Solving Congruences

Solving linear congruences, which have the form $ax \equiv b \pmod{m}$, is an essential task in the study of number theory and its applications, just as solving linear equations plays an important role in calculus and linear algebra.

To solve linear congruences, we employ inverses modulo m.

We explain how to work backwards through the steps of the Euclidean algorithm to find inverses modulo m.

Once we have found an inverse of a modulo m, we solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides of the congruence by this inverse.

We will show how to solve systems of linear congruences modulo pairwise relatively prime moduli. The result, we will prove is called the Chinese remainder theorem, and our proof will give a method to find all solutions of such systems of 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**

How can we solve the linear congruence $ax \equiv b \pmod{m}$, that is, how can we find all integers x that satisfy this congruence?

One method that we will describe uses an integer $\bar{a}$
such that $a\,\bar{a} \equiv 1 \pmod{m}$, if such an integer exists. Such an integer $\bar{a}$ is said to be an **inverse** of a modulo m.

Theorem 1 guarantees that an inverse of a modulo m exists whenever a and m are relatively prime

Theorem:

Let m be a positive integer, a and b be any integers, and $d = \gcd(a, m)$, the linear congruence is given as

$$ax \equiv b \ (mod\ m)$$

(a) The linear congruence has a solution if and only if d|b, and there is no solution otherwise.

(b) The solution of the linear congruent can be obtained by solving following congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \ (mod\ \frac{m}{d})$$

(c) The given congruence has d solutions, which are mutually incongruent modulo m

THEOREM 1

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. (That is, there is a unique positive integer $\boldsymbol{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to a modulo m.)

Proof: As $\gcd(a, m) = 1$, (a and m are relatively prime) by Theorem 6 of Section 4.3 (Bezouts Theorem), there are integers s and t such that $sa + tm = 1$.

This implies that $sa + tm \equiv 1 \pmod{m}$. But $tm \equiv 0 \pmod{m}$, it follows that $sa \equiv 1 \pmod{m}$.
Consequently, s is an inverse of a modulo m. That this inverse is unique modulo m is left as Exercise 7.

Technique/Observation to find inverse:

1. Using inspection to find an inverse of a modulo m is easy when m is small.
2. To find this inverse, we look for a multiple of a that exceeds a multiple of m by 1.
3. For example, to find an inverse of 3 modulo 7,

   we can find $j * 3$ for $j = 1, 2, \ldots, 6$, **stopping** when we find a multiple of 3 that is **one more than a multiple of 7**.

4. We can speed this approach up if we note that $2 * 3 \equiv -1 \pmod 7$. This means that $(-2) * 3 \equiv 1 \pmod 7$.

   Hence, $5 * 3 \equiv 1 \pmod 7$, so 5 is an inverse of 3 modulo 7

5. We can design a more efficient algorithm than brute force to find an inverse of a modulo m when $\gcd(a, m) = 1$ using the steps of the Euclidean algorithm

Examples Problems

1. Find the solution of the congruence $6\,x \equiv 3\ (mod\ 9)$

Solution: From the given congruence relation one can check that $2, 5, 8$ are the solutions. The same solution can be obtained by another method by the theorem (stated in the previous slide/page).

Since $\gcd(6,9) = 3$ and 3 divides 3, hence the congruence has three solutions. The solution of the given congruence can be obtained by solving linear congruence $2\,x \equiv 1\ (\text{mod}\ 3)$.

By Choosing $x = 0, 1, 2$ and testing the congruence, we get $x = 2$.

Thus the first solution to the given congruence is $x_0 = 2$.

Comparing the given congruence relation with $a\,x \equiv b\ (\text{mob}\ m)$,

we have $a = 6, b = 3, m = 9$.

Thus the other solutions are (by theorem (b) previous slide)

$$x_1 = x_0 + \frac{m}{d} = 2 + 3 = 5 \quad \text{and} \quad x_2 = x_0 + 2\frac{m}{d} = 2 + 6 = 8$$

Thus, the solutions are $2,5$ and 8.

