§ 4.4 Solving Congruences

Jessica Wei

Linear Congruence

DEF | Linear Congruence
A congruence of the form

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

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

Goal. Solve for x

Case 1: $a|b$

Q: if $a|b$, is the answer $x = \frac{b}{a} \mod m$?

Short Answer: Not always, i.e. $2 \cdot 7 \equiv 8 \mod 6 \neq 7 \equiv 4 \mod 6$

Long Answer...... (see below)

| Lemma 4.4.1 (4.3.2 in textbook)
Let $a, b, c \in \mathbb{Z}^+$. If $\gcd(a,\, b) = 1$, and $a|b \cdot c$, then $a|c$

PROOF

If $\gcd(a,\, b) = 1$, then $\exists s, t, \in \mathbb{Z}$ such that $a \cdot s \cdot c + t \cdot b \cdot c = c$.
Since $a|b \cot c$, $b \cdot c = a \cdot k$ for some $k \in \mathbb{Z}$.
Hence, $a \cdot s \cdot c + a \cdot k \cdot t = c \Rightarrow a(s \cdot c + k \cdot t) = c$ where $s \cdot c + k \cdot t \in \mathbb{Z}$
$\therefore a|c$

| THM 4.3.6
Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. If (1) $a \cdot c \equiv b \cdot a \mod m$ and (2) $\gcd(a,\, m) = 1$, then $c \equiv b \mod m$

PROOF

By (1), $a \cdot c - b \cdot a = m \cdot k \Rightarrow a(c - b) = m \cdot k$. Since $\gcd(a,\, m) = 1$ and $a|m \cdot k$, then by Lemma 4.4.1, $a|k$.

$\Rightarrow c - b = m(\frac{k}{a}$

$c - b = m \cdot q$ when $q = \frac{k}{a} \in \mathbb{Z}$

$c \equiv b \mod m$

Hence, (1) $a \cdot x \equiv b \mod m$ will have solution $x \equiv \frac{b}{a} \mod m$ if (2) $\gcd(a,\, m) = 1$.

Example 1. Solve $6 \cdot x \equiv 12 \mod 7$

Since $\gcd(6,\ 7) = 1$, then $x \equiv 2 \mod 7$

Answer: $x \equiv 2 \mod 7$

Goal. (con't) Solve for x

Case 2: $a \nmid b$

$$a \cdot x \equiv b \mod m$$

Idea: If we can find $\bar{a} \in \mathbb{Z}$ such that $\bar{a}a \equiv 1 \mod m$ then $\bar{a}ax \equiv x \mod m$.

$$x \equiv \bar{a}bc \mod m$$

| THM 4.4.1
If $\gcd(a,\ m) = 1$, $m > 1$, then there exists $\bar{a} \in \mathbb{Z}$ unique modulo m such that $\bar{a}a \equiv 1 \mod m$.

PROOF

Since $\gcd(a,\ m) = 1$, then $\exists s, t \in \mathbb{Z}$

$as + mt = 1$

$\Rightarrow (as + nt) - 1 = 0m$

$\Rightarrow as + mt \equiv 1 \mod m$

$\Rightarrow as + 0 \equiv 1 \mod m$

$\Rightarrow as \equiv 1 \mod m$ because $m|mt$

so $\bar{a}$ is actually the Bezout Coefficient of a with m.

Uniqueness Assume $\exists u \in \mathbb{Z} such that$

$ua \equiv 1 \mod m$

$ua\bar{a} \equiv \bar{a} \mod m \quad (a\bar{a} \equiv 1)$

$u \equiv \bar{a} \mod m$

So $\bar{a}$ is unique modulo m

Summarize

$ax \equiv b \mod m$

Requirement: $\gcd(a{,}m) = 1$

Case 1: If $a|b$, then $x = \frac{b}{a} \mod m$.

Case 2: If $a \nmid b$, then $x = \bar{a}b \mod m$ where $\bar{a}$ is the Bezout Coefficient(a.k.a. "inverse modulo m") of $\gcd(a,\ m)$.

Example 2. Find the inverse if possible.

