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.

References

These lecture notes have been derived from the following sources, Lipschutz & Lipson (2007) Susanna (2003), Rosen (2011), and Rosen (2012).

Intended learning outcomes

At the end of this lecture, you will be able to;

(i) Define linear congruence.

(ii) Solve linear congruence problems.

(iii) Determine the multiplicative inverse modulo.

Definition of terms

Definition 1: (linear congruence). A congruence of the form $ax \equiv b \ (mod \ m)$ where m is a positive integer, a and b are integers is called a linear congruence.

The solutions to a linear congruence $ax \equiv b \ (mod \ m)$ are the integers x that satisfy the congruence.

Definition 2: An integer $\bar{x}$ such that $\bar{x}x = 1 \ (mod \ m)$ 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 (see lecture 4 for an example).

Example 1: 2 is the inverse of 4 modulo 7 since $2 \cdot 4 \pmod 7 = 1 \pmod 7$

Remark 1: The inverse of *a* is unique. Any other inverse of $a \ (mod\ b)$ is congruent to $\bar{a} \ (mod\ b)$

Remark 2: Two integers a and b are said to be relatively prime if $\gcd(a, b) = 1$.

Theorem 1: If a and b are relatively prime and $b > 1$ then an inverse of $a \ (mod\ b)$ exists.

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

Working out *mod b* in equation (i) we have

$$sa \ (mod\ b) + tb \ (mod\ b) \equiv 1 \ (mod\ b)$$

$$sa \equiv 1 \ (mod\ b)$$

This mean that s is an inverse of $a \ (mod\ b)$

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.

a) Using Cayley table.

b) Euclidean algorithm and Bezout's identity.

Example 1: Find the inverse 2 modulo 11

Solution: (Using the Cayley table). Note that $Z_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$. Next we generate the Cayley table.

$\times_{11}$	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

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.

Alternatively,

Let x be the inverse of 2 then we have $2x = 1 \bmod 11$. Then (applying the Euclidean algorithm) we have;

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

$$=> 1 = 11 - 5(2)$$

Next we introduce modulo 11 to get;

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

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

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

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

Remark: The use of Cayley table is not a viable option more so when dealing with large numbers. Of course, the Cayley table will also consume more space in your machine.

Example 2: Determine the inverse of the following; $18 \bmod 306$

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

Example 3: Determine the inverse of the following; 129 mod 1137

Solution: Let x be such that $129x = 1 \bmod 1137$.

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

$$\Rightarrow 129 \text{ has no multiplicative inverse mod } 1137$$

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 4: Determine the inverse of the following; $19 \bmod 51$

Solution: Let x be the inverse of 19 then; $19x = 1\ mod\ 51$

$$=> 51 = 19 \cdot 2 + 13$$

$$19 = 13 \cdot 1 + 6$$

$$13 = 6 \cdot 2 + 1$$

$$=> 1 = 13 - 2(6) = 13 - 2[19 - 1(13)] = 3(13) - 2(19)$$

$$= 3[51 - 2(19)] - 2(19)$$

$$\therefore 1 = 3(51) - 8(19)$$

$$\therefore (3 \cdot 51) \bmod 51 + (-8 \cdot 19) \bmod 51 = 1 \bmod 51$$

$$(-8 \cdot 19) \bmod 51 = 1 \bmod 51$$

$$(43 \cdot 19\ ) \bmod 51 = 1 \bmod 51$$

$$=> 19^{-1} = 43$$

Solving linear congruences

Example 1: Solve the following linear congruence; $11\text{x} \equiv 3 \bmod 31$

Solution: We need to introduce another parameter t such that $11\text{t} = 1 \bmod 31 \cdots (\text{i})$.

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

$$\Rightarrow\ \text{x} = 3\text{t} \bmod 31 \cdots (\text{ii})$$

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. Thus, we have

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

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

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

$$\therefore 1 = 9 - 4(2) = 9 - 4[11 - 1(9)] = 5(9) - 4(11) = 5[31 - 2(11)] - 4(11)$$

$$= 5(31) - 14(11)$$

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

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

$$1 \bmod 31 = 5(31) \bmod 31 + (-14)(11) \bmod 31$$

$$\Rightarrow (-14)(11) = 1 \bmod 31$$

$$(31 - 14)(11) = 1 \bmod 31$$

$17 \cdot 11 = 1 \bmod 31 \Rightarrow \text{t} = 17$

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

$$x = (3 \cdot 17) \bmod 31$$

$$x = 51 \bmod 31$$

$$x = 20$$

Example 2: Solve the following linear congruence; $11x \equiv 2 \bmod 23$

Solution: We introduce another parameter t such the $11t = 1 \pmod{23}$....(i) then

$$11xt = 2t \bmod 23$$

Hence we can say that; $x = 2t \bmod 23 \cdots (ii)$

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

Then;

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

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

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

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

Theorem 1: (Chinese remainder theorem)

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

$$x \equiv a_1 \bmod m_1$$

$$x \equiv a_2 \bmod m_2$$

$$\cdots$$

$$\cdots$$

$$x \equiv a_n \bmod m_n$$

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

i.e., there is a solution x with $0 \leq x \leq m$, 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; $\mathrm{x} \equiv 1 \bmod 2, \mathrm{x} \equiv 2 \bmod 3, \mathrm{x} \equiv 3 \bmod 5, \mathrm{x} \equiv 4 \bmod 11$ (Rosen, 2012, p. 285).