Examples Problems

1. Find the solution of the congruence $2\,x \equiv 1\ (mod\ 5)$

Solution: Since $\gcd(2,5) = 1$, hence , the solution is unique under the congruence modulo 5.

Choosing $x = 0,1,2,3,4$ and testing the congruence, we get $x = 3$.

2. Find the solution of the congruence $3\,x \equiv 2\ (mod\ 4)$

Solution: Since $\gcd(3,4) = 1$, the solution is unique under the congruence modulo 4.

Choosing $x = 0,1,2,3$ and testing the congruence, we get $= 2$.

Exercise. Find the solution of the congruence $4\,x \equiv 3\ (mod\ 2)$

EXAMPLE

Find an inverse of 101 modulo 4620

Solution: For completeness, we present all steps used to compute an inverse of 101 modulo 4620.

First, we use the Euclidean algorithm to show that

$\gcd(101, 4620) = 1$.

Then we will reverse the steps to find Bézout coefficients a and b such that $101a + 4620b = 1$.

It will then follow that a is an inverse of 101 modulo 4620. The steps used by the Euclidean algorithm to find $\gcd(101, 4620)$ are

$$4620 = 45 * 101 + 75$$
$$101 = 1 * 75 + 26$$
$$75 = 2 * 26 + 23$$
$$26 = 1 * 23 + 3$$
$$23 = 7 * 3 + 2$$
$$3 = 1 * 2 + 1$$
$$2 = 2 * 1.$$

Since, the last nonzero remainder is 1,

therefore the $\gcd(101, 4620) = 1$

We can now find the Bézout coefficients for 101 and 4620 by working backwards through these steps, expressing $\gcd(101, 4620) = 1$ in terms of each successive pair of remainders.

In each step we eliminate the remainder by expressing it as a linear combination of the divisor and the dividend. We obtain

$$
\begin{aligned}
1 &= 3 - 1 * 2 \\
&= 3 - 1 * (23 - 7 * 3) && = -1 * 23 + 8 * 3 \\
&= -1 * 23 + 8 * (26 - 1 * 23) && = 8 * 26 - 9 * 23 \\
&= 8 * 26 - 9 * (75 - 2 * 26) && = -9 * 75 + 26 * 26 \\
&= -9 * 75 + 26 * (101 - 1 * 75) && = 26 * 101 - 35 * 75 \\
&= 26 * 101 - 35 * (4620 - 45 * 101) \\
&= -35 * 4620 + 1601 * 101.
\end{aligned}
$$

That $-35 * 4620 + 1601 * 101 = 1$ tells us that -35 and 1601 are Bézout coefficients of 4620 and 101, and 1601 is an inverse of 101 modulo 4620.

Example:

What are the solutions of the linear congruence $3x \equiv 4 \pmod 7$?

Solution: By earlier Example, 5 is an inverse of 3 modulo 7.

Multiplying both sides of the congruence by 5 shows that
$5 * 3x \equiv 5 * 4 \pmod 7$, as $15 \equiv 1 \pmod 7$ and $20 \equiv 6 \pmod 7$,

it follows that if x is a solution, then $x \equiv 20 \equiv 6 \pmod 7$.
We need to determine whether every x with $x \equiv 6 \pmod 7$ is a solution.
Assume that
$x \equiv 6 \pmod 7$. Then, by Theorem 5 of Section 4.1, it follows that
$3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod 7$, which shows that all such x satisfy the congruence. We conclude that the solutions to the congruence are the integers x such that $x \equiv 6 \pmod 7$, namely, 6, 13, 20, . . . and -1, -8,-15.

The Chinese Remainder Theorem

Question: Example-I

When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things?

This puzzle can be translated into the following question: What are the solutions of the systems of congruences

$x \equiv 2 \pmod 3$,
$x \equiv 3 \pmod 5$,
$x \equiv 2 \pmod 7$?

We will solve this system, and with it Sun-Tsu's puzzle, later in this section.

