Modular Arithmetic

Written by Andy Tran for the MaPS Correspondence Program

1 Introduction

As an extension to the **Divisibility** topic covered in term 1, **Modular Arithmetic** is an alternate system of arithmetic that is only concerned with the remainders of numbers after division by a certain modulus.

This is a powerful tool in **Number Theory** and can be used to prove many beautiful results. It also has many surprising applications in cryptography, communication and digital security!

We will go through the definitions and some examples of Modular Arithmetic and investigate results including **Quadratic Residues**, **Fermat's Little Theorem** and the **Chinese Remainder Theorem**.

2 Definition

Of course, in Number Theory, we won't always be dealing with expressions that perfectly divide each other. That is we will sometimes have a remainder! The system used to study these remainders is a very powerful tool called Modular Arithmetic.

Definition 2.1 *If two numbers a and b leave the same remainder when divided by a number m, then we write*

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

Another way to interpret this is that if $a - b$ is a multiple of m then $a \equiv b \pmod{m}$.

Example 2.2

$$8 \equiv 3 \pmod{5}$$
$$4 \equiv 16 \equiv 28 \pmod{12}$$
$$17 \equiv -3 \pmod{10}$$

Notice in the last case, we are also allowed to express negative numbers in modular arithmetic. In this case, if we apply the division algorithm to -3, we obtain that

$$-3 = 10 \cdot (-1) + 7$$

so -3 leaves a remainder of 7 when divided by 10 (because the remainder must be positive). Furthermore $17 - (-3) = 20$ which is a multiple of 10, so then $17 \equiv -3 \pmod{10}$.

Note that if we look at a number in modulo 2, we are simply looking at its parity (whether it is odd or even) and if we look at a number in modulo 10, we are only looking at its last digit.

3 Basic Properties

In this new form of arithmetic, we are able to perform arithmetic in *almost* the same way, provided that we are using the same modulus.

Addition: We may add numbers normally in the **same modulus**, for example:

$$9 \equiv 3 \pmod{6}$$
$$\implies 9 + 4 \equiv 3 + 4 \pmod{6}$$
$$\implies 13 \equiv 7 \pmod{6}$$

$$18 \equiv 4 \pmod{7}$$
$$12 \equiv 5 \pmod{7}$$
$$\implies 12 + 18 \equiv 4 + 5 \pmod{7}$$
$$\implies 30 \equiv 9 \pmod{7}$$

The reason why this works is due to the fact that addition doesn't change the sum of the remainders, as if $x = a_1m + b_1$ and $y = a_2m + b_2$, then $x + y = (a_1 + a_2)m + (b_1 + b_2)$, so $x + y \equiv b_1 + b_2 \pmod{m}$.

One thing to notice here is that if $a \equiv b \pmod{m}$, then $a + km \equiv b \pmod{m}$ for any integer k.

Subtraction: In a similar way, subtraction can take place normally in the **same modulus**:

$$\begin{aligned} & 19 \equiv 8 \pmod{11} \\ \implies & 19 - 5 \equiv 8 - 5 \pmod{11} \\ \implies & 14 \equiv 3 \pmod{11} \end{aligned}$$

$$\begin{aligned} & 17 \equiv 13 \pmod{4} \\ & 9 \equiv 1 \pmod{4} \\ \implies & 17 - 9 \equiv 13 - 1 \pmod{4} \\ \implies & 8 \equiv 12 \pmod{4} \end{aligned}$$

Again, this works because subtraction does not change the difference in remainders as if $x = a_1m + b_1$ and $y = a_2m + b_2$, then $x - y = (a_1 - a_2)m + (b_1 - b_2)$, so $x - y \equiv b_1 - b_2 \pmod{m}$.

