MATH221
Mathematics for Computer Science

Unit 9
Modular Arithmetic

OBJECTIVES

- Understand the concept of Congruence Modulo *n*.
- Apply the arithmetic of Congruences.
- Know the Classes of Congruence Modulo *n*.
- Know the Complete Set of Congruence Classes $\mathbb{Z}_n$.
- Know the properties of $\mathbb{Z}_n$.

Introduction

Congruence Arithmetic is a form of arithmetic dealing with integers in which all numbers having the same remainder when divided by a whole number are considered equivalent.

It has vast applications such as in cryptography, visual arts, game theory, etc.

Congruence Modulo *n*

Let $n \in \mathbb{N}$.

We define a relation on $\mathbb{Z}$ called ***congruence modulo n*** (denoted $\equiv$) by

$$\forall a, b \in \mathbb{Z}, (a \equiv b \pmod{n} \quad \Leftrightarrow \quad n \mid (a - b)).$$

Congruence Modulo *n*: Notes

1. "$a \equiv b \pmod{n}$" reads "*a* is congruent to *b* modulo *n*."

2. The definition says that $a \equiv b \pmod{n}$ if and only if *n* divides the difference between *a* and *b*.

   Example.

   $38 \equiv 2 \pmod{6}$ because $38 – 2 = 36$ and $6 \mid 36$.

Congruence Modulo *n*: Notes

3. Another way to think about congruence modulo *n* is in terms of remainders:

   $a \equiv b \pmod{n}$ if and only if *a* and *b* have the same remainder after being divided by *n*.

   Example.

   $38 \equiv 2 \pmod{6}$ because both 38 and 2 have remainder 2 after being divided by 6.

Exercise:

1. Find a value for $m \in \mathbb{N}$ in each case.

   (i) $14 \equiv m \pmod{8}$, $0 \leq m < 8$

   $14 - m = 8k$, $k \in Z$ (from def)

   Set $k = 1$, we have $14 - m = 8$ (we can set k to any integer that will get a $m \in \mathbb{N}$, hence, the solution for m is not unique). But, the solution in the range 0, ……,7 is unique. The solution in this range is the remainder of any solution divided by 8.

   Following the latter method, we get m = 6

   6

   (ii) $-3 \equiv m \pmod{8}$), $0 \leq m < 8$

   5

   (iii) $(n + 1) \equiv m \pmod{n}$, $n > 1$, $0 \leq m < n$

   1

Exercise:

3. Find a value for $x \in \mathbb{N}$ in each case.

   (a) $x \equiv -1 \pmod{7}$), $0 \leq x < 8$

   $x - (-1) = 7k$, $k \in Z$ (from def)

   Set $k = 1$, we have $x + 1 = 7$ (we can set k to any integer that will get a $x \in \mathbb{N}$, hence, the solution for m is not unique). But, the solution in the range 0, ……,6 is unique. The solution in this range is the remainder of any solution divided by 7.

   Following the latter method, We get x = 6

   6

   (b) $x \equiv 3 \pmod{5}$, $0 \leq x < 5$

   8

   (c) $x \equiv -4 \pmod{9}$, $0 \leq x < 9$

   5

Exercise:

4. If $m \equiv 0$ (mod 2), what can you say about m?
m is even.
$(m - 0) = 2k, k \in Z$ (from def)
We get $m = 2k$, $k \in Z$
From def of even, m is even

If $n \equiv 1$ (mod 2), what can you say about n?
n is odd.
$(n - 1) = 2k, k \in Z$ (from def)
We get $n = 2k + 1, k \in Z$
From def of odd, m is odd

Lemma 1

Let $n \in \mathbb{N}$, and $a, b, c, d \in \mathbb{Z}$.

(i) If $a \equiv b$ (mod n)
and $c \equiv d$ (mod n),
then $(a + c) \equiv (b + d)$ (mod n)
and $ac \equiv bd$ (mod n).

(ii) If $\gcd(a, n) = 1$
and $ab \equiv ac$ (mod n),
then $b \equiv c$ (mod n).

Note: After going through the details of the proof for this theorem, for the remaining theorems, lemma, etc., we shall focus on the application. For their proofs, please refer to the supplementary notes.

