

Week 5 Modular Arithmetic Reading Note

Notebook: Computational Mathematics

Created: 2020-04-21 2:48 PM

Updated: 2020-05-07 4:10 PM

Author: SUKHJIT MANN

Cornell Notes	Topic: Modular Arithmetic	Course: BSc Computer Science
		Class: Computational Mathematics[Reading]
		Date: May 06, 2020
Essential Question:		
What is divisibility and congruence among two numbers?		
Questions/Cues:		
<ul style="list-style-type: none">• What do we mean when we say a divides b?• What is meant by a trivial divisor?• What are some basic properties of divisibility?• What is the division algorithm/theorem?• What is a consequence observed when applying the division algorithm?• What is a prime number/integer?• What is "$a \bmod n$" and how does this relate to the remainder of a divides n?• What do mean when it is said that "a is congruent to b modulus n"?• What is a residue of a modulo n?• What properties does the congruence relation have in common with equality relation?• What is a residue class and its importance in the congruence of two numbers?• What are some arithmetic properties of congruences?		
Notes		
<p>Definition 1.2.1. Let a and b be integers with $a \neq 0$. We say a divides b, denoted by $a \mid b$, if there exists an integer c such that $b = ac$. When a divides b, we say that a is a <i>divisor</i> (or <i>factor</i>) of b, and b is a <i>multiple</i> of a. If a does not divide b, we write $a \nmid b$. If $a \mid b$ and $0 < a < b$, then a is called a <i>proper divisor</i> of b.</p>		
<p>Remark 1.2.1. We never use 0 as the left member of the pair of integers in $a \mid b$, however, 0 may occur as the right member of the pair, thus $a \mid 0$ for every integer a not zero. Under this restriction, for $a \mid b$, we may say that b is divisible by a, which is equivalent to say that a is a divisor of b. The notation $a^\alpha \parallel b$ is sometimes used to indicate that $a^\alpha \mid b$ but $a^{\alpha+1} \nmid b$.</p>		

Example 1.2.1. The integer 200 has the following positive divisors (note that, as usual, we shall be only concerned with positive divisors, not negative divisors, of an integer):

$$1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200.$$

Thus, for example, we can write

$$8 \mid 200, 50 \mid 200, 7 \nmid 200, 35 \nmid 200.$$

Definition 1.2.2. A divisor of n is called a *trivial divisor* of n if it is either 1 or n itself. A divisor of n is called a *nontrivial divisor* if it is a divisor of n , but is neither 1, nor n .

Example 1.2.2. For the integer 18, 1 and 18 are the trivial divisors, whereas 2, 3, 6 and 9 are the nontrivial divisors. The integer 191 has only two trivial divisors and does not have any nontrivial divisors.

Some basic properties of divisibility are given in the following theorem:

Theorem 1.2.1. Let a, b and c be integers. Then

- (1) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
- (2) if $a \mid b$, then $a \mid bc$, for any integer c .
- (3) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof.

- (1) Since $a \mid b$ and $a \mid c$, we have

$$b = ma, \quad c = na, \quad m, n \in \mathbb{Z}.$$

Thus $b + c = (m + n)a$. Hence, $a \mid (m + n)a$ since $m + n$ is an integer. The result follows.

- (2) Since $a \mid b$ we have

$$b = ma, \quad m \in \mathbb{Z}.$$

Multiplying both sides of this equality by c gives

$$bc = (mc)a$$

which gives $a \mid bc$, for all integers c (whether or not $c = 0$).

- (3) Since $a \mid b$ and $b \mid c$, there exists integers m and n such that

$$b = ma, \quad c = nb.$$

Thus, $c = (mn)a$. Since mn is an integer the result follows.

Theorem 1.2.2 (Division algorithm). For any integer a and any positive integer b , there exist unique integers q and r such that

$$a = bq + r, \quad 0 \leq r < b, \tag{1.41}$$

where a is called the *dividend*, q the *quotient*, and r the *remainder*. If $b \nmid a$, then r satisfies the stronger inequalities $0 < r < a$.

Example 1.2.3. Let $b = 15$. Then

- (1) when $a = 255$, $a = b \cdot 17 + 0$, so $q = 17$ and $r = 0 < 15$.
- (2) when $a = 177$, $a = b \cdot 11 + 12$, so $q = 11$ and $r = 12 < 15$.
- (3) when $a = -783$, $a = b \cdot (-52) + 3$, so $q = -52$ and $r = 3 < 15$.