Multiplication: Furthermore, we can perform multiplication normally in the same modulus:

$$\begin{aligned} & 9 \equiv 4 \pmod{5} \\ \implies & 9 \cdot 3 \equiv 4 \cdot 3 \pmod{5} \\ \implies & 27 \equiv 12 \pmod{5} \end{aligned}$$

$$\begin{aligned} & 13 \equiv 5 \pmod{8} \\ & 3 \equiv 11 \pmod{8} \\ \implies & 13 \cdot 3 \equiv 5 \cdot 11 \pmod{8} \\ \implies & 39 \equiv 55 \pmod{8} \end{aligned}$$

If we look a the remainders of each term, we can understand why this is allowed:

$$\begin{aligned} x &= a_1m + b_1 \\ y &= a_2m + b_2 \\ xy &= (a_1m + b_1)(a_2m + b_2) \\ \implies xy &= a_1m \cdot a_2m + a_1mb_2 + a_2mb_1 + b_1b_2 \\ \implies xy &= (a_1a_2m + a_1b_2 + a_2b_1)m + b_1b_2 \\ \implies xy &\equiv b_1b_2 \end{aligned}$$

Exponentiation: As exponentiation is essentially repeated multiplication, we can raise both sides **to the same power:**

$$\begin{aligned} & 7 \equiv 3 \pmod{4} \\ \implies & 7^2 \equiv 3^2 \pmod{4} \\ \implies & 49 \equiv 9 \pmod{4} \end{aligned}$$

$$\begin{aligned} & 4 \equiv -1 \pmod{5} \\ & 4^3 \equiv (-1)^3 \pmod{5} \\ \implies & 64 \equiv -1 \pmod{5} \end{aligned}$$

This means that modular arithmetic can be a useful tool when dealing with numbers with large powers.

But beware that we must raise both sides to the same power. Consider:

$$\begin{aligned} & 7 \equiv 2 \pmod{5} \\ & 1 \equiv 6 \pmod{5} \\ \text{but } & 7^1 \not\equiv 2^6 \pmod{5} \end{aligned}$$

Division: Strangely enough, division works in some cases but not others, for example:

$$\begin{aligned} 35 &\equiv 15 \pmod 4 \\ \implies \frac{35}{5} &\equiv \frac{15}{5} \pmod 4 \\ \implies 7 &\equiv 3 \pmod 4 \end{aligned}$$

$$\begin{aligned} 15 &\equiv 6 \pmod 9 \\ \text{but } \frac{15}{3} &\not\equiv \frac{6}{3} \pmod 9 \\ 5 &\not\equiv 2 \pmod 9 \end{aligned}$$

The reason for this difference is made clear if we investigate what happens when we divide a number which has already undergone the division algorithm.

$$\begin{aligned} x &= a_1 m + b_1 \\ \frac{x}{d} &= \frac{a_1}{d} m + \frac{b_1}{d} \end{aligned}$$

This means that $\frac{x}{d} \equiv \frac{b_1}{d}$ if and only if d and m are **coprime** (they do not share any common factors).

Exercise 3.1 *Decide if the following statements are true or false. If it is true, try to prove it. If it is false, find a counterexample and if possible, salvage the statement. You may assume that a, b, c, d, m, n are integers and p is a prime.*

1. $a \equiv b \pmod m \iff a + c \equiv b + c \pmod m$
2. $a \equiv b \pmod m \iff ac \equiv bc \pmod m$
3. $a \equiv b \pmod m \iff a^c \equiv b^c \pmod m$
4. $a \equiv b \pmod m$ and $c \equiv d \pmod m \implies a + c \equiv b + d \pmod m$
5. $a \equiv b \pmod m$ and $c \equiv d \pmod m \implies ac \equiv bd \pmod m$
6. $a \equiv b \pmod m$ and $c \equiv d \pmod m \implies a^c \equiv b^d \pmod m$
7. $ab \equiv 0 \pmod m \implies a \equiv 0 \pmod m$ or $b \equiv 0 \pmod m$
8. $ab \equiv ac \pmod{ad} \iff b \equiv c \pmod d$
9. $ab \equiv ac \pmod p \iff b \equiv c \pmod p$
10. $a^2 \equiv b^2 \pmod p \iff a \equiv \pm b \pmod p$

4 Quadratic Residues

A fascinating property in modular arithmetic is that square numbers can only take some remainders in particular moduli.

Example 4.1 *What are the possible remainders when a square number number is divided by 4? To be technical, we are asking what are the* ***quadratic residues*** *in* mod 4.