Lemma 1: Proof

(i) We know that
$a \equiv b$ (mod n) $\Rightarrow$ $n \mid (a - b)$
$\Rightarrow$ $\exists k \in \mathbb{Z}, a - b = nk$ (1)
$c \equiv d$ (mod n) $\Rightarrow$ $n \mid (c - d)$
$\Rightarrow$ $\exists q \in \mathbb{Z}, c - d = nq$ (2)
We must prove that $(a + c) \equiv (b + d)$ (mod n), that is,
$n \mid [(a + c) - (b + d)]$.
To do this, we must find l such that $(a + c) - (b + d) = ln$.
Adding equations (1) and (2), we have
$a + c - b - d = nk + nq$
$\Rightarrow$ $(a + c) - (b + d) = n(k + q)$.
By letting $l = k + q \in \mathbb{Z}$, we have $(a + c) \equiv (b + d)$ (mod n).

Lemma 1: Proof

Next we must prove that $ac \equiv bd$ (mod n), that is, $n \mid (ac - bd)$. To do this, we must find s such that $ac - bd = sn$. Consider

(1) × c: $ac - bc = nkc$ (3)
(2) × b: $cb - db = nqb$ (4)

Adding equations (3) and (4), we have
$ac - bc + cb - db = nkc + nqb$
$\Rightarrow$ $ac - db = n(kc + qb)$.
By letting $s = kc + qb \in \mathbb{Z}$, we have $ac \equiv bd$ (mod n).

Lemma 1: Proof

(ii) We know that $\gcd(a, n) = 1$ and $ab \equiv ac \pmod{n}$.

Now, by definition of congruence modulo n, we have

$$n \mid (ab - ac) \quad \Rightarrow \quad n \mid a(b - c)$$
$$\Rightarrow \quad n \mid (b - c).$$

Since $\gcd(a, n) = 1$, from Corollary in Unit 8, $n \mid (b - c)$.

Therefore, $b \equiv c \pmod{n}$.

Examples of (ii)

(a) $\gcd(5, 4) = 1$ and $5 \times 6 \equiv 5 \times 2 \pmod{4}$

[that is, $30 \equiv 10 \pmod{4}$].

Also, $6 \equiv 2 \pmod{4}$.

(b) $\gcd(6, 3) = 3$ and $6 \times 1 \equiv 6 \times 2 \pmod{3}$

[that is, $6 \equiv 12 \pmod{3}$].

However, $1 \not\equiv 2 \pmod{3}$.

This is because $\gcd(6, 3) \neq 1$.

Note that the condition that $\gcd(a, n) = 1$ is necessary.

Lemma 1: Note

Lemma 1 allow us to calculate remainders without actually performing a long division.

Lemma 1: Examples

Find x such that $3^9 \equiv x \pmod{5}$, $0 \leq x < 5$.

$3 \equiv 3 \pmod{5}$ (1)

Multiplying (1) and (1), $3^2 \equiv 9$

Since $9 \equiv 4 \pmod{5}$

Hence $3^2 \equiv 4 \pmod{5}$ (2)

From (1) and (2),

$3 \times 3^2 \equiv 3 \times 4 \pmod{5} \equiv 12 \pmod{5}$

But $3 \times 3^2 \equiv 3^3$ and $12 \equiv 2 \pmod{5}$, so

$3^3 \equiv 2 \pmod{5}$ (3)

Lemma 1: Examples

From (3),

$3^3 \times 3^3 \equiv 2 \times 2 \pmod{5} \equiv 4 \pmod{5}$

But $3^3 \times 3^3 = 3^6$, so

$3^6 \equiv 4 \pmod{5}$ (4)

From (3) and (4),

$3^3 \times 3^6 \equiv 2 \times 4 \pmod{5} \equiv 8 \pmod{5}$

But $3^3 \times 3^6 = 3^9$ and $8 \pmod{5} \equiv 3 \pmod{5}$, so

$3^9 \equiv 3 \pmod{5}$.

Therefore, $x = 3$.

Exercise:

Find the remainder when 7^7 is divided by 16.