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

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

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

$$1 + 2\mathrm{t} \equiv 2 \bmod 3 \cdots (\mathrm{ii})$$

Discussed in Lecture 4, *If* a *and* b *are integers and* m *is a positive integer, then* $a \equiv b \ (mod\ m)$ *if* $m|(a - b)$ then equation (ii) we can say;

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

$$3|2\mathrm{t} - 1$$

$$\therefore 2\mathrm{t} = 1 \bmod 3 \Rightarrow \mathrm{t} = 2 \bmod 3$$

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

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

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

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

$$5 + 6\mathrm{u} = 3 \bmod 5$$

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

$$5|6u + 2 \therefore 6\mathrm{u} = -2 \bmod 5 = 3 \bmod 5 \Rightarrow 5|6\mathrm{u} - 3 = 5|3(2\mathrm{u} - 1) \equiv 5|2\mathrm{u} - 1$$

Therefore, we have;

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

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

$$\therefore \mathrm{x} = 23 + 30\mathrm{v} \cdots (\mathrm{vi})$$

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

$$23 + 30\mathrm{v} = 4 \bmod 11$$

$$\Rightarrow 11|(23 + 30\mathrm{v}) - 4$$

$$11|30v + 19$$

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

$$\therefore 30\mathrm{v} = 3 \bmod 11$$

Thus

$$11|30v + 19 \equiv 11|30v - 3 \equiv 11|3(10v - 1) \equiv 11|10v - 1 \therefore 10v = 1 \bmod 11$$

$$\Rightarrow v = 10 \bmod 11$$

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

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

$$x = 323 + 330w$$

$$\Rightarrow x \equiv 323 \bmod 330$$

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

Solution: From $x \equiv 2 \bmod 3$ we have $x = 3t + 2 \cdots (i)$ for some integers t.

Hence $x \equiv 4 \bmod 7$ becomes $3t + 2 \equiv 4 \bmod 7$

Which implies then that;

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

$$7|3t - 2 \therefore 3t = 2 \bmod 7 \Rightarrow t = 3 \bmod 7$$

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

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

Hence we have equation $x \equiv 6 \bmod 10$ becomes $21u + 11 \equiv 6 \bmod 10$

Which implies that;

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

$$10|21u + 5 \Rightarrow 21u = -5 \bmod 10$$

$$21u = 5 \bmod 10 \therefore u = 5 \bmod 10$$

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

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

$$x = 210v + 116 \cdots (iii)$$

Therefore, our last equation $x \equiv 11 \bmod 21$ becomes;

$$210v + 116 \equiv 11 \bmod 21 \Rightarrow 116 \equiv 11 \bmod 21 \therefore x = 116 \bmod 210$$

Note that we can still proceed and have;

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

$$21|210v + 105$$

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

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

$$2\mathrm{v} \equiv 20 \bmod 21 \therefore \mathrm{v} \equiv 10 \bmod 21$$

Hence $\mathrm{v} = 21\mathrm{w} + 10$ for some integer w.

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

$$\Rightarrow \mathrm{x} \equiv 2216 \bmod 4410$$

However, 116 is the smallest positive integer satisfying all the congruences. By Chinese remainder theorem $m = m_1 m_2 m_3 m_4 = 3 \times 7 \times 10 \times 21 = 4410$

Exercise

1) Determine the inverse of the following
    a. 19 mod 391
    b. 23 mod 250
    c. 23 mod 270
    d. 231 mod 11793
2) Solve the following congruences
    a. $11\mathrm{x} \equiv 2 \bmod 23$
    b. $17\mathrm{x} \equiv 7 \bmod 43$
    c. $13\mathrm{x} \equiv 7 \bmod 33$
3) Find all solutions, if any, so the system of congruences (Rosen, 2012, p. 285)
    a. $\mathrm{x} \equiv 5 \bmod 6, \mathrm{x} \equiv 3 \bmod 10, \mathrm{x} \equiv 8 \bmod 15$
    b. $\mathrm{x} \equiv 7 \bmod 9, \mathrm{x} \equiv 4 \bmod 12, \mathrm{x} \equiv 16 \bmod 21$
    c. $\mathrm{x} \equiv 2 \bmod 3, \mathrm{x} \equiv 1 \bmod 4, \mathrm{x} \equiv 3 \bmod 5$
4) Attempt exercises in (Rosen, 2012, p. 284).

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