

# Modular Arithmetic

Andy Chong Sam

October 18, 2022

## 1 Remainder Quotient Formula

When performing an integer division we can document a quotient ( $q$ ) and a remainder ( $r$ ). In this document we will use the following notation to denote each:

$$\begin{aligned} a/b &= q \\ a \bmod b &= r \end{aligned}$$

Given a dividend  $a$ , and a divisor  $b$  that results in a quotient  $q$  and a remainder  $r$ , we can derive the following expression:

$$a = bq + r \tag{1}$$

Consider a simple integer division of 25 divided by 11. Since  $25/11 = 2$  and  $25 \bmod 11 = 3$ , all pieces of the operation can be encapsulated as:  $25 = (11)(2) + 3$ . Expression (1) can be used to demonstrate various properties in modular arithmetic.

## 2 Modular Arithmetic

### 2.1 Overview

A straightforward interpretation of the modulo operation ( $\bmod$ ) is that its output is the remainder of the division between two integers. A cyclical pattern is observed by varying  $x$  in  $x \bmod s$ , when  $s$  is left constant.

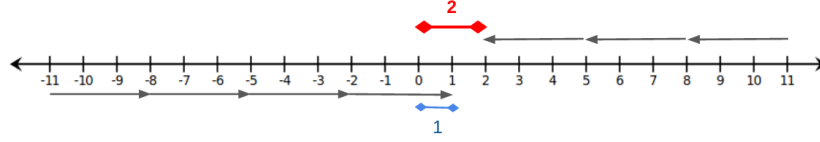
For  $x \bmod 1$ , the set of all possible outcomes is  $\{0\}$ .

For  $x \bmod 2$ , the set of all possible outcomes is  $\{0,1\}$ .

For  $x \bmod 5$ , the set of all possible outcomes is  $\{0,1,2,3,4\}$ .

### 2.2 Negative Dividends

When the dividend is negative, the results are less intuitive. For example:  $-11 \bmod 3 = 1$ . One way to visualize this outcome is by imagining a number line with an emphasis on the range of  $\bmod 3$ :  $\{0, 1, 2\}$



In the case of  $-11 \bmod 3$  we can see that there are 4 skips needed to enter the modulo range. The distance between where the last skip lands and 0 is the modulo. In this case, this distance is 1.

In the case of  $11 \bmod 3$  we can see that there are 3 skips needed to enter the modulo range. The distance between where the last skip lands and 0 is the modulo. In this case, this distance is 2.

For the operation  $a \bmod b$  and if  $a$  is negative, then we can calculate the modulo using the following expression:

$$a + \lceil \frac{a}{b} \rceil (b) + b \quad (2)$$

### 2.3 Modular Addition

The property of modular addition is as follows:

$$(a + b) \bmod c = ((a \bmod c) + (b \bmod c)) \bmod c \quad (3)$$

This relationship can be derived by using expression (1). Recall that if  $a$  is divisible by  $c$ , and  $b$  is divisible by  $c$ , then  $a+b$  is divisible by  $c$ . We first start by restating  $a + b$ :

$$\begin{aligned} a &= cq_1 + r_1 \therefore a \bmod c = r_1 \\ b &= cq_2 + r_2 \therefore b \bmod c = r_2 \\ a + b &= (cq_1 + r_1 + cq_2 + r_2) \\ a + b &= c(q_1 + q_2) + r_1 + r_2 \end{aligned}$$

Plugging the above result back into  $(a + b) \bmod c$  we get:

$$(c(q_1 + q_2) + r_1 + r_2) \bmod c$$

We can apply the following rule to simplify the above expression. If we have an operation  $a \bmod b$ , then we know that adding a multiple of  $b$  (say  $kb$ ), will result in the same modulo value:  $(a + kb) \bmod b = a \bmod b$ . We can now simplify further:

$$\begin{aligned} (c(q_1 + q_2) + r_1 + r_2) \bmod c \\ = (r_1 + r_2) \bmod c \end{aligned}$$

On the right hand side of expression (3) we can simplify further, using:

$$\begin{aligned} a &= cq_1 + r_1 \therefore a \bmod c = r_1 \\ b &= cq_2 + r_2 \therefore b \bmod c = r_2 \end{aligned}$$

So the right hand side becomes  $(r_1 + r_2) \bmod c$  as well.