The Chinese Remainder Theorem

The *Chinese remainder theorem*, named after the Chinese heritage of problems involving systems of linear congruences, states that when the moduli of a system of linear congruences are pairwise relatively prime, there is a unique solution of the system modulo the product of the moduli.

The Chinese Remainder Theorem

THEOREM 2:

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

$$x \equiv a_1 \pmod{m_1},$$
$$x \equiv a_2 \pmod{m_2},$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

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

Proof: To establish this theorem, we need to show that a solution exists and that it is unique modulo m.

To construct a simultaneous solution, first let $M_k = \frac{m}{m_k}$ for $k = 1, 2, \ldots, n$.

That is, M_k is the product of the moduli except for m_k . Because m_i and m_k have no common factors greater than 1 when $i \neq k$, it follows that $\gcd(m_k, M_k) = 1$.

Consequently, by Theorem 1, we know that there is an integer y_k, an inverse of M_k modulo m_k, such that $M_k y_k \equiv 1 \pmod{m_k}$.
To construct a simultaneous solution, form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n.$$

We will now show that x is a simultaneous solution.

First, note that because

$M_j \equiv 0 \pmod{m_k}$ whenever $j = k$, all terms except the k^{th} term in this sum are congruent to 0 modulo m_k.

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

we get $x \equiv a_k M_k y_k \equiv a_k \pmod{mk}$, for $k = 1, 2, \ldots, n$.

We have shown that x is a simultaneous solution to the n congruences.

We use this solution technique in solving **Question: Example-I, that is after mathematical formulation we have**

$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{5}$
$x \equiv 2 \pmod{7}$

Example: $x \equiv 2 \pmod 3$,
$x \equiv 3 \pmod 5$,
$x \equiv 2 \pmod 7$.

Solution: To solve the system of congruences in Example-I,

first let $m_1 = 3;\ m_2 = 5;\ m_3 = 7, a_1 = 2, a_2 = 3, a_3 = 2$.

Therefore, $m = 3 * 5 * 7 = 105$,

$$M_1 = \frac{m}{3} = 35,$$

$$M_2 = \frac{m}{5} = 21,$$

and $$M_3 = \frac{m}{7} = 15.$$

Now, $M_1 y_1 \equiv 1 (mod\ 3)$

We see that 2 is an inverse of $M_1 = 35$ modulo 3.

Since $35 * 2 \equiv 2 * 2 \equiv 1 \pmod 3$; therefore, $y_1 = 2$. (Cont….)

Now, consider $M_2 y_2 \equiv 1 (mod\ 5)$

1 is an inverse of $M_2 = 21$ modulo 5.

Since $21 \equiv 1 \pmod 5$; therefore, $y_2 = 1$.

Consider $M_3 y_3 \equiv 1 (mod\ 7)$

1 is an inverse of $M_3 = 15 \pmod 7$,

since $15 \equiv 1 \pmod 7$; therefore, $y_3 = 1$.

The solutions to this system are those x such that

$$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$$
$$= 2 * 35 * 2 + 3 * 21 * 1 + 2 * 15 * 1 = 233 \equiv 23 \ (mod\ 105).$$

It follows that 23 is the smallest positive integer that is a simultaneous solution.

We conclude that 23 is the smallest positive integer that leaves a remainder of 2 when divided by 3, a remainder of 3 when divided by 5, and a remainder of 2 when divided by 7.

Chinese Reminder Theorem by Back Substitution method (Another Method)

Example: Use the method of back substitution to find all integers x such that $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, and $x \equiv 3 \pmod 7$.
Solution: (By Theorem 4 in Section 4.1)

The first congruence can be rewritten as an equality,
$x = 5t + 1$ where t is an integer.