Definition 1.2.3. Consider the following equation

$$a = 2q + r, \quad a, q, r \in \mathbb{Z}, \quad 0 \leq r < q.$$

Then if $r = 0$, then a is *even*, whereas if $r = 1$, then a is *odd*.

Definition 1.2.4. A positive integer n greater than 1 is called *prime* if its only divisors are n and 1. A positive integer n that is greater than 1 and is not prime is called *composite*.

Example 1.2.4. The integer 23 is prime since its only divisors are 1 and 23, whereas 22 is composite since it is divisible by 2 and 11.

Definition 1.6.1. Let a be an integer and n a positive integer greater than 1. We define " $a \bmod n$ " to be the remainder r when a is divided by n , that is

$$r = a \bmod n = a - \lfloor a/n \rfloor n. \quad (1.219)$$

We may also say that " r is equal to a reduced modulo n ".

Remark 1.6.1. It follows from the above definition that $a \bmod n$ is the integer r such that $a = \lfloor a/n \rfloor n + r$ and $0 \leq r < n$, which was known to the ancient Greeks and Chinese some 2000 years ago.

Definition 1.6.2. Let a and b be integers and n a positive integer. We say that " a is congruent to b modulo n ", denoted by

$$a \equiv b \pmod{n} \quad (1.220)$$

if n is a divisor of $a - b$, or equivalently, if $n \mid (a - b)$. Similarly, we write

$$a \not\equiv b \pmod{n} \quad (1.221)$$

if a is not congruent (or incongruent) to b modulo n , or equivalently, if $n \nmid (a - b)$. Clearly, for $a \equiv b \pmod{n}$ (resp. $a \not\equiv b \pmod{n}$), we can write $a = kn + b$ (resp. $a \neq kn + b$) for some integer k . The integer n is called the *modulus*.

Clearly,

$$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid (a - b) \\ &\iff a = kn + b, \quad k \in \mathbb{Z} \end{aligned}$$

and

$$\begin{aligned} a \not\equiv b \pmod{n} &\iff n \nmid (a - b) \\ &\iff a \neq kn + b, \quad k \in \mathbb{Z} \end{aligned}$$

Definition 1.6.3. If $a \equiv b \pmod{n}$, then b is called a *residue* of a modulo n . If $0 \leq b \leq n-1$, b is called the *least nonnegative residue* of a modulo n .

Remark 1.6.2. It is common, particularly in computer programs, to denote the least nonnegative residue of a modulo n by $a \bmod n$. Thus, $a \equiv b \pmod{n}$ if and only if $a \bmod n = b \bmod n$, and, of course, $a \not\equiv b \pmod{n}$ if and only if $a \bmod n \neq b \bmod n$.

Example 1.6.2. The following are some examples of congruences or incongruences.

$$\begin{array}{lll} 35 \equiv 11 \pmod{12} & \text{since} & 12 \mid (35 - 11) \\ \not\equiv 12 \pmod{11} & \text{since} & 11 \nmid (35 - 12) \\ \equiv 2 \pmod{11} & \text{since} & 11 \mid (35 - 2) \end{array}$$

The congruence relation has many properties in common with the equality relation. For example, we know from high-school mathematics that equality is

- (1) reflexive: $a = a, \forall a \in \mathbb{Z}$;
- (2) symmetric: if $a = b$, then $b = a, \forall a, b \in \mathbb{Z}$;
- (3) transitive: if $a = b$ and $b = c$, then $a = c, \forall a, b, c \in \mathbb{Z}$.

We shall see that congruence modulo n has the same properties:

Theorem 1.6.1. Let n be a positive integer. Then the congruence modulo n is

- (1) reflexive: $a \equiv a \pmod{n}, \forall a \in \mathbb{Z}$;
- (2) symmetric: if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}, \forall a, b \in \mathbb{Z}$;
- (3) transitive: if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}, \forall a, b, c \in \mathbb{Z}$.

Proof.

