Modular Arithmetic

Jonathan Pei

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

Basic Operations

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

$$12|75 - 15.$$

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.

We will present a more rigorous proof on when division works in the next section.

Modular Inverses

When you divide by a number a, you are actually multiplying by another number b such that $ab = 1$. For example, in normal arithmetic dividing by 2 is actually multiplying by $\frac{1}{2}$. In this case $\frac{1}{2}$ would be the multiplicative inverse of 2.

Modular Inverses are very similar. The inverse of a number a modulo n, is the number b modulo n such that $ab \equiv 1 \pmod{n}$

Definition 1.3 A modular inverse of an integer a is the integer b such that $ab \equiv 1 \pmod{n}$

Example 1.4. Find the inverse of 5 (mod 11).

Solution. We can guess and check and find that $5 \cdot 9 \equiv 45 \equiv 1 \pmod{11}$. So $\boxed{9}$ is our inverse.

We will present 2 ways to find the modular inverse. The first way is to use brute force and check all numbers modulo n. We used this method in the above exercise. For very small numbers, this is often the fastest way to calculate inverses.

The second way is to use the Euclidean Algorithm.

Proposition 1.5 If $\gcd(a, b) \neq 1$, then a does not have a modular inverse mod b and vice versa.

Proof. Suppose that a did have an inverse. So $ax \equiv 1 \pmod{b}$ would have a solution. Equivalently, $ax + by = 1$ would have integer solutions. However, let $\gcd(a, b) = g$ and $\frac{a}{g} = a'$ and $\frac{b}{g} = b'$. So we can factor g out of the left side to get $g(a'x + b'y) = 1$. This is a contradiction because the left hand side has a factor of g, while the right side does not.

Proposition 1.6 $\gcd(a, b) = \gcd(a, a - b)$.

Proof. Consider any common divisor d of a and b. Clearly this common divisor also divides $a - b$. Now consider a common divisor d' of a and (a-b). We have $d'|a$ and $d'|(a - b)$ so $d'|b$. We have shown that every common divisor of a and b is a common divisor of a and (a-b). And every common divisor of a and (a-b) is a common divisor of a and b. So the common divisors of a and b and the common divisors of a and (a-b) are the same. Thus, the greatest common divisor is also the same.

Theorem 1.7 The Division Algorithm. For any pair of integers a and b, we can uniquely write a as $bq + r$ where $r < b$.

The r represents the remainder after a has been divided by b. It is pretty clear that this theorem is true. As an exercise prove that you can always find q and r, and that when $r < b$, r is unique.

Theorem 1.8 The Euclidean Algorithm.

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_n - 1 &= r_nq_{n+1} \\ \gcd(a,b) &= r_n \end{aligned}$$

Proof. By proposition 1.6, $\gcd(r_m, r_m + 1) = \gcd(a, b)$. So by repeatedly using the division algorithm, we get that $\gcd(a, b) = \gcd(r_n, 0) = r_n$.

Now in order to find a modular inverse, we use the Euclidean Algorithm. The trick is to write 1 as the sum of multiples of r_{m-1} and r_m.

Example. Find the inverse of 12 modulo 17.
Solution. First we use the Euclidean Algorithm. We get

$$\begin{aligned} 17 &= 12 \cdot 1 + 5 \\ 12 &= 5 \cdot 2 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

Now we write $1 = 5 - 2 \cdot 2$. We substitute the second equation and get $1 = 5 - 2 \cdot (12 - 5 \cdot 2) \implies 1 = 5 \cdot 5 - 2 \cdot 12$.
Substituting again gives us $1 = -2 \cdot 12 + 5 \cdot (17 - 12) \implies 1 = -7 \cdot 12 + 5 \cdot 17$. $-7 \cdot 12 + 5 \cdot 17 \equiv -7 \cdot 12 \equiv 10 \cdot 12 \pmod{17}$. So $\boxed{10}$ is the inverse of 12 modulo 17.

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 $2021 \cdot 2019 \cdot 2018 \cdot 2017 \mod 10$.

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?

5. Solve the congruence $37x = 12 \pmod{73}$

2 Chinese Remainder Theorem

Theorem 2.1 The Chinese Remainder Theorem states that if a_1, a_2, a_3, $\ldots$ 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 $a_1 a_2 a_3 \ldots a_n$

We present this theorem without proof as it goes beyond the scope of this handout. 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

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

Substituting this into our first equation we get $n = 35b + 8$.
Now we substitute this into the third congruence.

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

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