

Discrete Mathematics

Lecture 5

Linear Congruence

Lecturer: Kahenya, N.P



Introduction to lecture 5



Lecture 5 is a continuation of lecture 4 on *Introduction to Number theory*.



This lecture will introduce key concepts in linear congruence.



Linear congruence is applicable in such areas as hashing functions, pseudorandom numbers, and parity check digits.

A pair of black-rimmed glasses is resting on a stack of books. The top book has a red bookmark. The background is blurred, showing more books and a wooden surface.

References

These lecture notes have been derived from the following sources, Susanna (2003), Rosen (2011), and Rosen (2012).

Intended learning outcomes

Be	At the end of this lecture, you will be able to;
Define	Define linear congruence.
Solve	Solve linear congruence problems.
Determine	Determine the multiplicative inverse modulo.

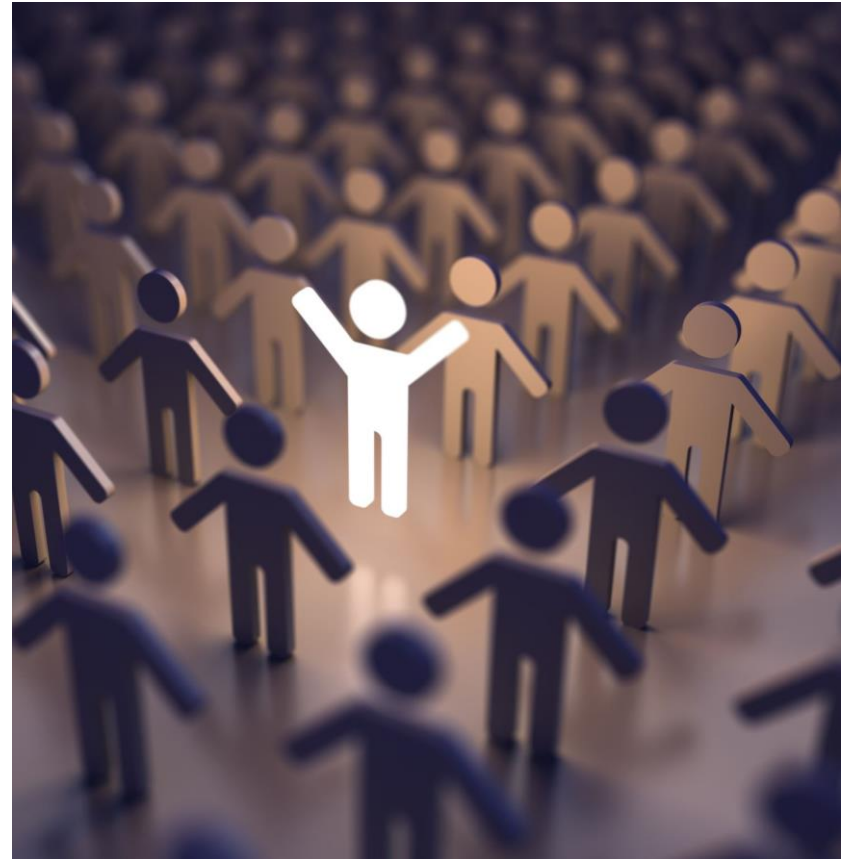
Definition of terms

- A congruence of the form $ax \equiv b \pmod{m}$ where m is a positive integer, a and b are integers is called a linear congruence.
- The solutions to a linear congruence $ax \equiv b \pmod{m}$ are the integers x that satisfy the congruence.



Inverse

- ❑ An integer \bar{x} such that $\bar{x}x = 1 \pmod{m}$ is said to be the inverse of x modulo m .
- ❑ The inverse of an integer modulo m may not exist.
- ❑ If m is a prime number, then all non-zero integers modulo m have an inverse.
- ❑ However, if m is a composite number, then all non-zero integers that are relatively prime to m have an inverse.
- ❑ The inverse of a is unique.
- ❑ Any other inverse of $a \pmod{b}$ is congruent to $\bar{a} \pmod{b}$



Theorem

If a and b are relatively prime and $b > 1$ then an inverse of $a \pmod{b}$ exists.

