BIT

8: Modular Arithmetic

EN1106 - Introductory Mathematics

Level I - Semester 1

UCSC

8.1 Introduction to Modular Arithmetic

Congruences

Following are some frequently used notations.

$\mathbb{R}$ - the set of all real numbers

$\mathbb{Z}$ - the set of all integers

$\mathbb{N}$ - the set of all positive integers

$a|b, a \neq 0$ - a divides b *or* b is divisible by b

$a \nmid b, a \neq 0$ - a does not divide b *or* b is not divisible by a

- **Definition 1:** Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that a divides b *or* that b is divisible by a, denoted by $a|b$, if there exists $c \in \mathbb{Z}$ such that $b = ca$. If no such exists, then we say that a does not divide b *or* b is not divisible by a.

- **Definition 2:** Let n be a fixed positive integer and let $a, b \in \mathbb{Z}$. We write a≡b(mod n) (read: a is congruent to b modulo n or a is congruent to b mod n) if a-b is divisible by n. If n does not divide a-b, then we write a≢b(mod n). In this case we say that a and b are incongruent modulo n. The integer n is called the modulus of the congruence a≡b(mod n).

For example,

- $17 \equiv 1 (\text{mod } 4)$, because $17-1=16$ is divisible by 4.
- Also, $-21 \equiv -3 (\text{mod } 6)$, because $-21-(-3)=-18$ is divisible by 6.
- However $20 \not\equiv 3 (\text{mod } 5)$, because $20-3=17$ is not divisible by 5.

Remark: Observe that $a \equiv b (\text{mod } n)$ if and only if both a and b leave the same remainder upon division by n (How?).

Let $n \in N$ be fixed. For any $a, b, c \in Z$, following three properties are hold by congruence modulo n.

I. $a \equiv a \pmod{n}$

II. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

III. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

The reader is encouraged to prove above properties.

Now, for a fixed positive integer n, consider the following sets.

$E_0=\{0+kn, \text{ where } k \in Z\}=\{0, 0 \pm n, 0 \pm 2n, 0 \pm 3n, \ldots\}$,

$E_1=\{1+kn, \text{ where } k \in Z\}=\{1, 1 \pm n, 1 \pm 2n, 1 \pm 3n, \ldots\}$,

$\vdots$

$E_{(n-1)}=\{(n-1)+kn, \text{ where } k \in Z\}=\{(n-1), (n-1) \pm n, (n-1) \pm 2n, (n-1) \pm 3n, \ldots\}$.

- Observe that for each $r, 0 \leq r \leq n-1$, E_r consists of all the integers which leaves r as the remainder when divided by n.
- In other words, E_r consists of the integers which differ from r by an integral multiple of n.
- The second and third properties (II and III) above imply that $E_0, E_1, \ldots, E_{n-1}$ are mutually disjoint sets.
- Moreover, by division algorithm any integer x can be written *uniquely* in the form $x = pn + r$, where $p \in \mathbb{Z}$ and $0 \leq r \leq n-1$.

- Hence, $x \equiv r \pmod{n}$.
- Therefore, every integer is congruent modulo n to one of the integers 0, 1, 2, …, n-1. Hence, any integer x falls into exactly one of these n sets.
- Thus the set of all integers, i.e. Z, is divided into exactly n disjoint sets (called congruence classes modulo n), each containing integers that are mutually congruent modulo n.
- These sets are determined by the possible remainders after division by n, namely 0,1,2,…,n-1.

When $n = 2$, the set of integers is divided into the two disjoint sets known as the set of odd integers and the set of even integers.

If $n = 3$, then there are three congruence classes modulo 3 namely,

$$
\begin{aligned}
E_0 &= \{ \quad \ldots, \quad -9, \quad -6, \quad -3, \quad 0, \quad 3, \quad 6, \quad 9, \quad \ldots \quad \} \\
E_1 &= \{ \quad \ldots, \quad -8, \quad -5, \quad -2, \quad 1, \quad 4, \quad 7, \quad 10, \quad \ldots \quad \} \\
E_2 &= \{ \quad \ldots, \quad -7, \quad -4, \quad -1, \quad 2, \quad 5, \quad 8, \quad 11, \quad \ldots \quad \}
\end{aligned}
$$

Observe that $E_0 \cup E_1 \cup E_2 = \mathbb{Z}$

- Note that for different n's we get different congruence classes.
- For example, if $n = 3$, then both 4 and 7 falls into E_1-the set consisting of all those integers which leaves 1 as the remainder upon division by 3.

