IMONST1 Workshop 2024 Answers
(Day 2: Number Theory)

Phua Yufan

September 2024

1 Prime Numbers

Exercise 1.2 12, 24
Exercise 1.3 5

2 Chinese Remainder Theorem

Exercise 3.2 59

3 Extra Problems

Problem 1: Prove that for any integer n, $n^2 \equiv 0$ or $1 \pmod 4$
We will prove that for any integer n, $n^2 \equiv 0$ or $1 \pmod 4$ by considering two cases: when n is even and when n is odd.

Case 1: $n = 2k$ **(Even)**
If n is even, we can write $n = 2k$ for some integer k. Now we compute n^2 mod 4:

$$n^2 = (2k)^2 = 4k^2.$$

Since $4k^2$ is clearly divisible by 4, we have:

$$n^2 \equiv 0 \pmod 4.$$

Therefore, if n is even, $n^2 \equiv 0 \pmod 4$.

Case 2: $n = 2k + 1$ **(Odd)**
If n is odd, we can write $n = 2k + 1$ for some integer k. Now we compute n^2 mod 4:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1.$$

Since $4(k^2 + k)$ is divisible by 4, we have:

$$n^2 \equiv 1 \pmod 4.$$

Therefore, if n is odd, $n^2 \equiv 1 \pmod 4$.

Conclusion:
For any integer n, we have:

$$n^2 \equiv 0 \pmod 4 \quad \text{if } n \text{ is even,}$$

and

$$n^2 \equiv 1 \pmod 4 \quad \text{if } n \text{ is odd.}$$

Thus, $n^2 \equiv 0$ or $1 \pmod 4$.

Problem 2: Solve the Congruence $7x \equiv 5 \pmod{24}$
We want to solve the congruence $7x \equiv 5 \pmod{24}$ for x.

Step 1: Find the inverse of 7 modulo 24 by trial and error
To solve this congruence, we need to find the inverse of 7 modulo 24. We do this by trial and error, checking for $7 \times k \equiv 1 \pmod{24}$. We compute the following products:

$$\begin{aligned}
7 \times 1 &\equiv 7 \pmod{24}, \\
7 \times 2 &\equiv 14 \pmod{24}, \\
7 \times 3 &\equiv 21 \pmod{24}, \\
7 \times 4 &\equiv 4 \pmod{24}, \\
7 \times 5 &\equiv 11 \pmod{24}, \\
7 \times 6 &\equiv 18 \pmod{24}, \\
7 \times 7 &\equiv 1 \pmod{24}.
\end{aligned}$$

We observe that $7 \times 7 \equiv 1 \pmod{24}$. Hence, the inverse of 7 modulo 24 is 7.

Now, work backward to express 1 as a linear combination of 7 and 24:

$$1 = 7 - 2 \times 3.$$

Substitute $3 = 24 - 3 \times 7$ from the first equation:

$$1 = 7 - 2 \times (24 - 3 \times 7) = 7 - 2 \times 24 + 6 \times 7,$$

$$1 = 7 + 6 \times 7 - 2 \times 24 = 7(7) - 2 \times 24.$$

Thus, $1 = 7 \times 7 - 2 \times 24$, which means that the inverse of 7 modulo 24 is 7.

Step 2: Multiply both sides by the inverse
Since the inverse of 7 modulo 24 is 7, we multiply both sides of the congruence $7x \equiv 5 \pmod{24}$ by 7:

$$7 \times 7x \equiv 7 \times 5 \pmod{24},$$

$$49x \equiv 35 \pmod{24}.$$

Since $49 \equiv 1 \pmod{24}$, this simplifies to:

$$x \equiv 35 \pmod{24}.$$

Now, reduce $35 \mod 24$:

$$35 \equiv 11 \pmod{24}.$$

Conclusion:
The solution to the congruence $7x \equiv 5 \pmod{24}$ is:

$$x \equiv 11 \pmod{24},$$

or $x = 11 + 24k$ for any integer k.

Problem 3: Determine if there is an integer x such that $x^2 \equiv -1 \pmod{17}$
We are tasked with determining whether there is an integer x such that $x^2 \equiv -1 \pmod{17}$. To solve this, we compute $x^2 \mod 17$ for all values of $x = 0, 1, 2, \ldots, 16$, and check whether any of them give $x^2 \equiv -1 \pmod{17}$ (which is equivalent to $x^2 \equiv 16 \pmod{17}$).

We compute $x^2 \mod 17$ for $x = 0, 1, 2, \ldots, 16$:

$$\begin{gathered}
0^2 \equiv 0 \pmod{17}, \\
1^2 \equiv 1 \pmod{17}, \\
2^2 \equiv 4 \pmod{17}, \\
3^2 \equiv 9 \pmod{17}, \\
4^2 \equiv 16 \pmod{17}, \\
5^2 \equiv 8 \pmod{17}, \\
6^2 \equiv 2 \pmod{17}, \\
7^2 \equiv 15 \pmod{17}, \\
8^2 \equiv 13 \pmod{17}, \\
9^2 \equiv 13 \pmod{17}, \\
10^2 \equiv 15 \pmod{17}, \\
11^2 \equiv 2 \pmod{17}, \\
12^2 \equiv 8 \pmod{17}, \\
13^2 \equiv 16 \pmod{17}, \\
14^2 \equiv 9 \pmod{17}, \\
15^2 \equiv 4 \pmod{17}, \\
16^2 \equiv 1 \pmod{17}.
\end{gathered}$$

From this, we see that:

$$4^2 \equiv 16 \pmod{17}, \quad \text{and} \quad 13^2 \equiv 16 \pmod{17}.$$

Conclusion:
There are two solutions to the equation $x^2 \equiv -1 \pmod{17}$:

$$x \equiv 4 \pmod{17} \quad \text{or} \quad x \equiv 13 \pmod{17}.$$

4 Past Year Questions

1. (2020, J19) 2
2. (2020, S15) 9
3. (2020, S17) 35
4. (2021, J4) 17
5. (2021, J15) 63
6. (2021, S15) 1020104
7. (2021, S17) 6
8. (2022, J9) 17
9. (2022, J13) 47
10. (2022, S14) 16
11. (2023, JC2) 72
12. (2023, SB4) 17
13. (2023, SB9) 5
14. (2023, SC2) 12
15. (2023, SC5) 77