## 2.4 Modular Multiplication

The property of modular multiplication is as follows:

$$(ab) \mod c = ((a \mod c) (b \mod c)) \mod c \quad (4)$$

This can be derived in a way similar to modular addition. The left hand side can be rewritten like so:

$$\begin{aligned} & ((cq_1 + r_1)(cq_2 + r_2)) \mod c \\ &= (c^2q_1q_2 + cq_1r_2 + cq_2r_1 + r_1r_2) \mod c \\ &= (c(cq_1q_2 + q_1r_2 + q_2r_1) + r_1r_2) \mod c \end{aligned}$$

Since  $c(cq_1q_2 + q_1r_2 + q_2r_1)$  is a multiple of  $c$ , we are left with:

$$(r_1r_2) \mod c$$

On to the right hand side of expression (4), using:

$$\begin{aligned} a &= cq_1 + r_1 \therefore a \mod c = r_1 \\ b &= cq_2 + r_2 \therefore b \mod c = r_2 \end{aligned}$$

We see that the right hand side of expression (4) becomes:

$$(r_1r_2) \mod c$$

## 2.5 Modular Exponentiation

Modular exponentiation takes the form of evaluation a problem like  $a^x \mod b$ . The challenge here is that  $a^x$  could easily become a very large number, causing errors on calculators. A commonly used technique to overcome this problem is known as "fast modular exponentiation" and it involves restating  $x$  using base-2. Suppose we are trying to evaluate  $7^{15} \mod 17$ . The first step is to translate the exponent into base-2. The number 15 thus becomes  $(1111)_2$ . We can expand this base-2 number with each term representing the binary symbol  $\{0,1\}$  times 2 raised to the power of the place value it appears in:

$$15 = (1)(2)^3 + (1)(2)^2 + (1)(2)^1 + (1)(2)^0$$

With this expansion in mind, we can restate the original problem like so:

$$\begin{aligned} & 7^{15} \mod 17 \\ &= (7^{(1)2^3+(1)2^2+(1)2^1+(1)2^0}) \mod 17 \\ &= (7^{8+4+2+1}) \mod 17 \end{aligned}$$

Finally, we can apply the algebraic rule of exponents and the property of modular multiplication:

$$\begin{aligned} & (7^{8+4+2+1}) \mod 17 \\ &= ((7^8 \mod 17) (7^4 \mod 17) (7^2 \mod 17) (7^1 \mod 17)) \mod 17 \end{aligned}$$

We have now broken the problem into individual components, thus making calculations easier and reducing the likelihood of overflow errors.

## 3 Euclidean Algorithm

### 3.1 GCD and Algorithm Steps

The Greatest Common Divisor (GCD) is the largest common divisor for a set of numbers.

The Euclidean Algorithm outlines a series of steps that can be followed to arrive at the GCD for two integers (say  $a$  and  $b$ ). We start by taking the larger of the two numbers, let's say  $a$ , and rewrite it using the remainder quotient formula:  $a = bq_1 + r_1$ . We will then evaluate  $b = r_1q_2 + r_2$ . We could potentially evaluate  $r_1 = r_2q_3 + r_3$ .

We could encapsulate this recursive operation as  $E(s, t) \rightarrow s = tq_n + r_n$ . We stop when  $s$  or  $t$  becomes 0, and the non-zero value will be the GCD.

**Ex. 1** Evaluate  $\gcd(93, 42)$

$$E(93, 42) \rightarrow 93 = (2)(42) + 9$$

$$E(42, 9) \rightarrow 42 = (4)(9) + 6$$

$$E(9, 6) \rightarrow 9 = (1)(6) + 3$$

$$E(6, 3) \rightarrow 6 = (2)(3) + 0$$

$$E(3, 0)$$

**Solution:**  $\gcd(93, 42) = 3$

**Ex. 2** Evaluate  $\gcd(4278, 8602)$

$$E(8602, 4278) \rightarrow 8602 = (2)(4278) + 96$$

$$E(4278, 96) \rightarrow 4278 = (44)(96) + 42$$

$$E(96, 42)$$

So  $\gcd(4278, 8602) = 42$

### 3.2 Bézout's Lemma

There are integers  $x$  and  $y$  such that  $\gcd(a, b) = xa + yb$ . Matrices with elementary row operations can be used to find  $x$  and  $y$ . We will demonstrate the algorithm using the two examples above.

