Ch 4.4: Solving Congruences

ICS 141: Discrete Mathematics for Computer Science I

KYLE BERNEY
DEPARTMENT OF ICS, UNIVERSITY OF HAWAII AT MANOA

Linear Congruences

- Let $m \in \mathbb{Z}^+$ and $a, b, x \in \mathbb{Z}$
- A linear congruence is a congruence of the form:

$$ax \equiv b \pmod{m}$$

- Ex: $a = 5$, $b = 3$, and $m = 8$

$$5x \equiv 3 \pmod{8}$$

  - $x = \ldots, -17, -9, -1, 7, 15, 23, 31, \ldots$

Linear Congruences

- Let $m \in \mathbb{Z}^+$ and $a, b, x \in \mathbb{Z}$
- A linear congruence is a congruence of the form:

$$ax \equiv b \pmod{m}$$

- Ex: $a = 5$, $b = 3$, and $m = 8$

$$5x \equiv 3 \pmod{8}$$

  - $x = \ldots, -17, -9, -1, 7, 15, 23, 31, \ldots$
- *Observation:* If we can find a solution x to the linear congruence, then we can find infinitely many others
  - All of the above solutions of x are congruent to each other modulo m

Linear Congruences

- Let $m \in \mathbb{Z}^+$ and $a, b, x \in \mathbb{Z}$
- A linear congruence is a congruence of the form:

$$ax \equiv b \pmod{m}$$

- Ex: $a = 5$, $b = 3$, and $m = 8$

$$5x \equiv 3 \pmod{8}$$

  - $x = \ldots, -17, -9, -1, 7, 15, 23, 31, \ldots$

- *Question:* How many mutually incongruent solutions are there?

Linear Congruences

- From Theorem 3 in the lecture slides of Chapter 4.1

  $$ax \equiv b \pmod{m} \Leftrightarrow ax = b + km$$

  for some integer k

- From Corollary 1 in the lecture slides of Chapter 4.3, in order that there exists integers x and $-k$ satisfying the equation

  $$ax + (-k)m = b$$

  it is necessary and sufficient that $d \mid b$, where $d = \texttt{GCD}(a, m)$

Linear Congruences

- For ease of exposition, let us consider the linear combination

$$ax + by = c$$

- Using Theorem 2 from the lecture notes of Chapter 4.3, and the Extended Euclidean Algorithm, we can find w and z such that

$$aw + bz = d$$

  where $d = \text{GCD}(a, b)$

Linear Congruences

- If $d \mid c$, then there exists an integer k such that

$$c = dk$$

- We have that $x_0 = wk$ and $y_0 = zk$ is a solution to

$$ax + by = c$$

since,

$$aw + bz = d$$

$$\Rightarrow awk + bzk = dk$$

$$\Rightarrow ax_0 + by_0 = c$$

Linear Congruences

- Suppose that x' and y' are also a solution to $ax + by = c$

$$ax' + by' = c = ax_0 + by_0$$

- Recall that $c = dk$, hence

$$\begin{aligned} \frac{a}{d}x' + \frac{b}{d}y' &= \frac{a}{d}x_0 + \frac{b}{d}y_0 \\ \Rightarrow \frac{a}{d}x' - \frac{a}{d}x_0 &= \frac{b}{d}y_0 - \frac{b}{d}y' \\ \Rightarrow \frac{a}{d}\left(x' - x_0\right) &= \frac{b}{d}\left(y_0 - y'\right) \end{aligned}$$

Linear Congruences

$$\frac{a}{d}\left(x' - x_0\right) = \frac{b}{d}\left(y_0 - y'\right)$$

- By definition of divisibility, it follows from the above equation that

$$\frac{b}{d} \,\Big|\, \frac{a}{d}(x' - x_0)$$

- From Corollary 2 in the lecture slides of Chapter 4.3,

$$\text{GCD}(a/d, b/d) = 1$$

- Therefore, from Lemma 2 in the lecture slides of Chapter 4.3,

$$\frac{b}{d} \,\Big|\, (x' - x_0)$$

Linear Congruences

- By definition of divisibility, there exists an integer t such that

$$x' - x_0 = t \cdot \frac{b}{d}$$

- Thus,

$$\begin{aligned} \frac{a}{d}(x' - x_0) &= \frac{b}{d}(y_0 - y') \\ \Rightarrow \frac{a}{d} \cdot t \cdot \frac{b}{d} &= \frac{b}{d}(y_0 - y') \\ \Rightarrow \frac{a}{d} \cdot t &= y_0 - y' \\ \Rightarrow y' &= y_0 - t \cdot \frac{a}{d} \end{aligned}$$