$7 \equiv 7 \pmod{16}$ (1)

Now, $7^2 = 49$ and $49 \equiv 1 \pmod{16}$, hence

$7^2 \equiv 1 \pmod{16}$ (2)

From (1) and (2),

$7 \times 7^2 \equiv 7 \times 1 \pmod{16} \equiv 7 \pmod{16}$

But $7 \times 7^2 = 7^3$, so

$7^3 \equiv 7 \pmod{16}$ (3)

Exercise:

From (3),

$7^3 \times 7^3 \equiv 7 \times 7 \pmod{16} \equiv 1 \pmod{16}$

But $7^3 \times 7^3 = 7^6$, so

$7^6 \equiv 1 \pmod{16}$ (4)

From (1) and (4) (multiply them side by side),

$7 \times 7^6 \equiv 7 \times 1 \pmod{16} \equiv 7 \pmod{16}$

But $7 \times 7^6 = 7^7$, so

$7^7 \equiv 7 \pmod{16}$.

Hence, 7^7 divide by 16, the remainder is 7

Notes:

In finding solutions for the types of problems as per the last example and exercise, we apply one of the following methods to raise the exponent on the left-hand-side:

1) Multiply the same modulo equation a certain number of times according to the need.
2) Multiply two different modulo equations together .

Theorem - Existence of inverses Modulo n

If a and n are relatively prime integers (so gcd(a, n) = 1), then there exists an integer s such that

as ≡ 1 (mod n).

We call s **an inverse of a modulo** n.

Example:

Since 2.3 = 6 ≡ 1 (mod 5), hence 3 is the inverse of 2 modulo 5.

Exercise: Finding an Inverse

Find an inverse for 43 modulo 60.

Using Euclidian Algo, we have:

60 =43 +17 ----- (1)
43 = 17x2 + 9 ------(2)
17= 9x1 + 8 ------(3)
9 = 8x1 + 1 ------ (4)
8 = 1x8 + 0
Hence, gcd(43, 60) =1

Exercise: Finding an Inverse

Find an inverse for 43 modulo 60.

Using Euclidian Algo, we have:

(1) ⇒ 17 = 60 – 43 ---- (6)
(2) ⇒ 9 = 43 – 17x2 ---- (7)
(3) ⇒ 8 = 17 – 9 x1 ---- (8)
(4) ⇒ 1 = 9 - 8x1 ---- (9)

Work backwards, we get

1 = 9 - 8x1 --- from (9)
= 9 – (17 – 9 x1) x1 = – 17 + 9x2 ---- from (8)
= -17 + (43 – 17x2)x2 = 43x2 – 17x5 --- from (7)
= 43x2 – (60 – 43)x5 ---- from (6)
= -60x5 + 43x7
= 7x43 – 5x60

Therefore, 7 is the inverse of 43 modulo 60

Lemma 2

Let $n \in \mathbb{N}$.

If $x \in \mathbb{Z}$, then x is congruent (modulo n) to exactly one element in $\{0, 1, 2, \ldots, n - 1\}$.

Note to Lemma 2:

This Lemma is important as it allows us to group integers according to their remainder after dividing by a given number $n \in \mathbb{N}$. This introduce the concept of congruence classes.

Congruence Modulo Relation: An Equivalence Relation

Let $n \in \mathbb{N}$. The **congruence modulo n** relation R on $\mathbb{Z}$ is defined as follows:

$$R = \{(a, b): a \equiv b \text{ (mod } n)\}$$

This relation is an equivalence relation.

For the proof of this equivalence relation, please refer to the supplementary notes.

Congruence Class

Let $n \in \mathbb{N}$ and $s \in \mathbb{Z}$.

We define the **congruence class** (or **residue class**) **of *s* modulo *n*** denoted $[s]$ by

$$[s] = \{x \in \mathbb{Z}: x \equiv s \text{ (mod } n)\}.$$

Exercise:

1. Write down 4 elements in the following congruence classes if $n = 4$.

   [0] = {…, 0, 4, 8, 12, …}
   [1] = {…, 1, 5, 9, 13, …}
   [2] = {…, 2, 6, 10, 14, …}
   [3] = {…, 3, 7, 11, 15, …}
   [4] = {…, 4, 8, 12, 16, …}
   [5] = {…, 5, 9, 13, 17,…}

Exercises:

2. How many distinct congruence classes are there in (mod 4) do you expect there to be?
   4

Lemma 3.

