Introduction to Sets and Logic (MATH 1190)

Instructor: Lili Shen
Email: shenlili@yorku.ca

Department of Mathematics and Statistics
York University

Nov 20, 2014

Homework announcement

Since Dec 4 will be the date of our last class, the TA will collect the homework (assigned today) on Nov 27 for the last time.

You do not need to hand in the homework of Nov 27 and Dec 4, but in order to prepare for the final exam, it is highly suggested to finish them by yourself.

Outline

1 Solving Congruences

Linear congruences

A congruence of the form

$$ax \equiv b \pmod{m},$$

where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence. In general, the solutions are expressed as

$$x \equiv c \pmod{m}$$

for some fixed integers c and m, which means all integers of the form $c + km$ $(k \in \mathbf{Z})$ satisfy $ax \equiv b \pmod{m}$.

Inverse of a modulo m

Definition

An integer $\overline{a}$ such that $a\overline{a} \equiv 1 \pmod{m}$ is called an inverse of a modulo m.

Inverse of a modulo m

One method of solving linear congruences makes use of an inverse $\overline{a}$, if it exists. Although we can not divide both sides of the congruence

$$ax \equiv b \pmod{m}$$

by a, we can multiply by $\overline{a}$ and obtain

$$\overline{a}ax \equiv \overline{a}b \pmod{m}.$$

Since $a\overline{a} \equiv 1 \pmod{m}$ implies

$$x \equiv a\overline{a}x \pmod{m},$$

it follows that the solutions of $ax \equiv b \pmod{m}$ are those integers x satisfying

$$x \equiv \overline{a}b \pmod{m}.$$

Finding inverses

When m is small, we may find an inverse of a modulo m simply by inspection. For example, in order to find an inverse of 3 modulo 7, we check $3 \cdot k$ for $k = 1, 2, 3, 4, 5, 6$ (i.e., the positive integers smaller than 7), and find that

$$5 \cdot 3 = 15 \equiv 1 \pmod 7,$$

so 5 is an inverse of 3 modulo 7.

When m is large, we may try to find its inverse in the following way.

Finding inverses

Theorem

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

In other words, there is a unique positive integer $\overline{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\overline{a}$ modulo m.

Finding inverses

Proof.

Since $\gcd(a, m) = 1$, there are integers s and t such that

$$sa + tm = 1.$$

Therefore, $sa \equiv 1 \pmod{m}$, and s is an inverse of a modulo m.

For the uniqueness of s, suppose that there is another integer s' satisfying $s'a \equiv 1 \pmod{m}$, then

$$sa - s'a \equiv 0 \pmod{m},$$

and consequently $m \mid a(s - s')$. Since $\gcd(a, m) = 1$, it follows that $m \mid (s - s')$, i.e., $s \equiv s' \pmod{m}$, as desired. □

Examples of solving linear congruences

Example

Solve the linear congruence $3x \equiv 4 \pmod{7}$, and find the smallest positive integer that is a solution of this congruence.

Examples of solving linear congruences

Solution.

First we find that 5 is an inverse of 3 modulo 7 by inspection, i.e.,

$$5 \cdot 3 \equiv 1 \pmod{7}.$$

Now we multiply both sides of $3x \equiv 4 \pmod{7}$ by 5, and obtain

$$15x \equiv 20 \pmod{7}.$$

It follows that the solutions are the integers satisfying

$$x \equiv 15x \equiv 20 \equiv 6 \pmod{7}.$$

The smallest integer that solves the congruence is 6. □

Examples of solving linear congruences

Example

Solve the linear congruence $19x \equiv 4 \pmod{141}$.

Examples of solving linear congruences

Solution.

First we find an inverse of 19 modulo 141

$$\begin{aligned} 141 &= 19 \cdot 7 + 8, \\ 19 &= 8 \cdot 2 + 3, \\ 8 &= 3 \cdot 2 + 2, \\ 3 &= 2 \cdot 1 + 1, \end{aligned}$$

it follows that $\gcd(19, 141) = \gcd(19, 8) = \gcd(8, 3) = \gcd(3, 2) = \gcd(2, 1) = 1$.