Proof: Since the $\gcd(a, b) = 1$ then by Bezout's theorem there exists integers s and t such that $sa + tb \equiv 1 \pmod{b}$ (i)

Working out mod b in equation (i) we have

$$sa \pmod{b} + tb \pmod{b} \equiv 1 \pmod{b}$$

$$sa \equiv 1 \pmod{b}$$

This means that s is an inverse of $a \pmod{b}$



Finding the multiplicative inverses \mathbb{Z}_m

In this lecture we shall review the following methods of determining the multiplicative inverse of integers modulo m .

- Using Cayley table.
 - Euclidean algorithm and Bezout's identity.
-

Inverse using Cayley table

Find the inverse 2 modulo 11

Solution: Note that

$$Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}.$$

Next, we generate the Cayley table.

From the table the inverse of 2 i.e., $2^{-1} = 6$.

Also $1^{-1} = 1$; $3^{-1} = 4$ and $7^{-1} = 8$ and so on.

\times_{11}	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Alternatively

Let x be the inverse of 2 then we have $2x = 1 \pmod{11}$.

Then (applying the Euclidean algorithm) we have;

$$11 \equiv 2 \cdot 5 + 1$$

$$\Rightarrow 1 = 11 - 5(2)$$

Next, we introduce modulo 11 to get;

$$11 \pmod{11} + (-5)(2) \pmod{11} = 1 \pmod{11}$$

$$(11 - 5)(2) \pmod{11} = 1 \pmod{11}$$

$$(6 \cdot 2) \pmod{11} = 1 \pmod{11}$$

$$\Rightarrow x = 2^{-1} = 6$$

Example 1



Determine the inverse of the following; $18 \pmod{306}$

Solution: Let x be the inverse of 18 modulo 306 then; $18x = 1 \pmod{306}$.

Applying the Euclidean algorithm to get;

$$306 = 17 \cdot 18 + 0$$

\Rightarrow 18 is a factor of 306 and hence it has no inverse modulo 306.

Remark: If given two integers a and b with $b > 1$, and the $\gcd(a, b) \neq 1$ then the inverse a modulo b does not exist.

Example 2

Determine the inverse of the following; $129 \pmod{1137}$

Solution: Let x be such that $129x = 1 \pmod{1137}$.

Next, we find the gcd i.e.

$$1137 = 129 \cdot 8 + 105$$

$$129 = 105 \cdot 1 + 24$$

$$105 = 24 \cdot 4 + 9$$

$$24 = 9 \cdot 2 + 6$$

$$9 = 6 \cdot 1 + 3$$

$$6 = 3 \cdot 2 + 0$$

The gcd is 3 \Rightarrow 129 has no multiplicative inverse mod 1137

Example 3

Determine the inverse of the following; $19 \pmod{51}$

Solving linear congruences

We need to introduce another parameter t such that $11t = 1 \pmod{31} \dots (i)$.

Next, we introduce t in our congruence to get; $11xt = 3t \pmod{31}$

$$\Rightarrow x = 3t \pmod{31} \dots (ii)$$

Next, we apply the Euclidean algorithm so that we can express the gcd of 31 and 11 as a linear combination of 31 and 11.

From equation (i) we know the gcd is 1.

Contd...

Thus, we have

$$31 = 11 \cdot 2 + 9$$

$$11 = 9 \cdot 1 + 2$$

$$9 = 2 \cdot 4 + 1$$

$$\begin{aligned} \therefore 1 &= 9 - 4(2) = 9 - 4[11 - 1(9)] = 5(9) - 4(11) = 5[31 - 2(11)] - 4(11) \\ &= 5(31) - 14(11) \end{aligned}$$

$$\Rightarrow 1 = 5(31) + (-14)(11) \dots \text{(iii)}$$

We introduce mod 31 to equation (iii) to get;

Contd...

$$\Rightarrow (-14)(11) = 1 \pmod{31}$$

$$(31 - 14)(11) = 1 \pmod{31}$$

$$17 \cdot 11 = 1 \pmod{31}$$

$$\Rightarrow t = 17$$

Replacing t with 17 in equation (ii) to get;

$$x = (3 \cdot 17) \pmod{31}$$

$$x = 51 \pmod{31}$$

$$x = 20$$

Example 4

Solve the following linear congruence; $11x \equiv 2 \pmod{23}$

Solution: We introduce another parameter t such that

$$11t = 1 \pmod{23} \dots (i)$$

$$\text{Then } 11xt = 2t \pmod{23}$$

$$\text{Hence, we can say that; } x = 2t \pmod{23} \dots (ii)$$

From (i) we can see that the 11 and 23 are relatively prime and hence $11t + 23s = 1$

Example 4...contd...

