SOLVING CONGRUENCE

LINEAR CONGRUENCE

- Goal: Solve $ax = b(\mathrm{mod}\ m)$ where $a, b \in \mathbb{Z}$
- Ideal 1: In algebra, $\frac{ax}{a} = \frac{b}{a} \rightarrow x = \frac{b}{a}$
- Does it work to say that $x = \frac{b}{a}(\mathrm{mod}\ m)$ at least when $a|b$?
- i.e. If $ax = b(\mathrm{mod}\ m)$ is it true that $x = \frac{b}{a}(\mathrm{mod}\ m)$?
- Consider $14 \equiv 8(mod\ 6)$
- $2 \times 7 \equiv 8(\mathrm{mod}\ 6) \rightarrow 7 \not\equiv 8(\mathrm{mod}\ 6)$
- Hence, we cannot take an algebraic approach

LEMMA 4.4.1

- Let $a, b, c \in \mathbb{Z}^+$. If $\gcd(a, b) = 1$ and $a|bc$ then $a|c$
- Proof:
- Since $\gcd(a, b) = 1, \exists s, t \in \mathbb{Z}$ such that $as + bt = 1$

$$as + bt = 1$$

$$asc + bct = c$$

- Since $a|bc$ then $\exists q \in \mathbb{Z}$ such that $bc = qa$
- So then $asc + qat = c \rightarrow a(sc + qt) = c \rightarrow a \times k = c$ where $k = sc + qt \in \mathbb{Z}$
- So then $a|c$

THEOREM 4.4.1

- Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$
- If (i) $ac \equiv bc(mod\ m)$ and (ii) $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$
- i.e. You can divide both sides of the congruence by c if it is relatively prime with m

INVERSE MODULO M

- Definition: $\bar{a}$ is called the inverse of a modulo m if $\bar{a} = 1 (\mathrm{mod}\ m)$

THEOREM 4.4.2

- $\bar{a}$ is called the inverse of a modulo m if $\gcd(a, m) = 1$ and $m > 1$ then $\exists k \in \mathbb{Z}^{\mathbb{Z}}$ such that $\bar{a}a - a = mk$
- And $\bar{a}$ is unique modulo m

PROOF FOR EXISTENCE OF THEOREM 4.4.2

- Since $\gcd(a, m) = 1$ then $\exists s, t \in \mathbb{Z}$ such that $as + mt = 1 \rightarrow as - 1$
- WTS: $\exists k \in \mathbb{Z}^{\mathbb{Z}}$ such that $\bar{a}a - a = mk$
- In Bezout ID we can rearrange the terms:
- $as - 1 = -mt \rightarrow as - 1 = m(-t) \rightarrow as - 1 = mk$ where $k = -t \in \mathbb{Z}$
- So then $as = 1 (\text{mod } m)$
- i.e. The inverse of a is its Bezout coefficient

PROOF FOR UNIQUENESS OF THEOREM 4.4.2

- Assume that $\bar{a}(s)$ is not unique modulo m. Then there must $\exists w \in \mathbb{Z}$ such that $aw = 1(mod\ m)$ as well as $s \neq w \pmod m$
- Since $as = 1 \pmod m$ and $1 = aw(mod\ m)$ then $as = aw(mod\ m)$ by Lemma 4.4.1
- Also since $\gcd(a, m) = 1$ then $\frac{1s}{a} = \frac{aw}{a} \pmod m$ by Theorem 4.4.1
- So then $s \equiv w \pmod m$
- A contradiction, therefore s must be unique modulo m

EXAMPLE 1

- Find the inverse of each of the following:
- $3 (mod\ 7)$
  - Check $\gcd(3,7) = 1$
  - Want: Bezout coefficient of 3
  - $7 = 2 \times 3 + 1 \rightarrow 1 = 7 - 2 \times 3 \rightarrow 3 = 3 \times 1 + 0 \rightarrow s = -2, \bar{a} = -2$
- $101 (mod\ 4620)$
  - Check gcd(101, 4620)=1
  - $1 = 1607 \times 101 - 35 \times 4620 \rightarrow \bar{a} = 1607$

EXAMPLE 2

- Solve the following:
- $3x \equiv 7(mod\ 7)$
  - $\gcd(3,7) = 1 \rightarrow 5 \cdot 3 - 2 \cdot 7 = 1 \rightarrow \overline{3}(mod\ 7) = 5$
  - $x \equiv 5 \cdot 7(mod\ 7) \equiv 35(mod\ 7) = 0$
- $19x \equiv 4\ (mod\ 144)$
  - $\gcd(19,144) = 1 \rightarrow 7 \cdot 144 - 53 \cdot 19 = 1 \rightarrow \overline{19}(mod\ 144) = -53$
  - $x \equiv -53 \cdot 4(mod\ 144) \equiv -212(mod\ 144) = 76$

