0 How to Read This Handout

Throughout this handout there will be numerous example problems to illustrate the concepts being taught. For maximum benefit, try to think about the example problems for a while before reading the solutions.

0.1 Homework

We will be discussing these problems at our meetings. If you have any questions or want more hints, feel free to email us at `n.soedjak@gmail.com` or `soedjak.ryan@gmail.com`.

0.2 Hints

Some of the homework problems come with hints, which are at the back of this handout. Hints are in random order, so you don't accidentally look at the hint to the next problem.

Be sure to seriously attempt the problem before resorting to the hints!

Contents

1 Introduction **2**
1.1 Definitions 2
1.2 Example Problems 2

2 Useful Properties of Congruences **4**
2.1 Overview 4
2.2 Example Problems 4

3 Homework **7**
3.1 Problems 7
3.2 Hints 8

4 Sources **9**

1 Introduction

1.1 Definitions

Modular arithmetic is a system of arithmetic in which two integers are considered the same if they have the same remainder when divided by a certain integer.

Specifically, let a, b, and m be integers. We say that $a \equiv b \pmod{m}$ (pronounced "a is congruent to b modulo m") if a and b have the same remainder when divided by m. Otherwise, $a \not\equiv b \pmod{m}$. The statement $a \equiv b \pmod{m}$ is called a **congruence** and the number m is called the **modulus** of the congruence. You can think of the congruence symbol $\equiv$ as a kind of equal sign in modular arithmetic.

An equivalent way to think of it is that $a \equiv b \pmod{m}$ if $a - b$ is a multiple of m. (Do you see why this is the same as saying that a and b have the same remainder when divided by m?)

Examples:

- $2 \equiv 14 \pmod{6}$ because $2 - 14 = -12$ is a multiple of 6.
- $100 \equiv 23 \pmod{11}$ because $100 - 23 = 77$ is a multiple of 11.
- $4 \equiv -1 \pmod{5}$ because $4 - (-1) = 5$ is a multiple of 5. (Notice that negative numbers are allowed in congruences!)
- $8 \not\equiv -8 \pmod{3}$ because $8 - (-8) = 16$ is *not* a multiple of 3.

Warning! Only integers are allowed in congruences.

Now let us introduce some more terminology. Instead of the word "remainder", we will often use the word "residue". For example, since the remainder when 23 is divided by 5 is 3, we say that the modulo 5 residue of 23 is 3. Here is the formal definition:

Definition: We say that r is the modulo m **residue** of n when $n \equiv r \pmod{m}$ and $0 \leq r < m$.

1.2 Example Problems

Problem 1. Which of the following are congruent to 6 (mod 8)?

(a) -18	(c) 54	(e) 754
(b) 27	(d) 254	(f) 1036

Solution: We want to find the ones that leave a remainder of 6 when divided by 8, or equivalently, when subtracted by 6 is a multiple of 8. We can simply check each one:

(a) $\frac{-18-6}{8} = \frac{-24}{8} = -3$ is an integer, so $-18 \equiv 6 \pmod 8$.

(b) $\frac{27-6}{8} = \frac{21}{8}$ is not an integer, so $27 \not\equiv 6 \pmod 8$.

(c) $\frac{54-6}{8} = \frac{48}{8} = 6$ is an integer, so $54 \equiv 6 \pmod 8$.

(d) $\frac{254-6}{8} = \frac{248}{8} = 31$ is an integer, so $254 \equiv 6 \pmod 8$.

(e) $\frac{754-6}{8} = \frac{748}{8} = \frac{187}{2}$ is not an integer, so $754 \not\equiv 6 \pmod 8$.

(f) $\frac{1036-6}{8} = \frac{1030}{8} = \frac{515}{4}$ is not an integer, so $1036 \not\equiv 6 \pmod 8$. □

Problem 2. How many numbers from 1 to 30 inclusive are congruent to $2 \pmod 6$?

Solution: The problem is equivalent to "How many numbers from 1 to 30 inclusive have a remainder of 2 when divided by 6?". Since 30 is a small number, we can simply list out all the numbers that work: $2, 8, 14, 20, 26$. (Note that each number is 6 more than the previous number.) Thus the answer is $\boxed{5}$. □

Problem 3. How many numbers from -150 to 150 inclusive are congruent to $5 \pmod{13}$?

Solution: We could list them all out like we did in the previous problem. However, we can use a bit of algebra to speed things up.

