MATH 565 Spring 2019 - Class Notes

3/13/19

Scribe: Michelle Tarr

Summary: This class covered how to solve linear equations modulo n using inverses and how to solve systems of concurrences with the Chinese Remainder Theorem.

Solving Linear Equations Modulo n

Consider $ax \equiv b \pmod{n}$

- How can we find a solution to this equation without trying every possible value of x?
- If $ax \equiv b \pmod{n}$, then $n \mid (b - ax)$ for some integer k, so $b - ax = nk$.
- We are looking for values of k and x that satisfy the equation $b = nk + ax$.
- Through previous investigation with the Euclidean Algorithm, we know that equations of the form $b = nk + ax$ have a solution if and only if $\gcd(a, n) \mid b$.

Theorem 1. *The equation $ax \equiv b \pmod{n}$ has a solution if and only if $\gcd(a, n) \mid b$. The solution to the equation is unique if and only if $\gcd(a, n) = 1$*

Example 1: Solve $3x \equiv 5 \pmod{6}$

Note that $\gcd(3, 6) = 3$ and $3 \nmid 5$. Thus this equation has no solution.

Example 2: Solve $3x \equiv 12 \pmod{6}$

Note that $\gcd(3, 6) = 3$ and $3 \mid 12$. Thus this equation has solutions, but they are not unique since $\gcd(3, 6) \neq 1$.

$$\begin{aligned}
&x \equiv 2 \pmod{6} \text{ since } 3(2) \equiv 6 \equiv 12 \pmod{6} \\
&x \equiv 4 \pmod{6} \text{ since } 3(4) \equiv 12 \pmod{6} \\
&x \equiv 6 \pmod{6} \text{ since } 3(6) \equiv 18 \equiv 12 \pmod{6}
\end{aligned}$$

Example 3: Solve $5x \equiv 2 \pmod{6}$

Note that $\gcd(5, 6) = 1$. Thus this equation has a solution and it is unique.

x	$5x \pmod 6$
0	$0 \pmod 6$
1	$5 \pmod 6$
2	$10 \equiv 4 \pmod 6$
3	$15 \equiv 3 \pmod 6$
4	$20 \equiv 2 \pmod 6$
5	$25 \equiv 1 \pmod 6$

Thus $x \equiv 4 \pmod 6$ is the one unique solution.

Definition: *If $a \cdot \bar{a} \equiv 1 \pmod n$ we say that $\bar{a}$ is the inverse of a modulo n.*

Example 4: $3 \cdot 4 \equiv 12 \equiv 1 \pmod{11}$, so 4 is the inverse of 3 modulo 11.

Theorem 2. *If $\gcd(a, n) = 1$, then a has a unique inverse modulo n.*

Proof. To find the inverse of a we are trying to solve the equation $ax \equiv 1 \pmod n$. By our previous theorem we know this equation has a solution if $\gcd(a, n) \mid 1$. Since $\gcd(a, n) = 1$, the inverse exists and is unique. □

Example 5: Find the inverse of $5 \pmod{21}$.

In order to find the inverse, we must solve the congruence $5x \equiv 1 \pmod{21}$, which means finding x and y such that $5x + 21y = 1$. This can be done using the Euclidean Algorithm:

$$\begin{aligned} 21 &= 4(5) + 1 \\ 5 &= 5(1) + 0 \\ 1 &= 1(21) - 4(5) \end{aligned}$$

Thus, $x \equiv -4 \equiv 17 \pmod{21}$ is the inverse of 5 modulo 21.

How to Solve A Linear Congruence:

Consider $ax \equiv b \pmod n$

- We can not divide by a in modular arithmetic so how can we cancel out a in order to find a solution for x?
- We can use inverses and multiply both sides of the congruence by the inverse of a, $\bar{a}$.

Example 6: Solve $5x \equiv 12 \pmod{21}$.

