Number Theory

Chapter 4

Edited by: Dr. Meshal Alfarhood

Solving Congruences

Section 4.4

Section Summary

Linear Congruences

- Finding Inverses

The Chinese Remainder Theorem

Fermat’s Little Theorem

The Euler’s Generalization

Linear Congruences

Definition: A congruence of the form $ax \equiv b \pmod{m}$ is called a *linear congruence*.

- The solutions to a linear congruence $ax \equiv b \pmod{m}$ are all integers x that satisfy the congruence.
- One method of solving linear congruences makes use of an inverse $\bar{a}$, if it exists.
  - If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m **exists**.

Definition: An integer $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$ is said to be an ***inverse* of *a* modulo *m***.

- **Example:** Find inverse of 3 modulo 7?
  - Since gcd(3,7)=1, so the inverse exists.
  - Thus: $\bar{a}3 \equiv 1 \pmod{7}$
  - By inspection: $\mathbf{\bar{a}=5}$ since $15 \equiv 1 \pmod{7}$
  - 5 is the inverse of 3 modulo 7

The existence of Inverse

Theorem: If *a and m are relatively prime* integers and $m > 1$, then an inverse of a modulo m **exists**.

Examples:

1. Find inverse of 4 modulo 7?
   - Since gcd(4,7)=1 → There exists an inverse of 4 modulo 7.

     $\bar{a}4 \equiv 1 (\bmod 7)$

     $8 \equiv 1 (\bmod 7)$ → $\bar{a}$=**2** is the inverse.
2. Find inverse of numbers [1-6] modulo 7?
   - Since 7 is prime, all numbers have an inverse modulo 7.

Number	1	2	3	4	5	6
Inverse	1	4	5	2	3	6

3. Construct inverse table for numbers [1-6] modulo 8?

Number	1	2	3	4	5	6
Inverse	1	-	3	-	5	-

Finding Inverses 1

To Find Inverse of *a* modulo *m*:

1. Use Euclidean algorithm to find gcd(a,m).
2. Express gcd as linear combination: **s**a + tm = 1.
3. **s** is the inverse of a modulo m.

Example 1: Find an inverse of 3 modulo 7.

Solution: Since gcd(3,7) = 1, an inverse of 3 modulo 7 exists.

- Using the Euclidean algorithm:
  - $7 = 2 \cdot 3 + 1$
- Working Backwards:
  - $1 = 1 \cdot 7 - 2 \cdot 3$
- Hence, **−2** is an inverse of 3 modulo 7.
- Also every integer congruent to −2 modulo 7 is an inverse of 3 modulo 7, i.e., -16,-9,5,12, etc.

Finding Inverses 2

Example 2: Find an inverse of 101 modulo 4620?

Solution:

Using Euclidean algorithm:

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

Working Backwards:

$1 = 3 - 1 \cdot 2$

$1 = 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3$

$1 = -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23$

$1 = 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = 26 \cdot 26 - 9 \cdot 75$

$1 = 26 \cdot (101 - 1 \cdot 75) - 9 \cdot 75 = 26 \cdot 101 - 35 \cdot 75$

$1 = 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101)$

$= -35 \cdot 4620 + \mathbf{1601} \cdot 101$

1601 is an inverse of 101 modulo 4620.

Using Inverses to Solve Congruences

We can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

Example 1: What are the solutions of the congruence $\mathbf{3x \equiv 4 \pmod{7}}$.

Solution:

- We found previously that **−2** is an inverse of 3 modulo 7.
- We multiply both sides of the congruence by **−2**, giving:

$$-2 \cdot 3x \equiv -2 \cdot 4 \pmod{7}$$

$$x \equiv -8 \pmod{7}$$

Because: -8 mod 7 = 6

$$x \equiv 6 \pmod{7}$$

- The solutions are all integers congruent to 6 modulo 7, such as 6,13,20,… and -1,−8,−15,…
- General solution is **6 + 7k** for $k \in Z$.

Using Inverses to Solve Congruences [2]

We can solve the congruence $ax \equiv b \pmod{m}$ by multiplying both sides by $\bar{a}$.

Example 2: What are the solutions of the congruence $\mathbf{2x \equiv 7 \pmod{17}}$.

Solution:

- We can find by inspection that **9** is an inverse of 2 modulo 17
- We multiply both sides of the congruence by **9**, giving:

$$9 \cdot 2x \equiv 9 \cdot 7 \pmod{17}$$

$$x \equiv 63 \pmod{17}$$

Because: 63 mod 17 = 12

$$x \equiv 12 \pmod{17}$$

- The solutions are all integers congruent to 12 modulo 17, such as 12,29,… and -5,−22,…
- General solution is **12 + 17k** for $k \in Z$.

The Chinese Remainder Theorem

The story behind this theorem:

- In the first century, the Chinese mathematician Sun-Tsu asked:
- There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5, the remainder is 3; when divided by 7, the remainder is 2. What will be the number of things?
- This puzzle can be translated into the solution of the system of congruences:

$x \equiv 2 \pmod{3}$,

$x \equiv 3 \pmod{5}$,

$x \equiv 2 \pmod{7}$?

The Chinese Remainder Theorem [2]

The Chinese Remainder Theorem: Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers > 1. Then the system:

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

has a unique solution modulo $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

The solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.

To construct a solution:

1. Compute $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$
2. Compute $M_k = m/m_k$ for every $k = 1, 2, \ldots, n$.
3. Compute y_k where y_k is the inverse M_k modulo m_k, such that
$$M_k \, y_k \equiv 1 \pmod{m_k}$$
4. The solution is: $x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n$ modulo m

The Chinese Remainder Theorem 3

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

Solution:

- 3, 5, and 7 ae pairwise relatively prime. → there exists a solution.
- $a_1 = 2$, $a_2 = 3$, $a_3 = 2$
- Let $m = 3 \cdot 5 \cdot 7 = 105$
- $M_1 = 105/3 = 35$, $M_2 = 105/5 = 21$, $M_3 = 105/7 = 15$.
- We see that
  - 2 is an inverse of $M_1 = 35$ modulo 3 since $70 \equiv 1 \pmod 3$
  - 1 is an inverse of $M_2 = 21$ modulo 5 since $21 \equiv 1 \pmod 5$
  - 1 is an inverse of $M_3 = 15$ modulo 7 since $15 \equiv 1 \pmod 7$
- The solution is $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$

$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1$$

$$= 233 \bmod 105 = 23$$

$$\boxed{x = 23 + 105k}$$