Every integer will be congruent to one of $\{0, 1, 2, 3\}$ in mod 4. Thus, the square of any integer will be congruent to one of the following:

$$\begin{aligned} 0^2 &\equiv 0 \\ 1^2 &\equiv 1 \\ 2^2 &\equiv 4 \equiv 0 \\ 3^2 &\equiv 9 \equiv 1 \end{aligned}$$

Hence, any square number will leave a remainder of 0 or 1 when divided by 4. This can be a very powerful tool when trying to prove that solutions to a Diophantine equation do not exist.

Example 4.2 *Prove that there are no integers x and y such that $x^2 + y^2 = 2023$.*

Recall that every square number leaves a remainder of 0 or 1 when divided by 4. This means that the possible remainders of the left hand side when divided by 4 are 0, 1 or 2.

$x^2 \pmod 4$	$y^2 \pmod 4$	$x^2 + y^2 \pmod 4$
0	0	0
0	1	1
1	0	1
1	1	2

But the right hand side leaves a remainder of 3 when divided by 4 as $2023 \equiv 3 \pmod 4$. This means that there cannot be any values of x and y such that the equation holds. □

Quadratic residues are particularly interesting in prime moduli, and in modulo 4, 8 and 16 - it is highly recommended that you investigate these yourself, and discover patterns in other moduli. Similarly, we can investigate cubic residues, quartic residues and so on.

Exercise 4.3 *What are the cubic residues in mod 7? That is, what are the possible remainders that a cube number can have when divided by 7?*

Exercise 4.4 *Prove that there are no integers x and y such that $x^3 + y^3 = 2020$.*

Exercise 4.5 *What are the quartic residues in mod 5? That is, what are the possible remainders that a fourth power can have when divided by 5?*

5 Fermat's Little Theorem

Consider the following table of residues in mod 7.

n	n^2	n^3	n^4	n^5	n^6	n^7
0	0	0	0	0	0	0
1	1	1	1	1	1	1
2	4	1	2	4	1	2
3	2	6	4	5	1	3
4	2	1	4	2	1	4
5	4	6	2	3	1	5
6	1	6	1	6	1	6

There are many interesting patterns here! In particular, notice that the column for n^6 stands out quite a bit from the rest because all the non-zero remainders become 1. In fact, this is a property that extends to all prime numbers.

Theorem 5.1 (Fermat's Little Theorem) *For any integer a and prime p, $a^p \equiv a \pmod p$*

Another version of the theorem states that for any prime p, and a coprime to p,

$$a^{p-1} \equiv 1 \pmod p.$$

This can be extremely useful when solving questions involving very large powers of numbers. We shall prove this theorem in the problem set.

Exercise 5.2 *What is the remainder when 3^{2022} is divided by 7?*

6 Inverses

We have already established that modular arithmetic behaves very similarly to normal arithmetic - which leads us to the question of whether fractions can exist in modular arithmetic. Without directly using division (because this isn't always allowed in modular arithmetic), we can actually interpret fractions in terms of multipilcation. ie. $\frac{1}{2}$ can be interpreted as the number x that satisfies the equation $2 \cdot x = 1$.

Example 6.1 (Inverses in $\mod 5$)

$$
\begin{aligned}
1 \cdot 1 \equiv 1 &\implies \frac{1}{1} \equiv 1 \\
2 \cdot 3 \equiv 6 \equiv 1 &\implies \frac{1}{2} \equiv 3 \\
3 \cdot 2 \equiv 6 \equiv 1 &\implies \frac{1}{3} \equiv 2 \\
4 \cdot 4 \equiv 16 \equiv 1 &\implies \frac{1}{4} \equiv 4
\end{aligned}
$$

However, be warned that not all numbers will have inverses.

