BLG501E – Discrete Mathematics

2021 – 2022 Fall Term

Asst. Prof. Gökhan SEÇİNTİ

Outline

- Congruences
- Linear Diophantine Equations
- Solving Linear Congruence
- The Chinese Remainder Theorem

Dividing Congruences by an Integer

- Dividing both sides of a valid congruence by an integer does not always produce a valid congruence (see Section 4.1).
- But dividing by an integer relatively prime to the modulus does produce a valid congruence:

Theorem 7: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = 1$, then $a \equiv b \pmod{m}$.

Proof: Since $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$ by Lemma 2 and the fact that $\gcd(c,m) = 1$, it follows that $m \mid a - b$. Hence, $a \equiv b \pmod{m}$.

◄

Dividing Congruences by an Integer (cont'd)

Theorem 7b: Let m be a positive integer and let *a*, *b*, and *c* be integers. If $ac \equiv bc$ (mod m) and gcd(c,m) = i, then $a \equiv b \pmod{m/i}$.

Proof:

Part 1, Lemma: $\gcd(m, c) = i \Rightarrow k = \frac{m}{i} \wedge l = \frac{c}{i} \Rightarrow k \perp l$

Proof: Assume $\gcd(k, l) = u \wedge u > 1$ then, $k = uk' \wedge l = ul'$

$$\Rightarrow k' = \frac{k}{u} = \frac{m}{ui} \wedge l' = \frac{l}{u} = \frac{c}{ui}$$

$$\Rightarrow cd(m, c) = ui \wedge \gcd(m, c) = i$$
$$\Rightarrow \mathrm{u} = 1$$

Dividing Congruences by an Integer (cont'd)

Theorem 7b: Let m be a positive integer and let *a*, *b*, and *c* be integers. If $ac \equiv bc$ (mod m) and gcd(c,m) = i, then $a \equiv b$ (mod m/i).

Proof:

Part 2: $\gcd(k, l) = 1 \wedge k = \frac{m}{i} \wedge l = \frac{c}{i} \wedge \gcd(m, c) = i$

Proof: $ac \equiv bc(modm) \Rightarrow m \mid (ac - bc) \Rightarrow m \mid (a - b)c$

$$ki|il(a - b) \Rightarrow qki = il(a - b) \Rightarrow qk|l(a - b)$$

$$\Rightarrow k|l\ (a - b)$$

We know $k \perp l$

Definition of modulo

$$k|l\ (a - b) \wedge k \perp l \Rightarrow k|a - b \Rightarrow a \equiv b\ modk$$

◀

Dividing Congruences by an Integer (cont'd)

Examples:

$a.\quad 40 \equiv 25\, mod\ 3$

$b.\quad 14 \equiv 8\, mod\ 6$

a. $\frac{40}{5} \equiv \frac{25}{5} mod\ 3 \Rightarrow 8 \equiv 5\, mod 3$

b. $14 \equiv 8\, mod\ 6\ \ \Rightarrow 7 \equiv 5\, mod 3$

Linear Diophantine Equations

$$ax + by = c\,; \qquad a, \mathrm{b}, \mathrm{c} \in I \wedge x, y \in I$$

integer solutions are sought for unknowns *x* and *y.*

i) Solution for special condition, where $\gcd(a, b) = 1$

$$\gcd(a, b) = 1 \Rightarrow as + bt = 1$$
$$\Rightarrow asc + btc = c$$

$$\boxed{x_0 = sc\,, y_0 = tc}$$

Other solutions:

$$ax_0 + by_0 = ax + by$$
$$a(x - x_0) = b(y_0 - y)$$

$$a|b(y_0 - y) \wedge \gcd(a, b) = 1 \Rightarrow a|(y_0 - y) \Rightarrow y_0 - y = ak$$
$$b|a(x - x_0) \wedge \gcd(a, b) = 1 \Rightarrow b|(x - x_0) \Rightarrow x - x_0 = bk$$