- But, if $n = 5$, then 4 belongs to E_4 - the set consisting of all those integers which leaves 4 as the remainder upon division by 5 and 7 belongs to E_2 - the set consisting of all those integers which leaves 2 as the remainder upon division by 5.
- Obviously the sets E_2 and E_4 are disjoint.
- So, we shall always be careful to fix n.

8.2 Rules of Modular Arithmetic (Addition, Subtraction and Multiplication)

Modular Arithmetic

- We will often do arithmetic with congruences, which is called *modular arithmetic.*
- Congruences have many of the same properties that equalities do.
- The following list gives several important rules that can be used when working with congruences.
- The first two of these are similar to the corresponding rules for equalities.

Properties of Addition, Subtraction and multiplication of Modular Arithmetic

- Let n be a fixed positive integer.

1. Let a, b, c $\in$ Z. Suppose $a \equiv b \pmod{n}$. Then,

    1.1 $(a + c) \equiv (b + c) \pmod{n}$

    1.2 $(a - c) \equiv (b - c) \pmod{n}$

    1.3 $(ac) \equiv (bc) \pmod{n}$

Check with the definition!

Example 1:

Because $15 \equiv 3(\text{mod } 6)$ it follows that

- $20 = (15 + 5) \equiv (3 + 5) = 8(\text{mod } 6)$
- $7 = (15 - 8) \equiv (3 - 8) = -5(\text{mod } 6)$
- $45 = (15 \cdot 3) \equiv (3 \cdot 3) = 9(\text{mod } 6).$

Properties of Addition, Subtraction and multiplication of Modular Arithmetic

2. Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$.

   Suppose $a_1 \equiv b_1 (\mathrm{mod}\, n)$ and $a_2 \equiv b_2 (\mathrm{mod}\, n)$.

   Then,

   2.1. $(a_1 + a_2) \equiv (b_1 + b_2) (\mathrm{mod}\, n)$
   2.2. $(a_1 - a_2) \equiv (b_1 - b_2) (\mathrm{mod}\, n)$
   2.3. $(a_1 \cdot a_2) \equiv (b_1 \cdot b_2) (\mathrm{mod}\, n)$

Example 2:

Because $19 \equiv 1 (\text{mod } 9)$ and $5 \equiv -4 (\text{mod } 9)$,

it follows that,

- $24 = (19 + 5) \equiv (1 + (-4)) = -3 (\text{mod } 9)$,
- $14 = (19 - 5) \equiv (1 - (-4)) = 5 (\text{mod } 9)$
- $95 = (19 \cdot 5) \equiv (1 \cdot (-4)) = -4 (\text{mod} 9)$.

- It is seen that multiplying both sides of a congruence by the same integer preserves the congruence (Property 1.3).
- Will it be the same if both sides of a congruence are divided by the same integer?

Example 3:

It is clear that $65 = (13 \cdot 5) \equiv (1 \cdot 5) = 5 (\mathrm{mod} 10)$.

However, it is not true that $13 \equiv 1 (\mathrm{mod}\ 10)$.

- So, in general, it is not true that division of both sides of a congruence by the same integer preserves the *congruence*.
- The next property gives a valid congruence when both sides of a congruence are divided by the same integer.

8.3 Properties of Modular Arithmetic

Properties of Modular Arithmetic

3. Let $a, b, c \in \mathbb{Z}$. Suppose $(ac) \equiv (bc)(\text{mod } n)$. Then,

   3.1. $a \equiv b(\text{mod } n)$ if $\gcd(c, n) = 1$

   3.2. $a \equiv b(\text{mod } \frac{n}{d})$ if $\gcd(c, n) = d$, where $d > 1$.

- Recall that for any two integers x and y, which are not both 0, $\gcd(x, y)$ denotes the greatest common divisor of x and y (obviously $\gcd(x, y) > 0$)

Example 4:

- Because $18=(6\cdot3)\equiv(1\cdot3)=3(\text{mod } 5)$ and $\gcd(3,5)=1$, it follows that $6\equiv1(\text{mod } 5)$.

- Also, because $65=(13\cdot5)\equiv(1\cdot5)=5(\text{mod } 10)$ and $\gcd(5,10)=5$, it follows that $13\equiv1(\text{mod } 10/5)$ or equivalently $13\equiv1(\text{mod } 2)$.

Properties of Modular Arithmetic

4. Fermat's Little Theorem:

Let $a \in \mathbb{Z}$ and let p be a prime number. Then,

4.1. $a^p \equiv a \pmod{p}$

4.2. $a^{p-1} \equiv 1 \pmod{p}$ if p does not divide a.