SOLVING SYSTEMS OF CONGRUENCES

- Goal: Solve
- $x = 2(mod\ 3)$
- $x = 3(mod\ 5)$
- $x = 2(mod\ 7)$
- i.e. find x such that is satisfies each congruences

THEOREM 4.4.3: CHINESE REMAINDER THEOREM

- Let $(m_1, m_2, \ldots, m_n)$ satisfy
- $\gcd(m_i, m_j) = 1$ if $i \neq j$ (i.e. the $m_i's$ are relatively prime
- $m_i > 1$, where $i = 1,2, \ldots, n$
- Then,

$$x = a_1 (mod\ m_1)$$
$$x = a_2 (mod\ m_2)$$
$$\ldots$$
$$x = a_n (mod\ m_n)$$

Has a unique solution modulo $\mathrm{m} = \mathrm{m}_1, \mathrm{m}_2, \ldots, \mathrm{m}_\mathrm{n}$

EXAMPLE 3

- Solve
- $x = 2(mod\ 3)$
- $x = 3(mod\ 5)$
- $x = 2(mod\ 7)$
- $\gcd(3,5) = \gcd(3,7) = \gcd(5,7) = 1$ and $m_1 = 3, m_2 = 5, m_3 = 7 > 1$
- By Chinese remainder theorem: $x = a_1 m_1 \overline{m_1} + a_2 m_2 \overline{m_2} + a_3 m_3 \overline{m_3}$
- $x = 2 \cdot 5 \cdot 7 +$

SOLVING CONGRUENCE

EXAMPLE 2

- Solve the following:
- $3x \equiv 7(mod\ 7)$
  - $\gcd(3,7) = 1 \rightarrow 5 \cdot 3 - 2 \cdot 7 = 1 \rightarrow \bar{3}(mod\ 7) = 5$
  - $x \equiv 5 \cdot 7(mod\ 7) \equiv 35(mod\ 7) = 0$
- $19x \equiv 4\ (mod\ 144)$
  - $\gcd(19,144) = 1 \rightarrow 7 \cdot 144 - 53 \cdot 19 = 1 \rightarrow \overline{19}(mod\ 144) = -53$
  - $x \equiv -53 \cdot 4(mod\ 144) \equiv -212(mod\ 144) = 76$

SOLVING SYSTEMS OF CONGRUENCES

- Goal: Solve
- $x = 2(mod\ 3)$
- $x = 3(mod\ 5)$
- $x = 2(mod\ 7)$
- i.e. find x such that is satisfies each congruences

THEOREM 4.4.3: CHINESE REMAINDER THEOREM

- Let $(m_1, m_2, \dots, m_n)$ satisfy
- $\gcd(m_i, m_j) = 1$ if $i \neq j$ (i.e. the $m_i's$ are relatively prime
- $m_i > 1$, where $i = 1,2, \dots, n$
- Then,

$$x = a_1 (mod\ m_1)$$
$$x = a_2 (mod\ m_2)$$
$$\dots$$
$$x = a_n (mod\ m_n)$$

Has a unique solution modulo $\mathrm{m} = \mathrm{m}_1 * \mathrm{m}_2 * \cdots * \mathrm{m}_\mathrm{n}$

CLAIM FROM CHINESE REMAINDER THEOREM

- The solution to the system of equations is:

$$x = a_1 * m_1 * \bar{m}_1 + a_2 * m_2 * \bar{m}_2 + \cdots + a_n * m_n * \bar{m}_n$$

EXAMPLE 3

- Solve
- $x = 2(mod\ 3)$
- $x = 3(mod\ 5)$
- $x = 2(mod\ 7)$
- $\gcd(3,5) = \gcd(3,7) = \gcd(5,7) = 1$ and $m_1 = 3, m_2 = 5, m_3 = 7 > 1$
- By Chinese remainder theorem: $x = a_1 m_1 \overline{m_1} + a_2 m_2 \overline{m_2} + a_3 m_3 \overline{m_3}$
- where $a_1 = 2, a_2 = 3, a_3 = 2$ and $M1 = 5 * 7 = 35, M2 = 3 * 7 = 21, M3 = 3 * 5 = 15$

EXAMPLE 3 (CONTINUED)

- $\bar{m}_1 * 35 = 1(mod\ 3) \rightarrow \bar{m}_1 = 2$
- $\bar{m}_2 * 21 = 1(mod\ 5) \rightarrow \bar{m}_2 = 1$
- $\bar{m}_3 * 15 = 1(mod\ 7) \rightarrow \bar{m}_3 = 1$
- So then,
- $x = 2 * 35 * 2 + 3 * 21 * 1 + 2 * 15 * 1 = 233$
- $x = 233(mod\ m) = 233(mod\ 105) = 23(mod\ 105) = 105k + 23$