$$x = bk + x_0, y = y_0 - ak$$

$$\boxed{x = bk + sc, y = tc - ak}$$

Linear Diophantine Equations

$$ax + by = c\,; \qquad a, \mathrm{b}, \mathrm{c} \in I \wedge x, y \in I$$

integer solutions are sought for unknowns *x* and *y.*

ii) Other cases, where $\gcd(a, b) = d > 1$

Theorem: $ax + by = c$ have solution(s) iff $\gcd(a, b) = d \wedge d|c$

Proof:

$$d|c \Rightarrow c = ld \Rightarrow l = \frac{c}{d}$$
$$\gcd(\mathrm{a}, \mathrm{b}) = \mathrm{d} \Rightarrow \mathrm{as} + \mathrm{bt} = \mathrm{d}$$
$$asl + btl = dl = c$$
$$ax_0 + by_0 = c$$

Initial solution exists.

$$x_0 = sl\,, y_0 = tl$$

If (x_0, y_0) is a solution then $d|c$

Bezout's Theorem

$$ax_0 + by_0 = c \wedge \gcd(a, b) = d$$

$as + bt = d \wedge d$,divides every linear combinaton of a and b. => d|c

Linear Diophantine Equations

$$ax + by = c\;; \qquad a, \mathrm{b}, \mathrm{c} \in I \wedge x, y \in I$$

integer solutions are sought for unknowns *x* and *y.*

ii) Other(general) cases, where $\gcd(a,b) = d > 1$ (cont'd)

$$ax + by = c \wedge \gcd(a,b) = d$$
$$ax_0 + by_0 = ax + by$$
$$a(x - x_0) = b(y_0 - y)$$

$a = k_1 d$
$b = k_2 d$

$x_0 = sl$
$y_0 = tl$
$d = as + bt$

$a|b(y_0 - y) \Rightarrow k_1 d|k_2 d(y_0 - y) \Rightarrow k_1|k_2(y_0 - y) \wedge \gcd(k_1, k_2) = 1$
$\Rightarrow k_1|(y_0 - y)$
$\ldots \Rightarrow k_2|(x - x_0)$

continued

Linear Diophantine Equations

$$ax + by = c \;; \qquad a, \mathrm{b}, \mathrm{c} \in I \wedge x, y \in I$$

integer solutions are sought for unknowns *x* and *y.*

$\Rightarrow k_1 | (y_0 - y)$

$\ldots \Rightarrow k_2 | (x - x_0)$

$$k_1 k = y_0 - y \wedge k_2 k = x - x_0$$

$$\left.\begin{matrix} x = k_2 k + x_0 \\ y = y_0 - k_1 k \end{matrix}\right\} \begin{matrix} y = y_0 - \dfrac{a}{d} k \\ x = x_0 + \dfrac{b}{d} k \end{matrix}$$

$$y = tl - \frac{a}{d} k$$

$$x = sl + \frac{b}{d} k$$

$$l = \frac{c}{d}$$

Linear Diophantine Equations

Example: Find the solution space for the following equation

$$172x + 20y = 1000$$

- Is there a solution where both x and y are positive?

Linear Congruences

Definition: A congruence of the form

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

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

- The solutions to a linear congruence $ax \equiv b(\bmod m)$ are all 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 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 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*.)

$$\gcd(a, m) = 1 \wedge \exists!\, \bar{a} \wedge 0 < \bar{a} < m \text{ such that, } a\bar{a} = 1 mod\ m$$

  Proof: Since gcd(*a*,*m*) = 1, by Theorem 6 of Section 4.3, there are integers *s* and *t* such that *sa* + *tm* = 1.
  - Hence, *sa* + *tm* $\equiv 1$ (mod *m*).
  - Since *tm* $\equiv 0$ (mod *m*), it follows that *sa* $\equiv 1$ (mod *m*)
  - Consequently, *s* is an inverse of *a* modulo *m*.
  - The uniqueness of the inverse is Exercise 7.

◄

Finding Inverses

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

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.
- 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

Example: Find an inverse of 101 modulo 4620.