Linear Congruences

- Therefore, there exists an integer t such that

$$x' = x_0 + t \cdot \frac{b}{d}$$

$$\text{and} \quad y' = y_0 - t \cdot \frac{a}{d}$$

- Furthermore, for all integers t, x' and y' are valid solutions to the linear combination $ax' + by' = c$ since

$$\begin{aligned} ax' + by' &= a\left(x_0 + t \cdot \frac{b}{d}\right) + b\left(y_0 - t \cdot \frac{a}{d}\right) \\ &= ax_0 + by_0 + t \cdot \frac{ab}{d} - t \cdot \frac{ab}{d} \\ &= c \end{aligned}$$

Linear Congruences

- Theorem 1: The linear combination

$$ax + by = c$$

has a solution if and only if $d \mid c$, where $d = \text{GCD}(a, b)$. Furthermore, if x_0 and y_0 are solutions to this equation, then the set of solutions consists of all integer pairs such that

$$x = x_0 + t \cdot \frac{b}{d} \quad \text{and} \quad y = y_0 - t \cdot \frac{a}{d}$$

for all integers t.

Linear Congruences

- Theorem 2: Let $d = \text{GCD}(a, m)$. The linear congruence

$$ax \equiv b \pmod{m}$$

  has no solution if $d \nmid b$ and it has d mutually incongruent solutions if $d \mid b$

- Ex: Since $\text{GCD}(15, 12) = 3$ and $3 \mid 9$, the linear congruence

$$15x \equiv 9 \pmod{12}$$

  has exactly 3 mutually incongruent solutions
  - By inspection, we find $x = 3$ is a valid solution
  - For $t = 0, 1, 2$ we obtain 3 mutually incongruent solutions given by

$$x = 3 + t \cdot \frac{12}{3} = 3 + 4t$$

Linear Congruences

- Definition: We say that a solution x of a linear congruence $ax \equiv b \pmod{m}$ is unique modulo m if any solution x' is congruent to $x \pmod{m}$
- Definition: If $a\overline{a} \equiv 1 \pmod{m}$, then $\overline{a}$ is the inverse of a modulo m.

Linear Congruences

- Corollary 1: If $\texttt{GCD}(a, m) = 1$, then a has an inverse and it is unique modulo m.

Linear Congruences

- Corollary 1: If $\text{GCD}(a, m) = 1$, then a has an inverse and it is unique modulo m.

- Proof: Since $\text{GCD}(a, m) = 1$, it follows from Theorem 2 that
$$ax \equiv 1 \pmod{m}$$
has a single mutually incongruent solution, i.e., it is unique modulo m.

Systems of Linear Congruences

- A solution to the system of k linear congruences

$$\begin{aligned} a_1x &\equiv b_1 \pmod{m} \\ a_2x &\equiv b_2 \pmod{m} \\ &\vdots \\ a_kx &\equiv b_k \pmod{m} \end{aligned}$$

  is an integer x that satisfies each of the congruences in the system

Systems of Linear Congruences

- The simplest examples of such problems occurs in the solution of a single linear congruence with a large modulus
- Let m have a prime factorization

$$m = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

- It follows from the Fundamental Theorem of Arithmetic that

$$a \equiv b \pmod{m}$$

  if and only if

$$\begin{aligned} a &\equiv b \pmod{p_1^{e_1}} \\ a &\equiv b \pmod{p_2^{e_2}} \\ &\vdots \\ a &\equiv b \pmod{p_k^{e_k}} \end{aligned}$$

Systems of Linear Congruences

- Ex: Solve the linear congruence

$$3x \equiv 11 \pmod{2275}$$

  - Prime factorization: $2275 = 5^2 \cdot 7 \cdot 13$
  - Need to solve the following system of linear congruences

$$3x \equiv 11 \pmod{25}$$
$$3x \equiv 11 \pmod{7}$$
$$3x \equiv 11 \pmod{13}$$

- To solve this system linear congruences, we need the following Theorem

Chinese Remainder Theorem

- Theorem 3: (Chinese Remainder Theorem) Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers and let $a_1, a_2, \ldots, a_k$ be arbitrary integers such that $\texttt{GCD}(a_i, m_i) = 1$. The system of linear congruences

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ a_2 x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ a_k x &\equiv b_k \pmod{m_k} \end{aligned}$$

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

Chinese Remainder Theorem

- Proof: From Theorem 2, there exists a unique solution c_i for each of the k linear congruences such that

$$a_i c_i \equiv b_i \pmod{m_i}$$

Let $n_i = m/m_i = m_1 \ldots m_{i-1} m_{i+1} \ldots m_k$. Since all m_i's are relatively prime, $\text{GCD}(n_i, m_i) = 1$. Thus, from Corollary 1, n_i has an inverse modulo m_i

$$n_i \overline{n_i} \equiv 1 \pmod{m_i}$$

Chinese Remainder Theorem

- Proof: Consider

$$x_0 = c_1 n_1 \overline{n_1} + c_2 n_2 \overline{n_2} + \ldots + c_k n_k \overline{n_k}$$

Notice that m_i divides each n_j except for n_i. Thus,

$$\begin{aligned} a_i x_0 &= a_i c_1 n_1 \overline{n_1} + a_i c_2 n_2 \overline{n_2} + \ldots + a_i c_k n_k \overline{n_k} \\ &\equiv a_i c_i n_i \overline{n_i} \pmod{m_i} \\ &\equiv a_i c_i \pmod{m_i} \\ &\equiv b_i \pmod{m_i} \end{aligned}$$

Hence, x_0 is a solution to each of the k linear congruences in the system. This shows the existance of a solution.