If $n \in \mathbb{N}$, then there are exactly n distinct congruence classes determined by n, namely [0], [1], [2], …, $[n - 1]$.

The Set of Congruence Classes

For all $n \in \mathbb{N}$, we let

$\mathbb{Z}_n = \{[0], [1], [2], …, [n - 1]\}$

and say that $\mathbb{Z}_n$ is the **complete set of congruence classes** modulo n or the complete set of residues modulo n.

Exercise:

1. What are $\mathbb{Z}_3$, $\mathbb{Z}_{218}$ and $\mathbb{Z}_1$?

   $\mathbb{Z}_3 = \{[0], [1], [2]\}$

   $\mathbb{Z}_{218} = \{[0], [1], [2], … [217]\}$

   $\mathbb{Z}_1 = \{[0]\}$

2. In $\mathbb{Z}_3$, what are the sets [4], [-2], [7] and [40] usually expressed as?

   [1]

Exercise:

3. How many "names" are there for [3] in $\mathbb{Z}_{10}$? List three.

   [3] = [13] = [23] = [33].

4. In $\mathbb{Z}_n$,

   $\{[0]\} \cup \{[1]\} \cup \{[2]\} \cup … \cup \{[n - 1]\}$

   $= \mathbb{Z}_n$

   and

   $[0] \cap [1] \cap [2] \cap … \cap [n - 1]$

   $= \varnothing$

The Set of Congruence Classes: Note

As seen in exercise 2 and 3, $\mathbb{Z}_n$ is a set of elements, each of which has an infinite number of names.

The names [0], [1], [2], …, $[n-1]$, however, are the standard ones, and we normally use these unless there is a specific reason to use others.

Aside:

A similar point arises about the names or representations of rational numbers. For example,

$$\frac{1}{2}=\frac{2}{4}=\frac{3}{6}=\frac{100}{200}=\ldots$$

the same rational number can be represented in infinitely many different ways.

Aside:

When we define + and × on $\mathbb{Z}_n$, we must make sure our definitions do NOT depend on the name of the congruence class.

Once this is proven, we can say that + and × on $\mathbb{Z}_n$ are **well-defined** operations.

Example:

Consider $\mathbb{Z}_{10}$.

Name of the congruence classes: [3] = [13] = [23] = [33].

Addition and Multiplication on Congruence Class

We define + and × on $\mathbb{Z}_n$ as follows.

$\forall [a], [b] \in \mathbb{Z}_n$, $[a] + [b] = [a + b]$

and $[a] \times [b] = [ab]$.

Example

In $\mathbb{Z}_3$, we know

$[1] = [4]$ and $[2] = [5]$.

We want

$[1] + [2] = [4] + [5]$.

Now, $[1] + [2] = [1 + 2] = [3] = [0]$

and $[4] + [5] = [4 + 5] = [9] = [0]$

Therefore, $[1] + [2] = [4] + [5]$.

Lemma 4

$[a] = [b]$ in $\mathbb{Z}_n \Leftrightarrow a \equiv b \pmod{n}$

Proposition 1.

Let $n \in \mathbb{N}$.

Addition and multiplication on $\mathbb{Z}_n$ are well-defined.

Proposition 1: Proof for Addition

Let $[a] = [c]$ and $[b] = [d]$ in $\mathbb{Z}_n$.

We must prove that $[a + b] = [c + d]$.

Now, $[a] = [c] \Rightarrow a \equiv c \pmod{n}$

and $[b] = [d] \Rightarrow b \equiv d \pmod{n}$.

Using Lemma 1, we can deduce that

$(a + b) \equiv (c + d) \pmod{n}$

and so $[a + b] = [c + d]$.

Therefore, addition on $\mathbb{Z}_n$ is well-defined.

Proposition 1: Proof for Multiplication

Let $[a] = [c]$ and $[b] = [d]$ in $\mathbb{Z}_n$.
We must prove that $[a \times b] = [c \times d]$.

Now, $[a] = [c] \Rightarrow a \equiv c \pmod{n}$
and $[b] = [d] \Rightarrow b \equiv d \pmod{n}$.

Using Lemma 1, we can deduce that
$(a \times b) \equiv (c \times d) \pmod{n}$
and so $[a \times b] = [c \times d]$.