Example 6.2 (Inverses in $\mod 8$**)**

$$
\begin{aligned}
1 \cdot 1 \equiv 1 &\implies \frac{1}{1} \equiv 1 \\
2 \cdot ? \equiv 1 &\implies \frac{1}{2} \text{ does not exist} \\
3 \cdot 3 \equiv 9 \equiv 1 &\implies \frac{1}{3} \equiv 3 \\
4 \cdot ? \equiv &\implies \frac{1}{4} \text{ does not exist} \\
5 \cdot 5 \equiv 25 \equiv 1 &\implies \frac{1}{5} \equiv 5 \\
6 \cdot ? \equiv 1 &\implies \frac{1}{6} \text{ does not exist} \\
7 \cdot 7 \equiv 49 \equiv 1 &\implies \frac{1}{7} \equiv 7 \\
8 \cdot ? \equiv 1 &\implies \frac{1}{8} \text{ does not exist}
\end{aligned}
$$

Notice how this links with how division only works in some cases. In particular, **the inverse of a number exists if and only if we can divide by that number**.

Theorem 6.3 (Inverses) *A number n in mod m has an inverse if and only if m and n are coprime.*

So we know how to determine whether or not the inverse of a number exists. But is there a method to find the inverse? [Hint: the Euclidean Algorithm!]

Exercise 6.4 *Find the inverse of 110 in mod 271.*

7 Wilson's Theorem

This is an interesting theorem which has some theoretical applications - a guided proof is left in the problem set.

Theorem 7.1 (Wilson's Theorem) *For any prime p, $(p-1)! \equiv -1 \pmod{p}$.*

8 Chinese Remainder Theorem

In all the previous sections, we only performed arithmetic in the same modulus, however this theorem allows us to combine equations from different moduli.

Theorem 8.1 (Chinese Remainder Theorem) *If $m_1, m_2, \ldots, m_n$ are pairwise relatively prime positive integers, and $a_1, a_2, \ldots a_n$ are a sequence of integers, then there is a unique remainder x in mod $m_1 m_2 \ldots m_n$, such that:*

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\cdots \\
x &\equiv a_n \pmod{m_n}
\end{aligned}
$$

To illustrate this, let us look at an example.

Example 8.2 *Find all numbers n such that $n \equiv 1 \pmod{3}, n \equiv 3 \pmod{4}$ and $n \equiv 5 \pmod{7}$.*

Since 3,4 and 7 are pairwise relatively coprime (no two of them share any common factors), then the Chinese Remainder Theorem simply tells us that there is a unique remainder n in $\pmod{3 \cdot 4 \cdot 7} = \pmod{84}$ which satisfies the above three modular equations.

Unfortunately, the theorem doesn't give us a method in finding out what this remainder is (however there do exist methods of efficiently finding the remainder). With some structured trial and error, we can come to the conclusion that $n \equiv 19 \pmod{84}$. □

One thing to pay attention to is the requirement that the moduli are pairwise relatively prime.

Exercise 8.3 *Can you find any numbers n such that $n \equiv 3 \pmod{4}$ and $n \equiv 2 \pmod{6}$?*

9 Additional Problems

These are some extra problems to help you develop a deeper understanding of divisibility and modular arithmetic.

1. (a) Prove the divisibility rule for 3 - *"A number is divisible by 3 if and only if the sum of its digits are divisible by 3."*
   (b) Prove the divisibility rule for 9 - *"A number is divisible by 9 if and only if the sum of its digits are divisible by 9."*
   (c) Prove the divisibility rule for 11 - *"A number is divisible by 11 if and only if the sum of its odd-positioned digits and the sum of the even-positioned digits differ by a multiple of 11."*
2. (a) Prove that for all integers n, the last digit of n^5 is the same as the last digit of n.
   (b) Show that $n^5 - n$ is divisible by 30 for all integers n.
3. Victor ate some jelly beans from a pile which originally had 100 jellybeans. If he splits the remaining jellybeans into piles of 8, there will be 5 left over, and if he splits them into piles of 9, there will be 7 left over. How many jellybeans did Victor eat?
4. Prove that
$$104^{3994} + 25^{3994} - 5^{3994} - 3^{3994}$$
is divisible by 187.
5. Let p and q be distinct primes. Show that
$$p^{q-1} + q^{p-1} - 1$$
is divisible by pq.
6. Prove that there is no triangular number which is five more than a multiple of 11.
7. Prove that there are no integer solutions to the equation $x^2 - 2y^2 = 10$.