MATH 3336 - Discrete Mathematics
Solving Congruences (4.4)

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

Our goal is to solve the linear congruence $ax \equiv b(mod\ m)$, that is to find all integers x that satisfy this congruence.

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

Example: Show that 5 is inverse of 3 modulo 7.

Check $5 \cdot 3 \stackrel{?}{\equiv} 1 \pmod 7$

$15 \equiv 1 \pmod 7$ true

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

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

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. (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.)

Example: Find an inverse of 2 modulo 17.

Need to find $\bar{a}$ such that

$\bar{a} \cdot 2 \equiv 1 \pmod{17}$

$\bar{a} = 9$

$9 \cdot 2 = 18 \equiv 1 \pmod{17}$

The Euclidean algorithm and Bézout coefficients gives us a systematic approach to finding inverses.

Example: Find an inverse of 3 modulo 7.

$7 = 2 \cdot 3 + 1 \rightarrow 1 = 7 - 2 \cdot 3 \pmod 7$

$3 = 3 \cdot 1 + 0$ stop

$1 \equiv -2 \cdot 3 \pmod 7$

$\gcd(3,7) = 1$ $\quad -2$ is an inverse of 3 mod 7

$0 < 5 < 7$

Example: Find an inverse of 19 modulo 141.

$141 = 7 \cdot 19 + 8 \rightarrow 8 = 141 - 7 \cdot 19$

$19 = 2 \cdot 8 + 3 \rightarrow 3 = 19 - 2 \cdot 8$

$8 = 2 \cdot 3 + 2 \rightarrow 2 = 8 - 2 \cdot 3$

$3 = 1 \cdot 2 + 1 \rightarrow 1 = 3 - 1 \cdot 2$

$2 = 2 \cdot 1 + 0$ stop

$= 3 - 1(8 - 2 \cdot 3)$

$= 3 \cdot 3 - 1 \cdot 8$

$= 3(19 - 2 \cdot 8) - 1 \cdot 8$

$= 3 \cdot 19 - 7 \cdot 8$

$= 3 \cdot 19 - 7(141 - 7 \cdot 19)$

$= 52 \cdot 19 - 7 \cdot 141$

$1 = 52 \cdot 19 - 7 \cdot 141$

$\pmod{141}$

$1 \equiv 52 \cdot 19 \pmod{141}$

52 is an inverse of 19 modulo 141

Example: What is the solution of the linear congruence $3x \equiv 4 (mod\ 7)$?

1. Find an inverse of 3 modulo 7 (ans = 5)

2. $5 \cdot 3x \equiv 5 \cdot 4 \pmod 7$

$1 \cdot x \equiv 20 \pmod 7$

$x \equiv 6 \pmod 7$

3. $x = 6 + 7k \quad k \in \mathbb{Z}$

m

$0 < m <$ modulo

The Chinese Remainder 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:

$$x \equiv 2 \ (mod\ 3),$$
$$x \equiv 3 \ (mod\ 5),$$
$$x \equiv 2 \ (mod\ 7).$$

- We'll see how the theorem that is known as the *Chinese Remainder Theorem* can be used to solve Sun-Tsu's problem.

Theorem: (*The Chinese Remainder Theorem*) Let $m_1, m_2, \dots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \dots, a_n$ arbitrary integers. Then the system

$$x \equiv a_1 (mod\ m_1)$$
$$x \equiv a_2 (mod\ m_2)$$
$$\vdots$$
$$x \equiv a_n (mod\ m_n)$$

has a unique solution modulo $m = m_1\, m_2 \dots m_n$

(That is, there is a solution x with $0 \leq x < m$ and all other solutions are congruent modulo m to this solution.)

We construct a solution for 3 congruences, i.e. $n = 3$ from Sun-Tsu's problem. Solution for any n can be constructed in a similar way.

$$x \equiv 2\ (mod\ 3), \qquad x \equiv 3\ (mod\ 5), \qquad x \equiv 2\ (mod\ 7)$$

Step 1: $a_1 =$ 2, $a_2 =$ 3, $a_3 =$ 2, $m_1 =$ 3, $m_2 =$ 5, $m_3 =$ 7.

Step 2: Check that m_1, m_2, m_3 are pairwise relatively prime. YES or NO

Step 3: Compute $M_1 = m_2m_3$, $M_2 = m_1m_3$, $M_3 = m_1m_2$, $m = m_1m_2m_3$

$M_1 =$ 35, $M_2 =$ 21, $M_3 =$ 15, $m =$ 105.

Step 4: Find an inverse y_1 of M_1 modulo m_1. $y_1 =$ 2.

$y_1 \cdot 35 \equiv 1 \pmod 3$

Find an inverse y_2 of M_2 modulo m_2. $y_2 =$ 1.

$y_2 \cdot 21 \equiv 1 \pmod 5$

Find an inverse y_3 of M_3 modulo m_3. $y_1 =$ 1.

$y_3 \cdot 15 \equiv 1 \pmod 7$

Step 5: Compute $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$.

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

Step 6: Verify $x \equiv 2\ (mod\ 3)$, $x \equiv 3\ (mod\ 5)$, $x \equiv 2\ (mod\ 7)$.

$\equiv 23 \pmod{105}$

$23 \equiv 2 \pmod 3$ $\quad 23 \equiv 3 \pmod 5$

$23 \equiv 2 \pmod 7$

Try this one: Fifteen pirates steal a stack of identical gold coins. When they try to divide them evenly, two coins are left over. A fight erupts and one of the pirates is killed. The remaining pirates try again to evenly distribute the coins. This time there is one coin left over. A second pirate is killed in the resulting argument. Now when the remaining pirates try to divide the coins evenly there are no coins left over. Use the Chinese Remainder Theorem to find the smallest number of coins that could have been in the sack.

Theorem: (***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 $a^{p} \equiv a \pmod{p}$

Fermat's little theorem is useful in computing the remainders modulo p of large powers of integers.

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

$p = 11 \quad a = 7 \quad 7^{10} \equiv 1 \pmod{11}$

$7^{222} = (7^{10})^{22} \cdot 7^2$

$\equiv 7^2 \pmod{11}$

$\equiv 49 \pmod{11}$

$\equiv 5 \pmod{11}$