**Ex. 3** Our claim is that there are integers  $x$  and  $y$  such that  $\gcd(93, 42) = 93x + 42y$ .

State Matrix	Division	Elementary Row Operation
$\begin{bmatrix} 1 & 0 & 93 \\ 0 & 1 & 42 \end{bmatrix}$	$93/42 = 2$ $93 \bmod 42 = 9$	$R_1 - 2R_2 \rightarrow R_1$
$\begin{bmatrix} 1 & -2 & 9 \\ 0 & 1 & 42 \end{bmatrix}$	$42/9 = 4$ $42 \bmod 9 = 6$	$R_2 - 4R_1 \rightarrow R_2$
$\begin{bmatrix} 1 & -2 & 9 \\ -4 & 9 & 6 \end{bmatrix}$	$9/6 = 1$ $9 \bmod 6 = 3$	$R_1 - R_2 \rightarrow R_1$
$\begin{bmatrix} 5 & -11 & 3 \\ -4 & 9 & 6 \end{bmatrix}$	$6/3 = 2$ $6 \bmod 3 = 0$	The stopping condition, that $6 \bmod 3 = 0$ , has been reached.

**Solution:** So  $x = 5$  and  $y = -11$ . We can verify this:  $(93)(5) + (42)(-11) = 3$ .

**Ex. 4** Our claim is that there are integers  $x$  and  $y$  such that  $\gcd(4278, 8602) = 8602x + 4278y$ .

State Matrix	Division	Elementary Row Operation
$\begin{bmatrix} 1 & 0 & 8602 \\ 0 & 1 & 4278 \end{bmatrix}$	$8602/4278 = 2$ $8602 \bmod 4278 = 46$	$R_1 - 2R_2 \rightarrow R_1$
$\begin{bmatrix} 1 & -2 & 46 \\ 0 & 1 & 4278 \end{bmatrix}$	$4278/46 = 93$ $4278 \bmod 46 = 0$	The stopping condition has been reached.

**Solution:** So  $x = 1$  and  $y = -2$ . We can verify this:  $(8602)(1) + (4278)(-2) = 46$

## 4 Congruence

### 4.1 Overview

The statement  $a \equiv b \pmod{n}$ , is another way of stating  $a \bmod n = b \bmod n$ . For example,  $7 \equiv 12 \pmod{5}$  is a true statement, since  $7 \bmod 5 = 2$  and  $12 \bmod 5 = 2$ . We also find that  $17 \bmod 5 = 2$ . These 3 integers belong to the same Congruence Class for mod 5.

Referring back to section 2.1, we know that the only possible outcomes of any integer  $x \bmod 5$  is  $\{0, 1, 2, 3, 4\}$ . Therefore there are 5 different congruence classes for mod 5.

## 4.2 Solving Congruence Problems

Several strategies can be applied to solve the problems of the form  $ax \equiv b \pmod{n}$ . For the next few examples, we will use the following five propositions:

**(p1)** If  $d$  divides  $n$  and we have  $ad \equiv bd \pmod{n}$ , we can simplify this to  $a \equiv b \pmod{\frac{n}{d}}$

**(p2)** If  $\gcd(a, n) = 1$  and we have  $ad \equiv bd \pmod{n}$ , we can simplify this to  $a \equiv b \pmod{n}$

**(p3)** There is a solution to  $ax \equiv b \pmod{n}$  if  $\gcd(a, n) | b$

**(p4)** For  $a\bar{a} \equiv 1 \pmod{n}$ , the inverse  $\bar{a}$  exists if  $\gcd(a, n) = 1$

**(p5)** For  $ax \equiv b \pmod{n}$  where multiple solutions exist, the spread between solutions is  $\frac{n}{\gcd(a, n)}$

Sometimes the solution to a problem is trivial and involves only algebra, consider the following two problems:

**Ex. 5** Solve  $8x \equiv 16 \pmod{5}$  :

First, we observe that  $\gcd(8, 5) = 1$ . We can divide both sides of the congruence by 8 (applying **p2**).

$$x \equiv 2 \pmod{5}$$

To verify our solution:

$$(8)(2) \equiv 16 \pmod{5}$$

$$16 \equiv 16 \pmod{5}$$

**Solution:**  $x \equiv 2 \pmod{5}$

**Ex. 6** Solve  $2x \equiv 8 \pmod{3}$  :

First, we observe that  $\gcd(2, 3) = 1$ . We can divide both sides of the congruence by 2 (applying **p2**).

$$x \equiv 4 \pmod{3}$$

To verify our solution:

$$(2)(4) \equiv 8 \pmod{3}$$

$$8 \equiv 8 \pmod{3}$$

**Solution:**  $4x \equiv ( \pmod{3})$

In some cases, algebra by itself will not work as the division on both sides of the congruence would not produce an integer. For these cases, we can first verify if a solution exists, and determine if  $a$  and  $n$  are coprime. If  $a$  and  $n$  are coprime, we can use the modulo multiplicative inverse.