- (1) For any integer a , we have $a = 0 \cdot n + a$, hence $a \equiv a \pmod{n}$.
- (2) For any integers a and b , if $a \equiv b \pmod{n}$, then $a = kn + b$ for some integer k . Hence $b = a - kn = (-k)n + a$, which implies $b \equiv a \pmod{n}$, since $-k$ is an integer.
- (3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a = k_1n + b$ and $b = k_2n + c$. Thus, we can get

$$a = k_1n + k_2n + c = (k_1 + k_2)n + c = k'n + c$$

which implies $a \equiv c \pmod{n}$, since k' is an integer. □

Theorem 1.6.1 shows that the congruence modulo n is an equivalence relation on the set of integers \mathbb{Z} . But note that the divisibility relation $a \mid b$ is reflexive, and transitive but not symmetric; in fact if $a \mid b$ and $b \mid a$ then $a = b$, so it is not an equivalence relation. The congruence relation modulo n partitions \mathbb{Z} into n *equivalence classes*. In number theory, we call these classes *congruence classes*, or *residue classes*. More formally, we have:

Definition 1.6.4. If $x \equiv a \pmod{n}$, then a is called a *residue* of x modulo n . The *residue class* of a modulo n , denoted by $[a]_n$ (or just $[a]$ if no confusion will be caused), is the set of all those integers that are congruent to a modulo n . That is,

$$\begin{aligned}
[a]_n &= \{x : x \in \mathbb{Z} \text{ and } x \equiv a \pmod{n}\} \\
&= \{a + kn : k \in \mathbb{Z}\}.
\end{aligned}
\tag{1.222}$$

Note that writing $a \in [b]_n$ is the same as writing $a \equiv b \pmod{n}$.

Example 1.6.3. Let $n = 5$. Then there are five residue classes, modulo 5, namely the sets:

$$\begin{aligned}
[0]_5 &= \{\dots, -15, -10, -5, 0, 5, 10, 15, 20, \dots\}, \\
[1]_5 &= \{\dots, -14, -9, -4, 1, 6, 11, 16, 21, \dots\}, \\
[2]_5 &= \{\dots, -13, -8, -3, 2, 7, 12, 17, 22, \dots\}, \\
[3]_5 &= \{\dots, -12, -7, -2, 3, 8, 13, 18, 23, \dots\}, \\
[4]_5 &= \{\dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots\}.
\end{aligned}$$

The first set contains all those integers congruent to 0 modulo 5, the second set contains all those congruent to 1 modulo 5, \dots , and the fifth (i.e., the last) set contains all those congruent to 4 modulo 5. So, for example, the residue class $[2]_5$ can be represented by any one of the elements in the set

$$\{\dots, -13, -8, -3, 2, 7, 12, 17, 22, \dots\}.$$

Clearly, there are infinitely many elements in the set $[2]_5$.

Example 1.6.4. In residue classes modulo 2, $[0]_2$ is the set of all even integers, and $[1]_2$ is the set of all odd integers:

$$\begin{aligned}
[0]_2 &= \{\dots, -6, -4, -2, 0, 2, 4, 6, 8, \dots\}, \\
[1]_2 &= \{\dots, -5, -3, -1, 1, 3, 5, 7, 9, \dots\}.
\end{aligned}$$

Example 1.6.5. In congruence modulo 5, we have

$$\begin{aligned}
[9]_5 &= \{9 + 5k : k \in \mathbb{Z}\} = \{9, 9 \pm 5, 9 \pm 10, 9 \pm 15, \dots\} \\
&= \{\dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots\}.
\end{aligned}$$

We also have

$$\begin{aligned}
[4]_5 &= \{4 + 5k : k \in \mathbb{Z}\} = \{4, 4 \pm 5, 4 \pm 10, 4 \pm 15, \dots\} \\
&= \{\dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots\}.
\end{aligned}$$

So, clearly, $[4]_5 = [9]_5$.

Definition 1.6.5. If $x \equiv a \pmod{n}$ and $0 \leq a \leq n - 1$, then a is called the *least (nonnegative) residue* of x modulo n .

Example 1.6.6. Let $n = 7$. There are seven residue classes, modulo 7. In each of these seven residue classes, there is exactly one least residue of x modulo 7. So, the complete set of all least residues x modulo 7 is $\{0, 1, 2, 3, 4, 5, 6\}$.