We know that the inverse of 5 modulo 21 is 17, so to solve for x we must multiply by 17 on both sides.

$$\begin{aligned} 5x &\equiv 12 \pmod{21} \\ 17(5x) &\equiv 17(12) \pmod{21} \\ 1x &\equiv 204 \equiv -6 \equiv 15 \pmod{21} \\ x &\equiv 15 \pmod{21} \end{aligned}$$

Systems of Congruences

- If $a \equiv b \pmod{n}$, then $n \mid (b - a)$.
- Any factor of n also divides b-a as well
- We can write congruences in the modulo of each of these factors to create a system of congruences.

Example 7: Consider $x \equiv 11 \pmod{42}$, which means $42 \mid (11 - x)$.

Since $42 = 2 \cdot 3 \cdot 7$, we know $2 \mid (11 - x)$, $3 \mid (11 - x)$, and $7 \mid (11 - x)$.

$$\begin{aligned} x &\equiv 11 \equiv 1 \pmod{2} \\ x &\equiv 11 \equiv 2 \pmod{3} \\ x &\equiv 11 \equiv 4 \pmod{7} \end{aligned}$$

- Can we go the other way and find one solution that works for a system of congruences simultaneously?

Theorem 3: Chinese Remainder Theorem. *If integers $m_1, m_2, ...m_k$ are all pairwise coprime, so that the* gcd *of any pair is 1, then any set of equations:*

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

has a unique solution modulo $M = m_1 \cdot m_2 \cdot ...m_k$

Proof. Suppose $m_1, m_2, ...m_k$ are pairwise coprime integers. Let $M = m_1 \cdot m_2 \cdot ...m_k$ be their product. Let $n_i = \frac{M}{m_i}$ be the product of all the values except m_i. Note that $\gcd(n_i, m_i) = 1$ since n_i is the product of numbers that are all coprime with m_i. Thus, each n_i has an inverse $\bar{n}_i \pmod{m_i}$. Compute $x = a_1 n_1 \bar{n}_1 + a_2 n_2 \bar{n}_2 + ...a_k n_k \bar{n}_k$.

Consider $x \equiv a_1 n_1 \bar{n}_1 + a_2 n_2 \bar{n}_2 + ... a_k n_k \bar{n}_k \pmod{m_j}$. Since $m_j \mid n_i$ for all $i \neq j$, we know that $a_i n_i \bar{n}_i \equiv 0 \pmod{m_j}$ for all $i \neq j$. This means $x \equiv a_j n_j \bar{n}_j \pmod{m_j}$. In addition, $n_j \bar{n}_j \equiv 1 \pmod{m_j}$ because $\bar{n}_j$ is the inverse of n_j modulo j. Thus $x \equiv a_j \pmod{m_j}$.

Therefore, x satisfies all the individual congruences $x \equiv a_i \pmod{m_i}$ simultaneously. $\square$

Example 8: Chinese Remainder Theorem: Find x such that

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 1 \pmod 3 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

Note that 2, 3, and 7 are all pairwise coprime and that $M = 2 \cdot 3 \cdot 7 = 42$.

$$\begin{array}{lll} a_1 = 0 & a_2 = 1 & a_3 = 6 \\ m_1 = 2 & m_2 = 3 & m_3 = 7 \\ n_1 = 3 \cdot 7 = 21 & n_2 = 2 \cdot 7 = 14 & n_3 = 2 \cdot 3 = 6 \\ \bar{n}_1 \equiv 21^{-1} \pmod 2 & \bar{n}_2 \equiv 14^{-1} \pmod 3 & \bar{n}_3 \equiv 6^{-1} \pmod 7 \\ \bar{n}_1 = 1 & \bar{n}_2 = 2 & \bar{n}_3 = 6 \end{array}$$

Use the Chiniese Remainer Theorem to compute $x = a_1 n_1 \bar{n}_1 + a_2 n_2 \bar{n}_2 + a_3 n_3 \bar{n}_3$. This gives $x = (0)(21)(1) + (1)(14)(2) + (6)(6)(6) = 244$. The solution to the system of congruences is $x \equiv 244 \equiv 34 \pmod{42}$.

Polynomial Equations Modulo n

Theorem 4: Legendre. *If $f(x) = a_d x^d + a_{d-1} x^{d-1} + ... a_0$ is a polynomial of degree $d > 0$ where $p \nmid a_d$, then $f(x) \equiv 0 \pmod p$ has at most d solutions.*