 1$, since $15 \times 1 = 15 \equiv 1 \pmod{7}$.

Now, we can compute the solution:

$$x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$$

Simplifying:

$$x \equiv 140 + 63 + 30 \pmod{105}$$

$$x \equiv 233 \pmod{105}$$

Finally, reduce $233 \mod 105$:

$$x \equiv 23 \pmod{105}$$

Thus, the solution is $x \equiv 23 \pmod{105}$. □

Exercise 3.2 (Scenario Question)

A teacher is organizing students into groups for a project. When the students are divided into groups of 4, there are 3 students left. When they are divided into groups of 5, there are 4 students left. Finally, when the students are divided into groups of 6, there are 5 students left. What is the smallest number of students in the class?

§4 Euler's Theorem

Euler's Theorem is a generalization of Fermat's Little Theorem. It states that if a and n are coprime integers, then:

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ is Euler's totient function, which counts the number of integers up to n that are coprime to n. For a prime number p, $\phi(p) = p - 1$, and for a power of a prime p^k, $\phi(p^k) = p^k - p^{k-1}$.

Example 4.1

Find the smallest integer n such that $5^n \equiv 1 \pmod{14}$.

Solution.

Step 1: Understanding the Problem

We are tasked with finding the smallest n such that when 5 is raised to the power of n, it leaves a remainder of 1 when divided by 14. In mathematical notation, we want to solve:

$$5^n \equiv 1 \pmod{14}$$

Step 2: Euler's Totient Function

Since $\gcd(5, 14) = 1$, Euler's theorem tells us that n must divide $\varphi(14)$. First, we calculate $\varphi(14)$, where $\varphi(n)$ is Euler's Totient function.

Factorize 14:

$$14 = 2 \times 7$$

Using the formula for Euler's Totient function:

$$\varphi(14) = \varphi(2) \times \varphi(7) = (2-1) \times (7-1) = 1 \times 6 = 6$$

This means n must be a divisor of 6. The divisors of 6 are $1, 2, 3, 6$.

Step 3: Testing Powers of 5 Modulo 14

Now, we will test each divisor to find the smallest n such that $5^n \equiv 1 \pmod{14}$.

- For $n = 1$:
$$5^1 \equiv 5 \pmod{14} \quad \text{(not 1)}$$
- For $n = 2$:
$$5^2 = 25 \quad \Rightarrow \quad 25 \div 14 = 1 \text{ remainder } 11, \quad 5^2 \equiv 11 \pmod{14} \quad \text{(not 1)}$$
- For $n = 3$:
$$5^3 = 5 \times 5^2 = 5 \times 25 = 125 \quad \Rightarrow \quad 125 \div 14 = 8 \text{ remainder } 13, \quad 5^3 \equiv 13 \pmod{14} \quad \text{(not 1)}$$
- For $n = 6$:
$$5^6 = (5^3)^2 = 13^2 = 169 \quad \Rightarrow \quad 169 \div 14 = 12 \text{ remainder } 1, \quad 5^6 \equiv 1 \pmod{14}$$

Thus, the smallest n such that $5^n \equiv 1 \pmod{14}$ is $n = 6$.

□

§5 Extended Euclidean Algorithm

The Extended Euclidean Algorithm is a powerful tool for finding the greatest common divisor (GCD) of two integers, and it also provides a way to express this GCD as a linear combination of the integers. This is particularly useful in solving Diophantine equations.

§5.1 Euclidean Algorithm

The Euclidean Algorithm is based on the following principle:

$$\gcd(a, b) = \gcd(b, a \mod b)$$

where a and b are integers and $a \mod b$ denotes the remainder when a is divided by b. This principle exploits the fact that the GCD of two numbers does not change if the larger number is replaced by its remainder when divided by the smaller number.

The algorithm proceeds with the following steps:

1. Given two integers a and b (where $a \geq b$), compute the remainder r when a is divided by b:
$$r = a \mod b$$
2. Replace a with b and b with r.
3. Repeat the process until b becomes zero. The non-zero remainder a at this point will be the GCD of the original a and b.

Example 5.1

What is the greatest common divisor of 252 and 198?

Solution. The Euclidean Algorithm may be utilised as follows: With that,

$$\begin{aligned} 252 &= 198 \cdot 1 + 54 \\ 198 &= 54 \cdot 3 + 36 \\ 54 &= 36 \cdot 1 + 18 \\ 36 &= 18 \cdot 2 + 0 \end{aligned}$$

Here, $\gcd(252, 198) = 18$. To express 18 as a linear combination of 252 and 198:

1. Start with the equation:
$$18 = 54 - 36 \cdot 1$$
2. Substitute $36 = 198 - 54 \cdot 3$ into the equation:
$$18 = 54 - (198 - 54 \cdot 3) \cdot 1$$
Simplifying this, we get:
$$18 = 54 \cdot 4 - 198$$
3. Finally, substitute $54 = 252 - 198$ into the equation:
$$18 = (252 - 198) \cdot 4 - 198$$
Simplifying further, we get:
$$18 = 252 \cdot 4 - 198 \cdot 5$$

Therefore, the GCD of 252 and 198 can be expressed as:

$$18 = 252 \cdot 4 - 198 \cdot 5$$

Since the remainder is now 0, the algorithm terminates. The GCD of 252 and 198 is the last non-zero remainder, which is $\boxed{18}$.