Therefore, multiplication on $\mathbb{Z}_n$ is well-defined.

Exercise:

1. Write out the addition and multiplication tables for $\mathbb{Z}_3$.
Are + and × closed operations?
Yes.

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Exercise:

2. Solve these equations for x in $\mathbb{Z}_3$?

$x + [2] = [0]$
$\Rightarrow \quad x = [1].$

$x \times [2] = [1]$
$\Rightarrow \quad x = [2]\,.$

$x \times [0] = [1]$
$\Rightarrow$ no solution.

$x + [0] = [2]$
$\Rightarrow \quad x = [2].$

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

×	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Exercise:

3. Write out the multiplication table for $\mathbb{Z}_4$.
Is × a closed operation on $\mathbb{Z}_4$?
Yes.

×	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Exercise:

×	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

4. Solve these equations for x in $\mathbb{Z}_4$.

$[2]x = [2]$

$\Rightarrow \quad x = [1]$ or $[3]$.

$[2]x = [0]$

$\Rightarrow \quad x = [0]$ or $[2]$.

$[2]x = [1]$

$\Rightarrow$ no solution.

$[3]x = [1]$

$\Rightarrow \quad x = [3]$.

Application: RSA Cryptography

Cryptography is the study of methods for sending secret messages. The basic idea is that someone sends an encrypted message to someone else for them to decrypt. There are many different techniques for encryption/decryption.

One such technique is called Public-Key Cryptography. In this form of cryptography the method of encryption is open to anyone, but the method of decryption is only known to those who need to know. The whole technique works on big primes numbers.

RSA cryptography was the first public-key cryptography technique. It was developed in 1976-77 by three MIT mathematicians/computer scientists, named Ronald **R**ivest, Adi **S**hamir and Leonard **A**dleman.

RSA Cryptography

The basic process behind RSA Cryptography is the following:

(1) Choose two large prime numbers p and q.
(2) Choose a positive integer e which is relatively prime to (p - 1)(q - 1).
(3) Choose an integer d such that ed ≡ 1 (mod (p - 1)(q -1)).
(4) The Public Key is the pair (e; pq).
(5) The Private Key is the pair (d; pq).

Encryption Step: Let the message to be encrypted be the integer M with 0 ≤ M < pq. (Note that computers turn everything into zeroes and ones, so working with integers is normal!) The encrypted message C called **ciphertext** is

$$C \equiv M^e \pmod{pq} \qquad (1)$$

RSA Cryptography

Decryption Step: The original message M is recovered from the encrypted message (ciphertext) C via

$$M \equiv C^d \pmod{pq} \qquad (2)$$

We will not prove how (2) works. But note that choosing 0 ≤ M < pq ensures that (2) gives back M. And since p and q are usually so large, requiring that 0 ≤ M < pq does not cause problems.

The whole process works because p and q are chosen to be primes of the order of several hundred digits. So their product is twice that size. And computers are not able to factor numbers of that size in any reasonable length of time.

Next, we now look at an example.

RSA Cryptography

Example

We use the Caesar cipher to send English messages using integers via

A = 1, B = 2, ….., Z = 26.

Betty chooses two prime numbers p = 5, q = 11, and computes pq = 55. She then chooses the positive integer e = 3 that is relatively prime to (5 -1)(11 -1) = 40.

So, Betty sets her public key to (3, 55).

Since 27 is an inverse of 3 modulo 40 (you can follow the earlier method to compute the inverse), Betty sets her private key to (27, 55).

Note that Betty will distribute the public key and she will not disclose the private key.

RSA Cryptography

Example (cont'd)

Bob wants to say “HI" to Betty (but he has to keep it top secret). The text is encoded as follows:

8 9

And, it is encrypted into ciphertext using equation (1) as follows:

8: $C = 8^3$ (mod 55) = 512 (mod 55) = 17

9: $C = 9^3$ (mod 55) = 729 (mod 55) = 14

So, Bob send the following message to Betty:

17 14

When Betty receives this message (in ciphertext) , she decrypts it as follows:

17: $M = 17^{27}$ (mod 55) = 8

14: $M = 14^{27}$ (mod 55) = 9

Hence, Betty receives: 8 9.

After translating to alphabet according to Caesar cipher, it is “HI”

End of Unit 9