- The above rules can be used to reduce a congruence and solve congruence equations.

- Suppose it is required to find the remainder that results when 5^{10} is divided by 7.
- Of course it is possible to compute 5^{10} first and then divide it by 7 to get the remainder. But, this procedure becomes tedious when relatively large numbers are involved.
- However, the knowledge of congruences can be used to tackle this kind of problems easily.

- Observe that, we need to find the integer x, $0 \leq x < 7$, such that $5^{10} \equiv x \pmod 7$.
- Notice that $5 \equiv -2 \pmod 7$.
- Repeated application of property 2.3 ,

  (10 times) yields, $5^{10} \equiv (-2)^{10} = (-1)^{10} 2^{10} \pmod 7 = 2^{10} \pmod 7$.
- Now, $2^3 \equiv 1 \pmod 7$.
- By applying the same property again we get $2^9 = (2^3)^3 \equiv 1^3 = 1 \pmod 7$.
- Now, multiplying both sides of the congruence $2^9 \equiv 1 \pmod 7$ by 2 gives $2^{10} \equiv 2 \pmod 7$.
- Since $5^{10} \equiv 2^{10} \pmod 7$ and $2^{10} \equiv 2 \pmod 7$ it follows that $5^{10} \equiv 2 \pmod 7$.
- Therefore, the remainder that results when 5^{10} is divided by 7 is 2
- **Remark**: If $a \equiv b \pmod n$, then for each positive integer k, $a^k \equiv b^k \pmod n$ (how?).

Example 5: what is the remainder when 2^{2020} is divided by 41?

Solution:

- Notice first that 41 is a prime number and 41 does not divide 2.
- Thus by Fermat's Little theorem, $2^{40}=2^{(41-1)}\equiv 1 \pmod{41}$.
- Since $2^{2020}=(2^{40})^{50}\cdot 2^{20}$ it follows that $2^{2020}\equiv 2^{20} \pmod{41}$.
- Since $2^5\equiv -9 \pmod{41}$, we have $2^{20}\equiv 9^4 \pmod{41}$.
- Finally, $9^4 \equiv 1 \pmod{41}$, because $9^2 \equiv -1 \pmod{41}$.
- Hence $2^{20} \equiv 1 \pmod{41}$.
- Therefore, $2^{2020} \equiv 1 \pmod{41}$.
- So, the remainder is 1.

The Congruence Equation $ax \equiv b \pmod{n}$

Definition 3:

- A congruence of the form $ax \equiv b \pmod{n}$, where x is an unknown integer, is called a linear congruence in one variable.

Suppose it has been given that $ax = b$, where a and b are real numbers with a≠0.

Then the value of x which satisfies this equation is $\frac{b}{a}$

Solving a congruence equation like $ax \equiv b \pmod{n}$is not that easy.

It is required to find an integer x such that ax-b is divisible by n

- The necessary and sufficient condition for the congruence equation $ax \equiv b(\text{mod } n)$ to have a solution is that gcd(a, n)divides b.
- If it does have a solution, then there are infinitely many solutions congruent modulo n.

- For example,
    - suppose we need to solve the congruence 2x≡3(mod 6).
    - Does there exist an integer x which satisfies the congruence 2x≡3(mod 6)?
    - If such an x does exist, then 2x-3=6y for some integer y.
    - This implies that 3 is an even number, which is a contradiction.
    - So, no such x exists.
    - Notice that gcd(2,6)=2 does not divide 3.

Properties of Modular Arithmetic

5. The linear congruence equation $ax \equiv b (\text{mod } n)$ has a solution if and only if $d = \gcd(a,n)$ divides b.

   If $ax \equiv b (\text{mod } n)$ has solutions, then there are two methods for solving the congruence equation $ax \equiv b (\text{mod } n)$.

- One method is to solve the Diophantine equation obtained from the given congruence equation.
- However, we will not discuss this method here.
- The other method is to use the rules for congruences given above.

Example 6: Solve $18x \equiv 5 (\text{mod } 7)$.

Solution:

Notice that $\gcd(18, 7) = 1$ and 1 divides 5.

Since $0 \equiv 7(\text{mod } 7)$, we get $18x = (18x + 0) \equiv (5+7) = 12(\text{mod } 7)$.

Now, since $\gcd(6,7)=1$ this implies $3x \equiv 2(\text{mod } 7)$.

Again, as before, $3x=(3x+0) \equiv (2+7)=9(\text{mod } 7)$.

Dividing both sides of this congruence by 3 gives $x \equiv 3(\text{mod } 7)$.