□

§6 Diophantine Equations

Diophantine equations are polynomial equations for which we seek integer solutions. A classic example is the linear Diophantine equation:

$$ax + by = c$$

where a, b, and c are given integers. A solution exists if and only if the greatest common divisor (gcd) of a and b divides c.

§6.1 Finding Solutions

To find solutions:

- Compute the gcd of a and b, say d.
- Verify that d divides c.
- Use the Extended Euclidean Algorithm to find a particular solution.

Example 6.1

For $a = 15$, $b = 25$, and $c = 35$:

$$\gcd(15, 25) = 5$$

Since 5 divides 35, there are integer solutions. One particular solution is $x = 2$, $y = -1$, which satisfies:

$$15 \cdot 2 + 25 \cdot (-1) = 35$$

If you would like to check for more information about divisibility test (which is not being covered in this workshop) before trying out the practice below, you may check out this website or search online for more notes.

§7 Extra Problems

1. Prove that for any integer n, $n^2 \equiv 0$ or $1 \pmod 4$.
2. Solve the congruence $7x \equiv 5 \pmod{24}$.
3. Determine if there is an integer x such that $x^2 \equiv -1 \pmod p$ for $p = 17$.

Hints and Solutions

1. Any square number is either 0 or 1 modulo 4 because if $n = 2k$ or $n = 2k + 1$ (even or odd), then $n^2 = 4k^2$ or $n^2 = 4k^2 + 4k + 1$.
2. Apply the Extended Euclidean Algorithm to find the multiplicative inverse of 7 modulo 24, then multiply both sides of the congruence by this inverse.
3. Check by calculating x^2 for all x such that $x \equiv k \pmod{17}$ where k runs from 0 to 16, or use the Legendre symbol.

§8 Past Year Questions

The following questions are sorted chronologically (not by difficulty).

1. (2020, J19) A perfect square ends with the same two digits. How many possible values of this digit are there?
2. (2020, S15) Find the sum of all integers n that fulfill the equation
$$2^n(6-n) = 8n$$
3. (2020, S17) Given a positive integer n. The number $2n$ has 28 positive factors, while the number $3n$ has 30 positive factors. Find the number of positive divisors of $6n$.
4. (2021, J4) A positive integer n is called special if n is divisible by 4, $n+1$ is divisible by 5, and $n+2$ is divisible by 6. How many special integers smaller than 1000 are there?
5. (2021, J15) How many integers n (with $1 \leq n \leq 2021$) have the property that $8n+1$ is a perfect square?
6. (2021, S15) Find the sum of all integers n with this property: both n and $n+2021$ are perfect squares.
7. (2021, S17) Determine the sum of all positive integers n that satisfy the following condition: when $6n+1$ is written in base 10, all its digits are equal.
8. (2022, J9) For any positive integer n, the factorial $n!$ is the product of all the positive integers smaller than or equal to n. For example, $5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$. Find the last two digits of $(1!)^2 + (2!)^2 + (3!)^2 + \cdots + (2022!)^2$.
9. (2022, J13) For a positive integer n we denote by $d(n)$ the number of distinct positive divisors of n and by $s(n)$ the sum of these divisors. For example, $d(2022)$ is equal to 8 since 2022 has eight distinct divisors $1, 2, 3, 6, 337, 674, 1011$ and 2022. As a result, $s(2022) = 1+2+3+6+337+674+1011+2022 = 4056$. Determine the largest positive integer n such that $s(n)d(n) = 96$.
10. (2022, S14) Let p and q be prime numbers. What is the largest possible value of the greatest common divisor of $(p+q)^4$ and $p-q$?
11. (2023, JC2) Determine the smallest positive integer n such that $\sqrt{2n}$ and $\sqrt[3]{3n}$ are both integers.
12. (2023, SB4) Given integers M and N such that:
$$4^4 \cdot 21^{21} \cdot M^M \cdot N^N = 3^3 \cdot 7^7 \cdot 14^{14} \cdot 18^{18}$$
Find $M+N$.
13. (2023, SB9) Find the smallest positive integer n such that the following statement is true: For every prime p, the number p^2+n is not prime.
14. (2023, SC2) Find the number of positive integers N such that $N < 1000$ and N has exactly 12 even factors and 6 odd factors. (Factors of N include 1 and N).
15. (2023, SC5) Find the smallest positive integer k such that $11!k$ is a perfect square.