Chinese Remainder Theorem

- Proof: Next, we will show uniqueness of the solution modulo m. Assume that y is also a solution to the k linear congruences in the system. From Theorem 2,

$$x_0 \equiv c_i \equiv y \pmod{m_i}$$

Hence, from Theorem 3 in the lecture slides of Chapter 4.1,

$$m_i \mid (x_0 - y)$$

for each m_i. Since all m_i's are pairwise relatively prime, i.e., they do not share a common factor,

$$m_1 m_2 \ldots m_k \mid (x_0 - y)$$
$$\Rightarrow m \mid (x_0 - y)$$

Therefore, $y \equiv x_0 \pmod{m}$ and x_0 is unique modulo m. ■

Chinese Remainder Theorem

- Ex:
$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$
- $a_1 = a_2 = a_3 = 1$
- $c_1 = 2,\ c_2 = 3,\ c_3 = 2$
- $m_1 = 3,\ m_2 = 5,\ m_3 = 7$
- $m = 3 \cdot 5 \cdot 7 = 105$
- $n_1 = 105/3 = 35,\ n_2 = 105/5 = 21,\ n_3 = 105/7 = 15$
- $\overline{n_1} = 2,\ \overline{n_2} = 1,\ \overline{n_3} = 1$

$$\begin{aligned} x_0 &= c_1 n_1 \overline{n_1} + c_2 n_2 \overline{n_2} + c_3 n_3 \overline{n_3} \\ &= (2 \cdot 35 \cdot 2) + (3 \cdot 21 \cdot 1) + (2 \cdot 15 \cdot 1) \\ &= 140 + 63 + 30 = 233 \\ &\equiv 23 \pmod{105} \end{aligned}$$

Chinese Remainder Theorem

- <u>Ex:</u>

$$3x \equiv 11 \pmod{25}$$
$$3x \equiv 11 \pmod{7}$$
$$3x \equiv 11 \pmod{13}$$

- $a_1 = a_2 = a_3 = 3$
- By inspection, we find that
  - $x \equiv 12 \pmod{25}$
  - $x \equiv 6 \pmod{7}$
  - $x \equiv 8 \pmod{13}$
- $c_1 = 12$, $c_2 = 6$, $c_3 = 8$
- $n_1 = 2275/25 = 91$, $n_2 = 2275/7 = 325$, $n_3 = 2275/13 = 175$

Chinese Remainder Theorem

- Ex:
$$3x \equiv 11 \pmod{25}$$
$$3x \equiv 11 \pmod{7}$$
$$3x \equiv 11 \pmod{13}$$
- Need to solve the following
$$91\overline{n_1} \equiv 16\overline{n_1} \equiv 1 \pmod{25}$$
$$325\overline{n_2} \equiv 3\overline{n_2} \equiv 1 \pmod{7}$$
$$175\overline{n_3} \equiv 6\overline{n_3} \equiv 1 \pmod{13}$$
- By inspection, we find
  - $\overline{n_1} = 11$
  - $\overline{n_2} = 5$
  - $\overline{n_3} = 11$

Chinese Remainder Theorem

- Ex:

$$3x \equiv 11 \pmod{25}$$
$$3x \equiv 11 \pmod{7}$$
$$3x \equiv 11 \pmod{13}$$

- $m = 25 \cdot 7 \cdot 13 = 2275$
- $c_1 = 12,\ c_2 = 6,\ c_3 = 8$
- $n_1 = 2275/25 = 91,\ n_2 = 2275/7 = 325,\ n_3 = 175$
- $\overline{n_1} = 11,\ \overline{n_2} = 5,\ \overline{n_3} = 11$

$$\begin{aligned} x_0 &= c_1 n_1 \overline{n_1} + c_2 n_2 \overline{n_2} + c_3 n_3 \overline{n_3} \\ &= (12 \cdot 91 \cdot 11) + (6 \cdot 325 \cdot 5) + (8 \cdot 175 \cdot 11) \\ &= 12012 + 9750 + 15400 = 37162 \\ &\equiv 762 \pmod{2275} \end{aligned}$$

Fermat's Little Theorem

- Theorem 4: (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

$$a^p \equiv a \pmod{p}$$

Fermat's Little Theorem

- Theorem 4: (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

$$a^p \equiv a \pmod{p}$$

- Proof: Out-of-scope of this course (requires knowledge of reduced residue systems and results related to Euler's ϕ function)