Examples of solving linear congruences

Consequently,

$$\begin{aligned}1 &= 3 - 2\\ &= 3 - (8 - 3 \cdot 2) = 3 \cdot 3 - 8\\ &= 3 \cdot (19 - 8 \cdot 2) - 8 = 3 \cdot 19 - 7 \cdot 8\\ &= 3 \cdot 19 - 7 \cdot (141 - 19 \cdot 7) = -7 \cdot 141 + 52 \cdot 19.\end{aligned}$$

Thus $52 \cdot 19 \equiv 1 \pmod{141}$, and thus 52 is an inverse of 19 modulo 141.

Examples of solving linear congruences

Now we multiply both sides of $19x \equiv 4 \pmod{141}$ by 52, and obtain

$$52 \cdot 19x \equiv 52 \cdot 4 = 208 \pmod{141}.$$

It follows that the solutions are the integers x satisfying

$$x = (52 \cdot 19x - 7 \cdot 141x) \equiv 208 \equiv 67 \pmod{141}.$$

□

The Chinese remainder theorem

In order to find solutions for a system of congruences like

$$\begin{aligned} x &\equiv 2 \pmod{3}, \\ x &\equiv 3 \pmod{5}, \\ x &\equiv 2 \pmod{7}, \end{aligned}$$

we introduce the following Chinese remainder theorem (also called Sun-Tsu theorem).

The Chinese remainder theorem

Theorem (The Chinese remainder theorem)

Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \dots, a_n$ arbitrary integers. Then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\cdots\cdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \dots m_n$. (That is, there is a unique solution x with $0 \leq x < m$, and all other solutions are congruent module m to this solution.)

The Chinese remainder theorem

Proof.

For $k = 1, 2, \ldots, n$, let

$$M_k = \frac{m}{m_k},$$

then $\gcd(m_k, M_k) = 1$. It follows that there is an inverse y_k of M_k modulo m_k, i.e.,

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Let

$$x = \sum_{k=1}^{n} a_k M_k y_k = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

The Chinese remainder theorem

Note that

$$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$$

for each $k = 1, 2, \ldots, n$, thus x is a solution for the system of congruences.

For the uniqueness of the solution, suppose that there is another integer y satisfying $y \equiv a_k \pmod{m_k}$ for each k, then $x \equiv y \pmod{m_k}$ for each k, and consequently $m_k \mid (x - y)$ for each k. Since $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, it follows that

$$m = m_1 m_2 \ldots m_n \mid (x - y),$$

i.e., $x \equiv y \pmod{m}$, as desired. □

Examples of solving linear congruences

Example

Solve the system of linear congruences

$$\begin{aligned} x &\equiv 2 \pmod 3, \\ x &\equiv 3 \pmod 5, \\ x &\equiv 2 \pmod 7. \end{aligned}$$

Examples of solving linear congruences

Solution 1.

Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = 35$, $M_2 = 21$, $M_3 = 15$. By inspection we find that

$$\begin{aligned} 35 \cdot 2 &\equiv 1 \pmod{3}, \\ 21 \cdot 1 &\equiv 1 \pmod{5}, \\ 15 \cdot 1 &\equiv 1 \pmod{7}. \end{aligned}$$

Thus those integers x satisfy

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$$

are the solutions. □

Examples of solving linear congruences

Solution 2 (back substitution).

If $x \equiv 2 \pmod 3$, then $x = 3t + 2$, where $t \in \mathbf{Z}$. Substituting this expression for x into the second congruence, we get

$$3t + 2 \equiv 3 \pmod 5,$$

and consequently $3t \equiv 1 \pmod 5$. Since 2 is an inverse of 3 modulo 5, we multiply both sides by 2 and obtain

$$6t \equiv 2 \pmod 5,$$

and consequently $t \equiv 2 \pmod 5$, which means $t = 5u + 2$, where $u \in \mathbf{Z}$, and thus $x = 3(5u + 2) + 2 = 15u + 8$.

Examples of solving linear congruences

Substituting this expression for x into the third congruence, we get

$$15u + 8 \equiv 2 \pmod{7},$$

and consequently $15u \equiv -6 \equiv 1 \pmod{7}$. Since 1 is an inverse of 15 module 7, it follows immediately that

$$u \equiv 1 \pmod{7},$$

which means $u = 7v + 1$, where $v \in \mathbf{Z}$, and thus

$$x = 15(7v + 1) + 8 = 105v + 23.$$

Therefore, those integers x satisfy $x \equiv 23 \pmod{105}$ are the solutions. □

Recommended exercises

Section 4.4: 5, 11, 20, 21, 23, 24.