Then;

$$23 = 2 \cdot 11 + 1$$

$$1 = 23 - 2 \cdot 11$$

$$1 = 23 + 11(-2) \cdots \text{(iii)}$$

Introducing mod 23 in equation (iii) we get

$$1 \bmod 23 = 23 \bmod 23 + 11(-2) \bmod 23$$

$$\Rightarrow (-2)11 \bmod 23 = 1 \bmod 23$$

$$(23 - 2)(11) \bmod 23 = 21 \cdot 11 \bmod 23 = 1 \bmod 23$$

Comparing the above with equation (i) it is clear that $t = 21$

Thus (ii) becomes; $x = 2 \cdot 21 \bmod 23 = 42 \bmod 23 = 19 \bmod 23$ i.e., $x = 19$

Chinese Remainder Theorem

Let m_1, m_2, \dots, m_n be pairwise relatively prime positive integers greater than and a_1, a_2, \dots, a_n arbitrary integers. Then the system;

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

...

...

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$

i.e., there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.



Example 1

Apply the Chinese remainder theorem (back substitution) to find the solutions to the system of the congruences;

$$x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 4 \pmod{11} \text{ (Rosen, 2012, p. 285).}$$

Solution: From $x \equiv 1 \pmod{2}$ and by the Theorem; *The integers a and b are congruent modulo m if and only if there is an integer k such that $a = km + b$, we have*

$$x = 1 + 2t \cdots \text{(i) for some integer } t.$$

Example 1...contd...

Next, we substitute this for x in the congruence $x \equiv 2 \pmod{3}$ to get

$$1 + 2t \equiv 2 \pmod{3} \cdots \text{(ii)}$$

Discussed in Lecture 4, *If a and b are integers and m is a positive integer, then*

$a \equiv b \pmod{m}$ if $m|(a - b)$ then equation (ii) we can say;

$$3|(1 + 2t) - 2$$

$$3|2t - 1$$

$$\therefore 2t = 1 \pmod{3} \Rightarrow t = 2 \pmod{3}$$

$\Rightarrow t = 2 + 3u \cdots \text{(iii)}$ for some integer u .

Example 1...contd...

Replacing t in equation (i) to get; $x = 1 + 2(2 + 3u) = 1 + 4 + 6u = 5 + 6u$

$$x = 5 + 6u \cdots \text{(iv)}$$

Next, we substitute this for x in the congruence $x \equiv 3 \pmod{5}$ to get;

$$5 + 6u = 3 \pmod{5}$$

$$\Rightarrow 5 \mid (5 + 6u) - 3$$

$$5 \mid 6u + 2 \therefore 6u = -2 \pmod{5} = 3 \pmod{5} \Rightarrow 5 \mid 6u - 3 = 5 \mid 3(2u - 1) \equiv 5 \mid 2u - 1$$

Therefore, we have;

$$2u = 1 \pmod{5} \therefore u = 3 \pmod{5} \Rightarrow u = 3 + 5v \cdots \text{(v)} \text{ for some integer } v.$$

Example 1...contd...

Equation (iv) becomes $x = 5 + 6(3 + 5v) = 5 + 18 + 30v = 23 + 30v$

$$\therefore x = 23 + 30v \dots (\text{vi})$$

Replacing in $x = 4 \pmod{11}$ to get;

$$23 + 30v = 4 \pmod{11}$$

$$\Rightarrow 11 \mid (23 + 30v) - 4$$

$$11 \mid 30v + 19$$

$$\text{but } 30v = -19 \pmod{11} = (11 - 19) \pmod{11} = -8 \pmod{11} = 3 \pmod{11}$$

$$\therefore 30v = 3 \pmod{11}$$

Example 1...contd...

