Solving Congruences

Section 4.4

Linear Congruences

Definition: A congruence of the form

$ax \equiv b(\bmod m)$,

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

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

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

Example: 5 is an inverse of 3 modulo 7 since $5 \cdot 3 = 15 \equiv 1(\bmod 7)$

One method of solving linear congruences makes use of an inverse $\bar{a}$, if it exists. Although we can not divide both sides of the congruence by a, we can multiply by $\bar{a}$ to solve for x.

Inverse of *a* modulo *m*

The inverse of a modulo m does not always exist. Check b=1,2,3,4,and 5 to see if ba = 1 (mod 6) has a solution.

The following theorem guarantees that an inverse of *a* modulo *m* does exist whenever *a* and *m* are relatively prime. Two integers *a* and *b* are relatively prime when gcd(*a*,*b*) = 1.

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*. (This means that there is a unique positive integer $\bar{a}$ less than *m* that is an inverse of *a* modulo *m* and every other inverse of *a* modulo *m* is congruent to $\bar{a}$ modulo *m*.) so is $\bar{a} + km$ for some integer k.

Proof: Since gcd(*a*,*m*) = 1, by Theorem 6 of Section 4.3, there are integers *s* and *t* such that $sa + tm = 1$. It turns out that this s is an inverse of a modulo m.

- Hence, $sa = 1+(-t)m$
- it follows that $sa \equiv 1 \pmod{m}$
- Consequently, *s* is an inverse of *a* modulo *m*.
- The uniqueness of the inverse is Exercise 7.

Finding Inverses[1]

The Euclidean algorithm and Bézout coefficients gives us a systematic approaches to finding inverses of a modulo m when a and m are relatively prime

Example: Find an inverse of 3 modulo 7.

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

- Using the Euclidian algorithm: $7 = 2 \cdot 3 + 1$.
- From this equation, we get $-2 \cdot 3 + 1 \cdot 7 = 1$, and see that -2 and 1 are Bézout coefficients of 3 and 7. -2 is the coefficient on 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., 5, -9, 12, etc.

Finding Inverses 2

Example: Find an inverse of 101 modulo 4620.

Solution: First use the Euclidian algorithm to show that gcd(101,4620) = 1.

$4620 = 45 \cdot 101 + 75$

$101 = 1 \cdot 75 + 26$

$75 = 2 \cdot 26 + 23$

$26 = 1 \cdot 23 + 3$

$23 = 7 \cdot 3 + 2$

$3 = 1 \cdot 2 + 1$

$2 = 2 \cdot 1$

Since the last nonzero remainder is 1, gcd(101,4620) = 1

Bézout coefficients : − 35 and 1601

1601 is the coefficient on 101.

Working Backwards:

$1 = 3 - 1 \cdot 2$

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

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

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

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

$= 26 \cdot 101 - 35 \cdot 75$

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

$= -35 \cdot 4620 + 1601 \cdot 101$

1601 is an inverse of 101 modulo 4620

Using Inverses to Solve Congruences

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

Example: What are the solutions of the congruence $3x \equiv 4(\bmod 7)$.

Solution: We found that −2 is an inverse of 3 modulo 7 (two slides back). We multiply both sides of the congruence by −2 giving

$$-2 \cdot 3x \equiv -2 \cdot 4(\bmod 7).$$

Because $-6 \equiv 1 \pmod 7$ and $-8 \equiv 6 \pmod 7$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 \pmod 7$ 6 was chosen because that is the number in {0,1,2,3,4,5,6} that is congruent to -8 modulo 7.

We need to determine if every x with $x \equiv 6 \pmod 7$ is a solution. Assume that $x \equiv 6 \pmod 7$. By Theorem 5 of Section 4.1, it follows that $3x \equiv 3 \cdot 6 = 18 \equiv 4(\bmod 7)$ which shows that all such x satisfy the congruence.

The solutions are the integers x such that $x \equiv 6 \pmod 7$, namely, 6,13,20 … and −1, − 8, − 15,…