Substituting this expression for x into the second congruence
tells us that $5t + 1 \equiv 2 \pmod 6$ this can be simplified to $5t \equiv 1 \pmod 6$

Now, find the inverse of 5 in mod 6 and multiple on both side by inverse of 5 gives $t \equiv 5 \pmod 6$ (which can be easily solved to show that)
Again by Theorem 4, we see that $t = 6u + 5$ where u is an integer. ..(Cont)

Substituting this expression for t back into the equation $x = 5t + 1$ we get, $x = 5(6u + 5) + 1 = 30u + 26.$
We insert this into the third equation to obtain
$30u + 26 \equiv 3 (\text{mod } 7)$ can be further simplify to $30u \equiv -23 (\text{mod } 7)$

Is equivalent to $2u \equiv 5 \ (\text{mod } 7)$, now to get the value of u alone on right hand side, multiply the congruence relation $2u \equiv 5 \ (\text{mod } 7)$ by 4 on both sides, we get $8u \equiv 20 (\text{mod } 7)$,

is equivalent to $u \equiv 6 \ (\text{mod } 7)$ and this can be expressed as $u = 7v + 6$ where v is an integer.
Now, substituting this expression for u into the equation $x = 30u + 26$ gives $x = 30(7v + 6) + 26 = 210v + 206$. Translating this back into a congruence, we find the solution to the simultaneous congruences,
$x \equiv 206 \ (\text{mod } 210)$.

Exercise Problems

1. Show that 937 is an inverse of 13 modulo 2436
2. Find an inverse of a modulo m for each of these pairs of relatively prime integers (using the method followed in Example 2 Text book).

   a) $a = 4, m = 9$ **b)** $a = 19, m = 141$
   c) $a = 55, m = 89$ **d)** $a = 89, m = 232$

3. Solve each of these congruences using the modular inverses.

a) $19x \equiv 4 \pmod{141}$
b) $55x \equiv 34 \pmod{89}$
c) $89x \equiv 2 \pmod{232}$

4. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 4 \pmod{11}$.

5. Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the method of back substitution.

6. Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod 6$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

7. Find all solutions, if any, to the system of congruences $x \equiv 7 \pmod 9$, $x \equiv 4 \pmod{12}$, and $x \equiv 16 \pmod{21}$.

Fermat's Little Theorem

- The great French mathematician Pierre de Fermat made many important discoveries in number theory.
- One of the most useful of these states that p divides $a^{p-1} - 1$ whenever p is prime and a is an integer not divisible by p.
- Fermat announced this result in a letter to one of his correspondents.
- However, he did not include a proof in the letter, stating that he feared the proof would be too long.
- Although Fermat never published a proof of this fact, there is little doubt that he knew how to prove it, unlike the result known as Fermat's last theorem.
- The first published proof is credited to Leonhard Euler

Fermat's Little Theorem

THEOREM 3 (FERMAT'S LITTLE THEOREM)

If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Furthermore, for every integer a we have

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

Remark: Fermat's little theorem tells us that if $a \in \boldsymbol{Z}_p$, then $a^{p-1} = 1$ in $\boldsymbol{Z}_p$.

Example: Fermat's Little Theorem

Example: Find 7^{222} **mod** 11

Solution: We can use Fermat's little theorem to evaluate 7222 **mod** 11 rather than using the fast modular exponentiation algorithm.

By Fermat's little theorem we know that $7^{10} \equiv 1 \pmod{11}$,
so $(7^{10})^k \equiv 1 \pmod{11}$ for every positive integer k.

To take advantage of this last congruence, we divide the exponent 222 by 10, finding that $222 = 22 \cdot 10 + 2$.

We now see that
$7^{222} = 7^{22*10+2} = (7^{10})^{22}7^2 \equiv (1)^{22} * 49 \equiv 5 \pmod{11}$.

It follows that 7^{222} **mod** $11 = 5$

Exercise Problems

1. Use Fermat's little theorem to find $7121 \bmod 13$.
2. Use Fermat's little theorem to find $231002 \bmod 41$.
3. Use Fermat's little theorem to compute $3302 \bmod 5$, $3302 \bmod 7$, and $3302 \bmod 11$.
4. Use your results from part (a) and the Chinese remainder theorem to find $3302 \bmod 385$. (Note that $385 = 5 \cdot 7 \cdot 11$.)