Thus

$$\begin{aligned}11|30v + 19 &\equiv 11|30v - 3 \equiv 11|3(10v - 1) \equiv 11|10v - 1 \therefore 10v = 1 \pmod{11} \\ &\Rightarrow v = 10 \pmod{11}\end{aligned}$$

Therefore $v = 10 + 11w \dots$ (vii) for some integer w .

Equation (vi) will now become $x = 23 + 30(10 + 11w) = 23 + 300 + 330w$

$$\begin{aligned}x &= 323 + 330w \\ &\Rightarrow x \equiv 323 \pmod{330}\end{aligned}$$

All integers of the form $323 + 330w, w \in \mathbb{Z}$ are solutions to our systems of congruences.

Example 2

Apply the Chinese remainder theorem (back substitution) to find the solutions to the system of the congruences;

$x \equiv 2 \pmod{3}$, $x \equiv 4 \pmod{7}$, $x \equiv 6 \pmod{10}$, $x \equiv 11 \pmod{21}$ (Lipschutz & Lipson, 2007, p. 296).

Solution: From $x \equiv 2 \pmod{3}$ we have $x = 3t + 2 \dots$ (i) for some integers t .

Hence $x \equiv 4 \pmod{7}$ becomes $3t + 2 \equiv 4 \pmod{7}$

Example 2...contd...

Which implies then that;

$$7|(3t + 2) - 4$$

$$7|3t - 2 \therefore 3t = 2 \pmod{7} \Rightarrow t = 3 \pmod{7}$$

This can be written as; $t = 7u + 3$ for some integer u .

Therefore equation (i) becomes $x = 3(7u + 3) + 2 = 21u + 11 \dots$ (ii)

Hence, we have equation $x \equiv 6 \pmod{10}$ becomes $21u + 11 \equiv 6 \pmod{10}$

Example 2...contd...

Which implies that;

$$10|(21u + 11) - 6$$

$$10|21u + 5 \Rightarrow 21u = -5 \pmod{10}$$

$$21u = 5 \pmod{10} \therefore u = 5 \pmod{10}$$

Hence, we have; $u = 10v + 5$ for some integer v .

We write equation (ii) as; $x = 21(10v + 5) + 11$

$$x = 210v + 116 \dots \text{(iii)}$$

Example 2...contd...

We write equation (ii) as; $x = 21(10v + 5) + 11$

$$x = 210v + 116 \dots \text{(iii)}$$

Therefore, our last equation $x \equiv 11 \pmod{21}$ becomes;

$$210v + 116 \equiv 11 \pmod{21} \Rightarrow 116 \equiv 11 \pmod{21} \therefore x = 116 \pmod{210}$$

Example 2...contd...

Note that we can still proceed and have;

$$21|(210v + 116) - 11$$

$$21|210v + 105$$

$$21|105(2v + 1)$$

$$21|2v + 1 \therefore 2v \equiv -1 \pmod{21}$$

$$2v \equiv 20 \pmod{21} \therefore v \equiv 10 \pmod{21}$$

Hence $v = 21w + 10$ for some integer w .

Therefore equation (iii) becomes $x = 210(21w + 10) + 116 = 4410w + 2216$

$$\Rightarrow x \equiv 2216 \pmod{4410}$$

Example 3...contd...

□ However, 116 is the smallest positive integer satisfying all the congruences.

□ By Chinese remainder theorem

$$m = m_1 m_2 m_3 m_4 = 3 \times 7 \times 10 \times 21 = 4410$$





References

Lipschutz, S., & Lipson, M. (2007). *Discrete Mathematics*. McGraw-Hill.

Rosen, K. (2011). *Elementary Number Theory and Its Application* (6th ed.). Person.

Rosen, K. (2012). *Discrete mathematics and its application* (7th ed.). McGraw-Hill.

Susanna, S. E. (2003). *Discrete Mathematics with Application* (3rd ed.). Brooks Cole.

<https://www.youtube.com/watch?v=4-HSjLXrfPs>

<https://www.youtube.com/watch?v=pMA-dD-KCWM>