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

Working Backwards:

$$42620 = 45\cdot101 + 75$$
$$101 = 1\cdot75 + 26$$
$$75 = 2\cdot26 + 23$$
$$26 = 1\cdot23 + 3$$
$$23 = 7\cdot3 + 2$$
$$3 = 1\cdot2 + 1$$
$$2 = 2\cdot1$$

Since the last nonzero remainder is 1, gcd(101,4260) = 1

$$1 = 3 - 1\cdot2$$
$$1 = 3 - 1\cdot(23 - 7\cdot3) = -1\cdot23 + 8\cdot3$$
$$1 = -1\cdot23 + 8\cdot(26 - 1\cdot23) = 8\cdot26 - 9\cdot23$$
$$1 = 8\cdot26 - 9\cdot(75 - 2\cdot26) = 26\cdot26 - 9\cdot75$$
$$1 = 26\cdot(101 - 1\cdot75) - 9\cdot75$$
$$= 26\cdot101 - 35\cdot75$$
$$1 = 26\cdot101 - 35\cdot(42620 - 45\cdot101)$$
$$= -35\cdot42620 + 1601\cdot101$$

Bézout coefficients : − 35 and 1601

1601 is an inverse of 101 modulo 42620

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 $x \equiv -8 \equiv 6 \pmod 7$

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 $-1, -8, -15, \ldots$

Using Inverses to Solve Congruences

Example: $19x \equiv 37 \ mod \ 141$, find x?

Using Inverses to Solve Congruences

General Case:

$$ax \equiv b \; mod \; m \wedge \gcd(a, m) = d > 1, m \in N^{+}; a, b, x \in I$$

Theorem: Congruence have solution **iff** d|b,

$\gcd(a, m) = d$

Left blank as a practice

Using Inverses to Solve Congruences

Example: $28x \equiv 14 \; mod \; 21$

General Solution Set of Linear Congruences

$$ax \equiv b \bmod m \Rightarrow ax - my = b$$

Employ LDE solution
$ax + by = c, \gcd(a, b) = d \wedge d|c$

$$y = tl - \frac{a}{d}k$$
$$x = sl + \frac{b}{d}k$$

$$x = x_0 + \frac{-m}{d}k \bmod m$$

where $\gcd(a, m) = d,\ d|b$

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:

  $x \equiv 2 \pmod{3}$,

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

  $x \equiv 2 \pmod{7}$?

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

The Chinese Remainder Theorem

Theorem 2: (*The Chinese Remainder Theorem*) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\;\;\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$.

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

- **Proof**: We'll show that a solution exists by describing a way to construct the solution. Showing that the solution is unique modulo m is Exercise 30.

continued →

The Chinese Remainder Theorem

To construct a solution first let $M_k = m/m_k$ for $k = 1,2,\ldots,n$ and $m = m_1 m_2 \cdots m_n$.

Since $\gcd(m_k, M_k) = 1$, by Theorem 1, there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_k y_k \equiv 1 \pmod{m_k}.$$

Form the sum

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n .$$

Note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k.

Because $M_k y_k \equiv 1 \pmod{m_k}$, we see that $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$, for $k = 1,2,\ldots,n$.

Hence, x is a simultaneous solution to the n congruences.

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

$$\vdots$$

$$x \equiv a_n \pmod{m_n}$$

◄

The Chinese Remainder Theorem

Example: Consider the 3 congruences from Sun-Tsu's problem:

$x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_3 = m/5 = 21$, $M_3 = m/7 = 15$.
- We see that
  - 2 is an inverse of $M_1 = 35$ modulo 3 since $35 \cdot 2 \equiv 2 \cdot 2 \equiv 1 \pmod 3$
  - 1 is an inverse of $M_2 = 21$ modulo 5 since $21 \equiv 1 \pmod 5$
  - 1 is an inverse of $M_3 = 15$ modulo 7 since $15 \equiv 1 \pmod 7$
- Hence,

$$x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$$
$$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$$

- We have shown that 23 is the smallest positive integer that is a simultaneous solution. Check it!

The Chinese Remainder Theorem

Example:

$x \equiv 9 \; mod 13$

$x \equiv 8 \; mod \; 11$, x =?

$x \equiv 1 \; mod \; 7$

Additional Reads

Reads:

- Chap. 4 and 5, Discrete Math. and Its applications, K.H. Rosen
- Chap. 4.8, Handbook of Discrete and Combinatorial Math., K.H. Rosen