For a problem  $ax \equiv b \pmod{n}$ , we first check if  $\gcd(a, n) = 1$ . If so, we can evaluate  $a\bar{a} \equiv 1 \pmod{n}$ . Once we determine the value of  $\bar{a}$ . We can multiply both sides of the original congruence by  $\bar{a}$ :

$$\begin{aligned} a\bar{a}x &\equiv \bar{a}b \pmod{n} \\ x &\equiv \bar{a}b \pmod{n} \end{aligned}$$

Let's clarify what happens to the dropped coefficient on the left. The expression  $a\bar{a}x \equiv \bar{a}b \pmod{n}$  can be restated as  $a\bar{a}x \pmod{n} = \bar{a}b \pmod{n}$ .

On the left hand side,  $\bar{a}$  is an integer, that when multiplied by  $ax$  and divided by  $n$ , produces a remainder of 1:  $a\bar{a}x \pmod{n} = 1$ . This is functionally equivalent to saying  $(1)x \pmod{n} = 1$ . We can now rewrite the left hand side:

$$\begin{aligned} a\bar{a}x \pmod{n} &= \bar{a}b \pmod{n} \\ (1)x \pmod{n} &= \bar{a}b \pmod{n} \\ x &\equiv \bar{a}b \pmod{n} \end{aligned}$$

Let's consider a few examples:

**Ex. 7** Solve  $3x \equiv 7 \pmod{11}$

We first determine that  $\gcd(3, 11) = 1$ , so the method can be applied. Since  $1|11$ , an inverse  $\bar{a}$  exists. After some tests, we determine that  $\bar{a}$  is 4.

$$\begin{aligned} (3)(4) \pmod{11} &= 1 \\ \therefore \bar{a} &= 4, \end{aligned}$$

We can now use  $\bar{a}$  to solve the original problem:

$$\begin{aligned} 4x &\equiv (4)(7) \pmod{11} \\ x &\equiv 28 \pmod{11} \end{aligned}$$

We can improve the answer by reporting the smallest positive value. The spread is 11, so  $x \equiv 6 \pmod{11}$  is the best answer. Finally, we can do a quick verification:

$$\begin{aligned} (3)(6) \pmod{11} &= 18 \pmod{11} \\ &= 7 \end{aligned}$$

Solution:  $x \equiv 6 \pmod{11}$

**Ex. 8** Solve  $21x \equiv 14 \pmod{91}$

We notice that  $\gcd(21, 91) = 7$ , so at first glance the inverse technique might not work. However, we can simplify the congruence by dividing both sides by 7, and also divide 91 by 7 (Applying **p1**):

$$\begin{aligned} 21x &\equiv 14 \pmod{91} \\ 3x &\equiv 2 \pmod{13} \end{aligned}$$

We can now apply the technique. We find  $\gcd(3, 13) = 1$ , and since  $1|13$  an inverse exists. After testing some numbers we find:

$$\begin{aligned} (3)(9) &\pmod{13} = 1 \\ \therefore \bar{a} &= 9 \end{aligned}$$

We can now use  $\bar{a}$  to solve the original problem:

$$\begin{aligned} (9)(3)x &\equiv (9)(2) \pmod{13} \\ x &\equiv 18 \pmod{13} \end{aligned}$$

Like the previous problem, we can report a slightly better answer by using the spread, which is 13, leaving us with  $x \equiv 5 \pmod{13}$ . We can verify the answer:

$$\begin{aligned} (21)(5) &\pmod{91} \\ &= 105 \pmod{91} \\ &= 14 \end{aligned}$$

Solution:  $x \equiv 5 \pmod{13}$



**Ex. 9** Solve  $19x \equiv 4 \pmod{141}$

Since  $\gcd(19, 141) = 1$  and  $1 \mid 141$ , the inverse technique can be applied. First we find  $\bar{a}$ :

$$\begin{aligned} (19)(52) \pmod{141} &= 1 \\ \therefore \bar{a} &= 52 \end{aligned}$$

We can now use  $\bar{a}$  to solve the original problem:

$$\begin{aligned} (52)(19)x &\equiv (52)(4) \pmod{141} \\ x &\equiv 208 \pmod{141} \end{aligned}$$

Since the spread is 141, a better answer to report would be  $x \equiv 67 \pmod{141}$ . Let's verify the result:

$$\begin{aligned} (19)(67) \pmod{141} \\ &= 1273 \pmod{141} \\ &= 4 \end{aligned}$$

Solution:  $x \equiv 67 \pmod{141}$

## 5 The Chinese Remainder Theorem

The Chinese remainder Theorem outlines an algorithm that can be used to solve a system of congruences. The steps are illustrated below using a system of three congruences. Suppose we want to solve the following:

$$\begin{aligned} x &\equiv b_1 \pmod{c_1} \\ x &\equiv b_2 \pmod{c_2} \\ x &\equiv b_3 \pmod{c_3} \end{aligned}$$