(a) 3 modulo 7 = -2 $\equiv$ 5 $\quad (-2 \mod 7 = 5)$
$7 = 2 \cdot 3 + 1 \Rightarrow 1 = 7 - 2 \cdot 3$ where 2 is the Bezout Coefficient of 3
$3 = 3 \cdot 1 + 0$
Answer: 5

(b) 101 modulo 4620
$4620 = 45 \cdot 101 + 75 \Rightarrow 75 = 4620 - 45 \cdot 101$
$101 = 1 \cdot 75 + 26 \Rightarrow 26 = 101 - 75$
$75 = 2 \cdot 26 + 23 \Rightarrow 23 = 75 - 2 \cdot 26$
$26 = 1 \cdot 23 + 3 \Rightarrow 3 = 26 - 1 \cdot 23$
$23 = 7 \cdot 3 + 2 \Rightarrow 2 = 23 - 7 \cdot 3$
$3 = 1 \cdot 2 + 1 \quad \checkmark \quad \Rightarrow 1 = 3 - 2$
$2 = 2 \cdot 1 + 0$

$1 = 3 - 2 \Rightarrow 3 - (23 - 7 \cdot 3)$
$= (8 \cdot 3) - 23 \Rightarrow (8(26 - 23)) - 23$
$= 8 \cdot 26 - 9 \cdot 23 \Rightarrow 8 \cdot 26 - 9(75 - 2 \cdot 26)$
$= 26 \cdot 26 - 9 \cdot 75 \Rightarrow 26(101 - 75) - 9 \cdot 75$
$= 26 \cdot 101 - 35 \cdot 78 \Rightarrow 26 \cdot 101 - 35(4620 - 48 \cdot 101)$
$= 26 \cdot 101 - 35(4620) + 1575 \cdot 101 \Rightarrow 1601 \cdot 101 - 35 \cdot 4620$
Answer: $\bar{a} = 1601$

Example 3. Solve $3x \equiv 4 \mod 7$

* gcd(3, 7) = 1 $\quad \checkmark$

* inverse of 3 modulo 7 = 5

$\Rightarrow 5 \cdot 3x \equiv 5 \cdot 4 \mod 7$

$\Rightarrow x \equiv 20 \mod 7$

$x \equiv 6 \mod 7$

$x - 6 = 7k$ where $k \in \mathbb{Z}$

Answer: $x = 7k + 6$

Check

$k = 0 \quad x = 6 \quad 3 \cdot 6 \stackrel{?}{=} 4 \mod 7 \quad \checkmark$

$k = 1 \quad x = 13 \quad 3 \cdot 13 \stackrel{?}{=} 4 \mod 7 \quad \checkmark$

Goal. Solve a system of linear congruences.

$x \equiv a_1 \mod m_1$

$x \equiv a_2 \mod m_2$

$x \equiv a_3 \mod m_3$

OR more compactly...
$x \equiv a_i \mod m_i$ where $i = 1, 2, 3....n$

| Chinese Remainder THM
The system

$$x \equiv a_i \mod m \qquad i = 1, ..., n$$

has a unique solution modulo $m = m_1 \cdot m_2 \cdot ...m_n$ provided that:

(i) $\gcd(m_i, m_j) = 1 \quad i \neq j$

(ii) $m_i > 1$

PROOF

Existence: For m $M_k = \frac{m}{m_k} = m_1 \cdot m_2 ... m_{k-1} \cdot m_{k+1} ... m_n$ (Notice that m_k is missing)

Then $\gcd(M_k, m_k) = 1$ i.e. they will be relatively prime.

By THM 4.4.1, $\exists \bar{M}_k \in \mathbb{Z}$ such that $\bar{M}_k M_k \equiv 1 \mod M_k$. We claim that $x = a_1 M_1 \bar{M}_1 + a_2 M_2 \bar{M}_2 + ... a_n M_n \bar{M}_n$ solves the system.

To show that this is true, notice that for any $j = 1, ...n$: $M_j \equiv 0 \mod M_k$ for $j \neq k$

This is because $M_j = m_1 m_2 ... m_{j-1} m_{j+1} ... m_k m_{k+1} ... m_n$

So $m_k | M_j$. Then... (anything M_k is going away [$= 0$])

$x = a_1 M_1 \bar{M}_1 + ... + a_1 M_k \bar{M}_k + ... a_n M_n \bar{M}_n \equiv 0 + 0 + ... + a_1 M_k \bar{M}_k + 0 ... + 0 \mod m_k$

$\Rightarrow x = a_k M_k \bar{M}_k \mod M_k$

$\Rightarrow x = a_x \cdot 1 \mod m_k$

$\Rightarrow x = a_x \mod m_k$

This is true for any $k = 1, 2, ...n$

Hence $x = a_1 M_1 \bar{M}_1 + a_2 M_2 \bar{M}_2 + ... a_n M_n \bar{M}_n$ solves the system.