So, any integer x which leaves 3 upon division by 7 would satisfy the given congruence equation.

In other words if $x=3+7k$, where k is an integer, then $18x$ will leave a remainder of 5 when divided by 7 (check for example $x=3,-4,10$).

Example 7:

Solve $9x\equiv12 \pmod{15}$.

Solution: Observe that $3=\gcd(9,15)$ divides 12.

Thus, the given congruence equation has solutions.

Notice that x_0 is a solution of $9x\equiv12 \pmod{15}$ if and only if x_0 is a solution of $3x\equiv4 \pmod 5$ (Property 3.2).

For if $9x_0 \equiv 12 \pmod{15}$, then there exists $y_0 \in Z$ such that $9x_0=12+15y_0$.

Thus, $3x_0=4+5y_0$. That is $3x_0 \equiv 4 \pmod{5}$.

On the other hand if x_0 satisfies $3x \equiv 4 \pmod{5}$, then there exists $y' \in Z$ such that $3x_0=4+5y'$.

Multiplying the equation by 3 gives $9x_0=12+15y'$.

Thus $9x_0 \equiv 12 \pmod{15}$.

Now consider the congruence $3x \equiv 4 \pmod{5}$.

Clearly this congruence has solutions because gcd(3,5) divides 4.

Notice that $2 \equiv -3 \pmod{5}$.

Therefore $6x=(3x)\cdot 2 \equiv 4\cdot(-3)=-12 \pmod{5}$.

- Dividing both sides of the congruence by 6 gives $x \equiv -2 \pmod 5$ or equivalently $x \equiv 3 \pmod 5$ (why?).
- Therefore, any integer x of the form $x=3+5k$, where $k \in Z$, will satisfy the congruence $3x \equiv 4 \pmod 5$ and hence the congruence $9x \equiv 12 \pmod{15}$.
- Now, suppose we need to write x in the form of $15p+r$, where $p \in Z$ and r is a possible remainder after division by 15, i. e. r is an element of the set $\{0,1,2,\ldots,13,14\}$.
- It is clear that $k=3k'+0$ or $k=3k'+1$ or $k=3k'+2$, where $k' \in Z$ (recall the discussion at the beginning about partitioning Z into disjoint sets known as congruence classes modulo n).

- Hence, $x=3+5(3k'+0)=3+15k'$ or $x=3+5(3k'+1)=8+15k'$ or $x=3+5(3k'+2)=13+15k'$.
- Therefore, any integer x in any one of the disjoint sets $\{3+15k', \text{where } k' \in Z\}$, $\{8+15k', \text{where } k' \in Z\}$ and $\{13+15k', \text{where } k' \in Z\}$ will satisfy the congruence $9x \equiv 12 \pmod{15}$.

- **Remark**: Unlike the previous example, in this example there are three disjoint sets (congruence classes modulo 15) from which x can take values.
- Actually the number of such sets is equal to gcd(a,n).
- Following theorem summarizes this fact.

Theorem 1:

Let a, b, $n \in Z$ be such that $n>0$ and $\gcd(a, n)=d$. If $d|b$, then $ax \equiv b \pmod{n}$ has exactly d incongruent solutions modulo n.

Modular Inverses

- Now consider the linear congruence $ax \equiv 1 \pmod{n}$.
- As you know this congruence has a solution if and only if $\gcd(a,n)=1$.

Definition 4:

- Let a be an integer and let n be a fixed positive integer such that $\gcd(a,n)=1$. An integer solution x of $ax \equiv 1 \pmod{n}$ is called an inverse of a modulo n.

- **Example 8:**

  Find an inverse of 13 modulo 17.

Solution:

- We need to find an x such that $13x \equiv 1 \pmod{17}$.
- Clearly such an x exists because $\gcd(13,17)=1$.
- Suppose x_0 satisfies the congruence $13x \equiv 1 \pmod{17}$.
- Then $13x_0 \equiv 1 \pmod{17}$.
- Notice that $1 \equiv 52 \pmod{17}$.
- Thus, $13x_0 \equiv 52 \pmod{17}$.
- Dividing both sides of the congruence by 13 yields $x_0 \equiv 4 \pmod{17}$.

- Therefore, any integer x of the form $x=4+17k$, where k is an integer, will be an inverse of 13 modulo 17.
- For example,

  if $x=4$, then $13\cdot 4=52\equiv 1 \pmod{17}$;

  if $x=21$, then $13\cdot 21=273\equiv 1 \pmod{17}$;

  if $x=-13$, then $13\cdot(-13)=-169\equiv 1 \pmod{17}$ and so on.