

# Modular Arithmetic

Placeholder

June 30, 2020

Note: This handout is for people with little to no experience with modular arithmetic. If you are already familiar with modular arithmetic, feel free to do the problems at the bottom and the ones dispersed throughout.

## 1 Introduction

In essence, modular arithmetic is the addition, subtraction, multiplication and sometimes division of the remainders of numbers.

**Definition 1.1** Two numbers are said to be congruent modulo  $n$  if their difference is evenly divisible by  $n$ . So  $a$  is congruent to  $b$  modulo  $n$  if  $n|(a - b)$ . This congruence is written as

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

Modular congruences are very similar to regular equations. For instance, you can add two congruences as if they were equations.

If we have  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$  then  $a + c \equiv b + d \pmod{n}$ . This can be easily proven from the definition of modular congruences.

$$\begin{aligned} a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n} \\ \implies n|(a - b) \text{ and } n|(c - d) \\ \implies n|(a - b) + (c - d) \\ \implies n|(a + c) - (b + d) \\ \implies \boxed{a + c \equiv b + d \pmod{n}} \end{aligned}$$

Subtraction and multiplication follow similarly.

**Example 1.2** Solve the congruence  $4x \equiv 3 \pmod{7}$

*Solution* We multiply by 2 to get  $8x \equiv 6 \pmod{7} \implies \boxed{x \equiv 6 \pmod{7}}$

Division in modular arithmetic is a little different. As an example, consider the congruence

$$15 \equiv 75 \pmod{12}.$$

Dividing both sides by 3 yields

$$5 \equiv 25 \pmod{12}.$$

So clearly there is a problem here. Let's examine the definition of modular congruence again. With our current example, we have

$$12 \nmid 75 - 15.$$

When we divide  $75 - 15$  by 3, we "remove" a factor of 3, so 12 doesn't divide the quotient. Notice that if we divided both sides of the original congruence by 5, we get

$$3 \equiv 15 \pmod{12}$$

which is true. As long as you divide by a number that is relatively prime to the modulus, you won't "remove" any important factors so the congruence holds true.

So when you divide in modular arithmetic, you need to make sure you divide by a number that doesn't share any factors with the modulus.

If you need to divide by a number that is not relatively prime, you simply divide the modulus by the gcd of itself and the divisor.

From our original example again, if we divide both sides by 3, while also dividing 12 by 3, we get

$$5 \equiv 25 \pmod{4}$$

which is clearly true.

## Exercises

1. Prove that subtraction and multiplication work in modular arithmetic.
2. Prove the divisibility rules for the numbers 2 through 11.  
(The rule for 7 is you take the last digit, double it then subtract it from the remaining digits. If the difference is divisible by 7, then the original number was divisible by 7)
3. Compute  $2021 \cdot 2019 \cdot 2018 \cdot 2017 \pmod{10}$ .
- 4.(AMC 8) How many positive three-digit integers have a remainder of 2 when divided by 6, a remainder of 5 when divided by 9, and a remainder of 7 when divided by 11?

## 2 Chinese Remainder Theorem

**Theorem 2.1** The Chinese Remainder Theorem states that if  $a_1, a_2, a_3, \dots, a_{n-1}, a_n$  are all relatively prime, then the system

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ x &\equiv b_3 \pmod{a_3} \\ &\vdots \\ x &\equiv b_{n-1} \pmod{a_{n-1}} \\ x &\equiv b_n \pmod{a_n} \end{aligned}$$

has a unique solution modulo  $a_1 a_2 a_3 \dots a_n$

We present this theorem without proof as it goes beyond the scope of this hand-out. This theorem guarantees solutions to many problems involving modular arithmetic.

**Example 2.2** If a teacher arranges her students in rows of 5, there are 3 students left in the last row. If she arranges them in rows of 7, there is 1 student left in the last row. If she arranges them in rows of 9, there are 6 students left in the last row. What is the least number of students she could have.

*Solution.* We can rephrase this problem in terms of modular arithmetic. Let  $n$  be the number of students. Thus, the problem boils down to solving the system

$$\begin{aligned} n &\equiv 3 \pmod{5} \\ n &\equiv 1 \pmod{7} \\ n &\equiv 6 \pmod{9} \end{aligned}$$

The Chinese Remainder Theorem guarantees that there is a unique solution modulo  $5 \cdot 7 \cdot 9$ .

We can rewrite the first congruence as  $n = 3 + 5a$  where  $a$  is an integer. Substituting into the second congruence we get

$$\begin{aligned} 3 + 5a &\equiv 1 \pmod{7} \\ \implies 5a &\equiv 5 \pmod{7} \\ \implies a &\equiv 1 \pmod{7} \\ \implies a &= 1 + 7b. \end{aligned}$$

Substituting this into our first equation we get  $n = 35b + 8$ .

Now we substitute this into the third congruence.

$$\begin{aligned} 35b + 8 &\equiv 6 \pmod{9} \\ \implies -b &\equiv 7 \pmod{9} \\ \implies b &\equiv 2 \pmod{9} \\ \implies b &= 2 + 9c. \end{aligned}$$

Substituting, we get  $n = 215c + 78$ . Since we want  $n$  to be as small as possible, we set  $c = 0$  and get  $n = 78$

## 3 Orders

### Exercises