Fermat's Little Theorem

We can use Fermat's little theorem to compute a^n **mod** p, where p is prime and $p \nmid a$.

First, we use the division algorithm to find the quotient q and remainder r when n is divided by $p - 1$, so that $n = q(p - 1) + r$ where $0 \leq r < p - 1$.

It follows that $a^n = a^{q(p-1)+r} = (a^{p-1})^q a^r \equiv 1^q a^r \equiv a^r \pmod{p}$. Hence, to find a^n **mod** p,

we only need to compute a^r **mod** p.

We will take advantage of this simplification many times in our study of number theory.

Definition:

Let b be a positive integer. If n is a composite positive integer, and $b^{n-1} \equiv 1 \pmod{n}$, then n is called a *pseudoprime to the base* b.

Example:

The integer 341 is a pseudoprime to the base 2 because it is composite $(341 = 11 \cdot 31)$ and as (Exercise 37 shows)
$2^{340} \equiv 1 \pmod{341}$.

Carmichael number

Definition:

A composite integer n that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all positive integers b with $\gcd(b, n) = 1$ is called a *Carmichael number*.

These numbers are named after Robert Carmichael, who studied them in the early twentieth century.

Example:

The integer 561 is a Carmichael number.

To see this, first note that 561 is composite because $561 = 3 \cdot 11 \cdot 17$.
Next, note that if $\gcd(b, 561) = 1$, then $\gcd(b, 3) = \gcd(b, 11) = \gcd(b, 17) = 1$.
Using Fermat's little theorem we find that
$b^2 \equiv 1 \pmod 3$, $b^{10} \equiv 1 \pmod{11}$, and $b^{16} \equiv 1 \pmod{17}$.
It follows that

$$b^{560} = (b^2)^{280} \equiv 1 \pmod 3,$$
$$b^{560} = (b^{10})^{56} \equiv 1 \pmod{11},$$
$$b^{560} = (b^{16})^{35} \equiv 1 \pmod{17}.$$

(By Exercise 29), it follows that $b^{560} \equiv 1 \pmod{561}$ for all positive integers b with $\gcd(b, 561) = 1$.

Hence 561 is a Carmichael number

Primitive Roots and Discrete Logarithms

In the set of positive real numbers, if $b > 1$, and $x = b^y$, we say that y is the logarithm of x to the base b. Here, we will show that we can also define the concept of logarithms modulo p of positive integers where p is a prime

Definition:

A *primitive root* modulo a prime p is an integer r in Z_p such that every nonzero element of Z_p is a power of r.

Example:

Determine whether 2 and 3 are primitive roots modulo 11.

Solution:

When we compute the powers of 2 in $\boldsymbol{Z_{11}}$, we obtain $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$.
Because every element of $\boldsymbol{Z_{11}}$ is a power of 2, 2 is a primitive root of 11.
When we compute the powers of 3 modulo 11, we obtain $3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4, 3^5 = 1$.

We note that this pattern repeats when we compute higher powers of 3.
Because not all elements of $\boldsymbol{Z_{11}}$ are powers of 3, we conclude that 3 is not a primitive root of 11.

- Suppose that p is a prime, r is a primitive root modulo p, and a is an integer between 1 and p - 1 inclusive. If re **mod** $p = a$ and $0 \leq e \leq p - 1$, we say that e is the *discrete logarithm* of a modulo p to the base r and we write $\log_r a = e$ (where the prime p is understood).

Example:

Find the discrete logarithms of 3 and 5 modulo 11 to the base 2.

Solution:

When we computed the powers of 2 modulo 11 in earlier Example, we found that $2^8 = 3$ and $2^4 = 5$ in $\boldsymbol{Z}_{11}$.

Hence, the discrete logarithms of 3 and 5 modulo 11 to the base 2 are 8 and 4, respectively. (These are the powers of 2 that equal 3 and 5, respectively, in $\boldsymbol{Z}_{11}$.)

We write $\log_2^3 = 8$ and $\log_2^5 = 4$ (where the modulus 11 is understood and not explicitly noted in the notation).