A number congruent to $5 \pmod{13}$ can be written as $13n + 5$, where n is an integer. Therefore, we want to find the number of integers $13n + 5$ such that

$$-150 \leq 13n + 5 \leq 150,$$

or equivalently, the number of integers n that satisfies the above. Subtracting 5 from both sides and dividing everything by 13 gives

$$-\frac{155}{13} \leq n \leq \frac{145}{13}.$$

The smallest integer greater than $-\frac{155}{13}$ is -11, and the largest integer less than $\frac{145}{13}$ is 11, so

$$-11 \leq n \leq 11.$$

There are $\boxed{23}$ integers between -11 and 11 inclusive. □

As we just saw, writing a number that is congruent to $k \pmod m$ in the form $mn + k$ where n is an integer is a very useful tactic.

2 Useful Properties of Congruences

2.1 Overview

So why are congruences useful? Well, they have the following useful properties.

Consider four integers a, b, c, d and a positive integer m such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then, we can combine the two congruences in the following ways:

- Addition: $a + c \equiv b + d \pmod{m}$.
- Subtraction: $a - c \equiv b - d \pmod{m}$.
- Multiplication: $ac \equiv bd \pmod{m}$.
- Exponentiation: $a^e \equiv b^e \pmod{m}$ where e is a positive integer. (Note that since exponentiation is just repeated multiplication, this is a consequence of repeatedly applying the Multiplication Property above.)

These properties are probably fairly intuitive and unsurprising. For this reason we will omit their proofs. However, definitely try to prove them if you're interested!

Warning! Division is not defined in modular arithmetic. Thus, there is no Division Property.

Warning! It turns out it is *not* true that $a^c \equiv b^d \pmod{m}$. A counterexample: $2 \equiv 5 \pmod{3}$ and $4 \equiv 1 \pmod{3}$ but $2^4 \not\equiv 5^1 \pmod{3}$.

2.2 Example Problems

Problem 4. What is the remainder when the arithmetic series

$$4 + 13 + 22 + 31 + \cdots + 184$$

is divided by 9?

Solution: First we find the number of terms in the arithmetic series. If we add 5 to each term in the sequence

$$4, 13, 22, 31, \ldots, 184,$$

we get

$$9, 18, 27, 36, \ldots, 189.$$

Dividing each term by 9 results in

$$1, 2, 3, 4, \ldots, 21.$$

Since each time we modified the sequence the number of terms in the sequence didn't change, it follows that there are 21 terms in the original arithmetic series. We now present two continuations.

Continuation 1. Notice that each of the terms in the arithmetic series is congruent to 4 (mod 9). Therefore by the Addition Property,

$$\begin{aligned} 4+13+22+31+\cdots+184 &\equiv \underbrace{4+4+4+4+\cdots+4}_{21\ 4\text{'s}} \\ &= 21(4) \\ &= 84 \\ &\equiv 3 \pmod 9. \end{aligned}$$

Hence, the answer is $\boxed{3}$.

Continuation 2. By the formula for arithmetic series,

$$\begin{aligned} 4+13+22+31+\cdots+184 &= 21\left(\frac{4+184}{2}\right) \\ &= 21\cdot 94 \end{aligned}$$

Now we could multiply out $21\cdot 94$ and find its remainder when divided by 9. However, the Product Property provides a quicker way. Since $21 \equiv 3 \pmod 9$ and $94 \equiv 4 \pmod 9$, the Product Property tells us that

$$21\cdot 94 \equiv 3\cdot 4 = 12 \equiv 3 \pmod 9.$$

Again, we find the answer is $\boxed{3}$. □

Problem 5. What is the remainder when the product

$$4901\cdot 4902\cdot 4903\cdot 4904\cdot 4905$$

is divided by 7?

Solution: In theory, we could simply multiply the product out and find its modulo 7 residue. A more efficient approach, however, is to observe that by the Multiplication Property, the product is congruent in modulo 7 to the product of the modulo 7 residues of the factors. Since 4900 is a multiple of 7, we have

$$\begin{aligned} 4901 &\equiv 1 \pmod 7, \\ 4902 &\equiv 2 \pmod 7, \\ 4903 &\equiv 3 \pmod 7, \\ 4904 &\equiv 4 \pmod 7, \\ 4905 &\equiv 5 \pmod 7, \end{aligned}$$

Therefore,

$$\begin{aligned} 4901 \cdot 4902 \cdot 4903 \cdot 4904 \cdot 4905 &\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \\ &= 120 \\ &\equiv \boxed{1} \pmod 7. \end{aligned}$$

□

Problem 6. What is the remainder when 7^{2015} is divided by 6?