The theorem can be used if  $c_1, c_2, c_3$  are coprime. We first calculate  $N = (c_1)(c_2)(c_3)$ . We then setup the following table:

$b_i$	$N_i$	$\bar{a}$	$b_i N_i a_i$
$b_1$	$N_1 = n_2 n_3$	$\bar{a}_1$	$b_1 N_1 a_1$
$b_2$	$N_2 = n_1 n_3$	$\bar{a}_2$	$b_2 N_2 a_2$
$b_3$	$N_3 = n_1 n_2$	$\bar{a}_3$	$b_3 N_3 a_3$

The column  $N_i$  represents the calculation  $N_i = \frac{N}{n_i}$ . The column  $\bar{a}$  is the solution to  $\bar{a}$  in  $N_i \bar{a}_i \equiv 1 \pmod{c_i}$ . The solution to the system is the sum of the last column mod N:

$$\left( \sum_{i=1}^3 b_i N_i a_i \right) \pmod{N}$$

Here is an example of the algorithm in action.

**Ex. 10** Suppose that there is a group of students, and the instructor has a choice to group everyone into teams of 3, 4, or 5. If groups of 3 are created, there will be 2 students unassigned students left over. If groups of 4 are made, then there will be 3 students left over, and in the case of groups of 5, then there will be 1 student left over. We want to find a class size that would result in the above outcomes.

The problem can be summarized into the following system of congruences:

$$\begin{aligned}x &\equiv 3 \pmod{4} \\x &\equiv 1 \pmod{5} \\x &\equiv 2 \pmod{3}\end{aligned}$$

From the initial setup, we can see that  $N = (4)(5)(3) = 60$ . We can start to fill in some of the table details:

$b_i$	$N_i$	$\bar{a}$	$b_i N_i a_i$
3	15	$\bar{a}_1$	$b_1 N_1 a_1$
1	12	$\bar{a}_2$	$b_2 N_2 a_2$
2	20	$\bar{a}_3$	$b_3 N_3 a_3$

The next step is to figure out  $\bar{a}_i$ . After some trial and error, we determine the following:

$$\begin{aligned}(15)(3) &\equiv 1 \pmod{15} \therefore \bar{a}_1 = 3 \\(12)(3) &\equiv 1 \pmod{12} \therefore \bar{a}_2 = 3 \\(20)(2) &\equiv 1 \pmod{20} \therefore \bar{a}_3 = 2\end{aligned}$$

We can now complete the table:

$b_i$	$N_i$	$\bar{a}$	$b_i N_i a_i$
3	15	3	135
1	12	3	36
2	20	2	80

The sum of the last column is 251. At this point, we have  $x \equiv 251 \pmod{60}$ . Since the spread is 60, the best reportable answer is  $x \equiv 11 \pmod{60}$ . We can verify this result:

$$11 \pmod{4} = 3 \quad 11 \pmod{5} = 1 \quad 11 \pmod{3} = 2$$

So a class size of 15 meets the criteria, with 3 students left if groups of 4 are made, 1 student left if groups of 5 are made, and 2 left with groups of 3.

**Ex. 11** Here is an additional example. solve the following system:

$$x \equiv 3( \mod 5)$$

$$x \equiv 1( \mod 7)$$

$$x \equiv 6( \mod 8)$$

First, we determine that  $N = (5)(7)(8) = 280$ . We can partially fill our table:

$b_i$	$N_i$	$\bar{a}$	$b_i N_i a_i$
3	56	$\bar{a}_1$	$b_1 N_1 a_1$
1	40	$\bar{a}_2$	$b_2 N_2 a_2$
6	35	$\bar{a}_3$	$b_3 N_3 a_3$

The next step is to figure out  $\bar{a}_i$ . After some trial and error, we determine the following:

$$(56)(1) \equiv 1( \mod 8) \therefore \bar{a}_1 = 1$$

$$(40)(5) \equiv 1( \mod 7) \therefore \bar{a}_2 = 3$$

$$(40)(5) \equiv 1( \mod 7) \therefore \bar{a}_3 = 3$$

We complete the table:

$b_i$	$N_i$	$\bar{a}$	$b_i N_i a_i$
3	56	1	168
1	40	3	120
6	35	3	630

Given the sum of the last column, we have  $x \equiv 918( \mod 280)$ . Since the spread is 280, the best reportable answer is  $x \equiv 78( \mod 280)$