$\mathbb{Z}/n\mathbb{Z}$ also denoted by \mathbb{Z}_n , residue classes modulo n ;
a ring of integers; a field if n is prime

The finite set $\mathbb{Z}/n\mathbb{Z}$ is closely related to the infinite set \mathbb{Z} . So, it is natural to ask if it is possible to define addition and multiplication in $\mathbb{Z}/n\mathbb{Z}$ and do some reasonable kind of arithmetic there. Surprisingly, addition, subtraction and multiplication in $\mathbb{Z}/n\mathbb{Z}$ will be much the same as that in \mathbb{Z} . Let us first investigate some elementary arithmetic properties of congruences.

Theorem 1.6.5. For all $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

- (1) $a \pm b \equiv c \pm d \pmod{n}$,
- (2) $a \cdot b \equiv c \cdot d \pmod{n}$,
- (3) $a^m \equiv b^m \pmod{n}$, $\forall m \in \mathbb{N}$.

Theorem 1.6.5 is equivalent to the following theorem, since

$$\begin{aligned} a \equiv b \pmod{n} &\iff a \bmod n = b \bmod n, \\ a \bmod n &\iff [a]_n, \\ b \bmod n &\iff [b]_n. \end{aligned}$$

Theorem 1.6.6. For all $a, b, c, d \in \mathbb{Z}$, if $[a]_n = [b]_n$, $[c]_n = [d]_n$, then

- (1) $[a \pm b]_n = [c \pm d]_n$,
- (2) $[a \cdot b]_n = [c \cdot d]_n$,
- (3) $[a^m]_n = [b^m]_n$, $\forall m \in \mathbb{N}$.

The fact that the congruence relation modulo n is stable for addition (subtraction) and multiplication means that we can define binary operations, again called addition (subtraction) and multiplication on the set of $\mathbb{Z}/n\mathbb{Z}$ of equivalence classes modulo n as follows (in case only one n is being discussed, we can simply write $[x]$ for the class $[x]_n$):

$$\begin{aligned} [a]_n + [b]_n &= [a + b]_n \\ [a]_n - [b]_n &= [a - b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n \end{aligned}$$

Example 1.6.11. Let $n = 12$, then

$$\begin{aligned} [7]_{12} +_{12} [8]_{12} &= [7 + 8]_{12} = [15]_{12} = [3]_{12}, \\ [7]_{12} -_{12} [8]_{12} &= [7 - 8]_{12} = [-1]_{12} = [11]_{12}, \\ [7]_{12} \cdot_{12} [8]_{12} &= [7 \cdot 8]_{12} = [56]_{12} = [8]_{12}. \end{aligned}$$

In many cases, we may still prefer to write the above operations as follows:

$$\begin{aligned} 7 + 8 &= 15 \equiv 3 \pmod{12}, \\ 7 - 8 &= -1 \equiv 11 \pmod{12}, \\ 7 \cdot 8 &= 56 \equiv 8 \pmod{12} \end{aligned}$$

We summarise the properties of addition and multiplication modulo n in the following two theorems.

Theorem 1.6.7. The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n has the following properties with respect to addition:

- (1) Closure: $[x] + [y] \in \mathbb{Z}/n\mathbb{Z}$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
- (2) Associative: $([x] + [y]) + [z] = [x] + ([y] + [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.
- (3) Commutative: $[x] + [y] = [y] + [x]$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
- (4) Identity, namely, $[0]$.
- (5) Additive inverse: $-[x] = [-x]$, for all $[x] \in \mathbb{Z}/n\mathbb{Z}$.

Theorem 1.6.8. The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n has the following properties with respect to multiplication:

- (1) Closure: $[x] \cdot [y] \in \mathbb{Z}/n\mathbb{Z}$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
- (2) Associative: $([x] \cdot [y]) \cdot [z] = [x] \cdot ([y] \cdot [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.
- (3) Commutative: $[x] \cdot [y] = [y] \cdot [x]$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
- (4) Identity, namely, $[1]$.
- (5) Distributivity of multiplication over addition: $[x] \cdot ([y] + [z]) = ([x] \cdot [y]) + ([x] \cdot [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.

Definition 1.6.10. Two integers x and y are said to be multiplicative inverses if

$$xy \equiv 1 \pmod{n}, \quad (1.228)$$

where n is a positive integer greater than 1.

Summary

In this week, we learned about the divisibility of two numbers and the congruence between two numbers.