Solution: We want to find the residue of $7^{2015} \pmod 6$. The exponentiation suggests somehow using the Exponentiation Property. We can use it in the following way: $7 \equiv 1 \pmod 6$, so the Exponentiation Property tell us that $7^{2015} \equiv 1^{2015} \pmod 6$. But $1^{2015} = 1$, so we have just $7^{2015} \equiv 1 \pmod 6$. Therefore, the remainder when 7^{2015} is divided by 6 is $\boxed{1}$. □

Problem 7. What is the units digit of 7^{2015}?

Solution: What does this problem have to do with modular arithmetic? If you think about it, the units digit of a number is the remainder when that number is divided by 10, or equivalently, the modulo 10 residue of the number. So we want to find the residue of $7^{2015} \pmod{10}$. Unfortunately, the trick we used in the previous problem doesn't work here because the residue of 7 (mod 10) is just 7.

We can begin by finding the modulo 10 residues of the first few powers of 7:

$$\begin{aligned} 7^1 &= 7(7^0) \equiv 7(1) \equiv 7 \pmod{10} \\ 7^2 &= 7(7^1) \equiv 7(7) \equiv 9 \pmod{10} \\ 7^3 &= 7(7^2) \equiv 7(9) \equiv 3 \pmod{10} \\ 7^4 &= 7(7^3) \equiv 7(3) \equiv 1 \pmod{10} \\ 7^5 &= 7(7^4) \equiv 7(1) \equiv 7 \pmod{10} \\ 7^6 &= 7(7^5) \equiv 7(7) \equiv 9 \pmod{10} \\ 7^7 &= 7(7^6) \equiv 7(9) \equiv 3 \pmod{10} \\ 7^8 &= 7(7^7) \equiv 7(3) \equiv 1 \pmod{10} \end{aligned}$$

We see that the modulo 10 residues of the first few powers of 7 are $7, 9, 3, 1, 7, 9, 3, 1 \ldots$. There seems to be a pattern: it goes $7, 9, 3, 1$ and repeats. This pattern holds forever because 7 times any specific modulo 7 residue never changes, so when a residue repeats, all subsequent residues repeat as well. This forms the pattern.

Therefore, the residue of $7^{2015} \pmod{10}$ is the same as the 2015^{th} term of the sequence $7, 9, 3, 1, \ldots$. Since the sequence repeats every 4 terms and $2015 \equiv 3 \pmod 4$, the residue of $7^{2015} \pmod{10}$ is equivalent to the 3^{rd} term of $7, 9, 3, 1, \ldots$, which is $\boxed{3}$. □

3 Homework

3.1 Problems

Problem 8. When three positive integers are divided by 47, the remainders are 25, 20, and 3, respectively. When the sum of the three integers is divided by 47, what is the remainder?

Problem 9. Eleven girls are standing around a circle. A ball is thrown clockwise around the circle. The first girl, Ami, starts with the ball, skips the next three girls and throws to the fifth girl, who then skips the next three girls and throws the ball to the ninth girl. If the throwing pattern continues, including Ami's initial throw, how many total throws are necessary for the ball to return to Ami?

Problem 10. If a and b are integers such that $ab \equiv 17 \pmod{20}$, then what is the remainder when $(a+10)(b+10)$ is divided by 20?

Problem 11. What is the remainder when 5^{1337} is divided by 6? *Hints:* 1

Problem 12. What is the units digit of 9^{142}?

Problem 13. Marsha has two numbers, a and b. When she divides a by 70 she gets a remainder of 64. When she divides b by 105 she gets a remainder of 99. What remainder does she get when she divides $a+b$ by 35?

Problem 14. What is the remainder when $3^0 + 3^1 + 3^2 + \ldots + 3^{2009}$ is divided by 8?

Problem 15. Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999\ 9\text{'s}}$ is divided by 1000.

Problem 16. Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

Problem 17. What is the tens digit in the sum $7! + 8! + 9! + \cdots + 2006!$? *Hints:* 2

3.2 Hints

1. What is a number that is congruent to 5 (mod 6) that is easy to work with?

2. Find the modulo 100 residue of the sum.

4 Sources

Problem 1: AoPS Introduction to Number Theory
Problem 8: AoPS Introduction to Number Theory
Problem 9: MATHCOUNTS
Problem 10: AoPS Introduction to Number Theory
Problem 13: AoPS Introduction to Number Theory
Problem 14: AMC 10
Problem 15: AIME
Problem 16: AMC 10
Problem 17: AMC 10