Example 1. Solve

$$x \equiv 2 \mod 3$$
$$x \equiv 3 \mod 5$$
$$x \equiv 2 \mod 7$$

with the Chinese Remainder Theorem

*$m_1 = 3, m_2 = 5, m_3 = 7, m = 3 \cdot 5 \cdot 7 = 105$

*$M_1 = 5 \cdot 7 = 35, M_2 = 3 \cdot 7 = 21, M_3 = 3 \cdot 5 = 15$

*Need $\bar{M_1} \cdot 35 \equiv 1 \mod 3 \Rightarrow 2$, $\bar{M_2} \cdot 21 \equiv 1 \mod 5 \Rightarrow 1$, $\bar{M_3} \cdot 15 \equiv 1 \mod 7 \Rightarrow 1$

$x = a_1 M_1 \bar{M_1} + a_2 M_2 \bar{M_2} + a_3 M_3 \bar{M_3}$

$=2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 140 + 63 + 30 = 233 \equiv ? \mod 105$ where $? = 23$

$\Rightarrow x \equiv 23 \mod 105 \Rightarrow x - 23 = 105k \quad k \in \mathbb{Z}$

Answer: $x = 105k + 23$

Example 2. Solve

$$x \equiv 2 \mod 3 \quad (1)$$
$$x \equiv 3 \mod 5 \quad (2)$$
$$x \equiv 2 \mod 7 \quad (3)$$

with substitution

(1) $\quad x - 2 = 3k \quad k \in \mathbb{Z} \Rightarrow x = 3k + 2 \quad (A)$

Plug (A) into (2).

$3k + 2 \equiv 3 \mod 5 \Rightarrow mk \equiv 1 \mod 5 \qquad 3\bar{a} \equiv 1 \mod 5$ where $\bar{a} \equiv 2$

$2 \cdot 3k \equiv 2 \cdot 1 \mod 5 \Rightarrow k \equiv 2 \mod 5$

$k - 2 = 5q \quad q \in \mathbb{Z} \Rightarrow k = 5q + 2 \quad (B)$

Plug (B) into (A) – This results in an x that solves (1) and (2).

$x = 3k + 2 = 3(5q + 2) + 2 \Rightarrow x = 15q + 8 \quad (C)$

Plug (C) into (3).

$15q + 8 \equiv 2 \mod 7$

$15q \equiv -2 \mod 7$

$15q \equiv 1 \mod 7$ where $\bar{a}15 \equiv 1 \mod 7$, $\bar{a} \equiv 1$

$1 \cdot 15q \equiv 1 \cdot 1 \mod 7$

$q = 1 \mod 7 \Rightarrow q = 7u + 1 \quad (D)$

Plug (D) into (C) to obtain an x that satisfies the whole system.

$x = 15(7u + 1) + 8 = 105u + 15 + 8$

Answer: $x = 105u + 23$

Fermat's Little Theorem & Modular Exponentiation

| THM 4.4.2
If p is prime & $p \nmid a$ then...

(i) $a^{p-1} \equiv 1 \mod p$

(ii) $a^p \equiv a \mod p$

Example 3. Find each of the following
a) $7^{222} \mod 11 =? \mod m$
*Idea: Recall $a \mod m = b \mod m$ if and only if $a \equiv b \mod m$. We will reduce 7^{222} into a smaller number b modulo m. i.e. $7^{222} \equiv ?smaller \mod 11$
Notice 11 is prime & $p = 11 \nmid 7$
Hence, by FLT...

$$7^{11-1} \equiv 1 \mod 11 \Rightarrow 7^{10} \equiv 1 \mod 11$$

*Claim: If $a = b \mod m$. then $a^k = b^k \mod m$ for $k \in \mathbb{Z}^+$
*Proof: $(7^{10})^{21} \equiv 1^{20} \mod 11$
$7^{222} = 1 \mod 11 \Rightarrow 7^2 \cdot 7^{200} = 7^2 \cdot 1 \mod 11$
$7^{222} \equiv 7^2 \mod 11 \Rightarrow 7^{222} \mod 11 \equiv 7^2 \mod 11 = 49 \mod 11$
Answer: $5 \mod 11$

b) $7^{121} \mod 13 =? \mod 13$
*Goal: $7^{121} =? \mod 13$, $p = 13$, $13 \nmid 7$
$\Rightarrow 7^{13-1} \equiv 1 \mod 13$ by FLT
$\Rightarrow (7^{12})^{10} \equiv 1^{10} \mod 13$
$7 \cdot 7^{120} \equiv 1 \cdot 7 \mod 13$
$7^{121} = 7 \mod 13$
$\Rightarrow 7^{121} \mod 13 = 7 \mod 13$
Answer: 7