University of Colorado **Boulder**

Department of Computer Science
CSCI 2824: Discrete Structures
Chris Ketelsen

Lectures 20:
Solving Congruences

Solving Congruences

A congruence of the form

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

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

Goal: Find all integers x that satisfy this congruence

Solving Congruences

This is analogous to the linear equation

$$ax = b$$

One way to solve this simple equation is to multiply both sides by $\frac{1}{a}$

$$\frac{1}{a}ax = \frac{1}{a}b \quad \Rightarrow \quad x = \frac{b}{a}$$

Here we use the fact that $\frac{1}{a}$ is the multiplicative **inverse** of a

Recall that $\frac{1}{a}$ is the multiplicative inverse of a because $\dfrac{1}{a}a = 1$

We'll employ the same strategy to solve the linear congruence

Solving Congruences

Strategy: Find a number $\bar{a}$ such that $\bar{a}a \equiv 1 \pmod{m}$.

The number $\bar{a}$ is called the **inverse** of a modulo m

If we know the inverse then we can find the solution to the linear congruence by

$$x = \bar{a}b \pmod{m}$$

Solving Congruences

Example: Solve $3x \equiv 4 \pmod{7}$

Note that $-2 \cdot 3 = -6 = -1 \cdot 7 + 1 \equiv 1 \pmod{7}$

So the inverse of 3 modulo 7 is -2

Multiplying both sides of the linear congruence by -2 gives

$$x \equiv -2 \cdot 4 \pmod{7} \equiv -8 \pmod{7} \equiv 6 \pmod{7}$$

So any x congruent to 6 mod 7 is a solution, e.g. $6,\ 13,\ 20, \ldots$

Check: $3 \cdot 6 = 18 = 2 \cdot 7 + 4 \equiv 4 \pmod{7}$ ✓

Check: $3 \cdot 13 = 39 = 5 \cdot 7 + 4 \equiv 4 \pmod{7}$ ✓

Solving Congruences

OK, so if we can find an inverse of a then we can solve the linear congruence $ax \equiv b \pmod{m}$

Question: Does such an inverse always exist?

Question: If so, can we find it more systematically?

Solving Congruences

Theorem: If a and m are relatively prime then an inverse of a modulo m exists

Proof: Becaues gcd$(a, m) = 1$ Bezout's theorem tells us that there exist integers s and t such that

$$sa + tm = 1$$

This implies that $sa + tm \equiv 1 \pmod{m}$

Because $tm \equiv 0 \pmod{m}$ it follows that $sa \equiv 1 \pmod{m}$

Clearly s is the inverse of a modulo m that we're after

Note: The proof also shows us how to find the inverse

Solving Congruences

The inverse of a is exactly the coefficient s in Bezout's Theorem

We saw how to find such an s last time

Example: Determine the inverse of 19 modulo 141

First do the Euclidean algorithm and confirm that $\gcd(19, 141) = 1$

$$\begin{aligned} 141 &= 7 \cdot 19 + 8 \\ 19 &= 2 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \end{aligned}$$

The EA will terminate on the next step. The last remainder is 1 so we know that 19 and 141 are relatively prime and the theorem applies

Solving Congruences

Example: Determine the inverse of 19 modulo 141

We find the inverse by plugging back into the Euclidean algorithm to find the linear combination $19s + 141t = 1$. We have

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (8 - 2 \cdot 3) = 3 \cdot 3 - 1 \cdot 8 \\
&= 3 \cdot (19 - 2 \cdot 8) - 1 \cdot 8 = 3 \cdot 19 - 7 \cdot 8 \\
&= 3 \cdot 19 - 7 \cdot (141 - 7 \cdot 19) \\
&= 52 \cdot 19 - 7 \cdot 141
\end{aligned}
$$

Thus $s = 52$ is the inverse of 19 modulo 141

Check: $19 \cdot 52 = 988 = 7 \cdot 141 + 1 \equiv 1 \pmod{141}$

Solving Congruences

Example: Solve the linear congruence $19x \equiv 4 \pmod{141}$

Multiplying both sides of the congruence by 52 (the inverse of 19 modulo 141) gives

$$\begin{aligned} x &\equiv 52 \cdot 4 \pmod{141} \\ &\equiv 208 \pmod{141} \\ &\equiv 67 \pmod{141} \end{aligned}$$

$$\textbf{Check :} \quad \begin{aligned} 19 \cdot 67 &\equiv 988 \pmod{141} \\ &\equiv 7 \cdot 141 + 4 \pmod{141} \\ &\equiv 4 \pmod{141} \quad \checkmark \end{aligned}$$

Solving Congruences

EFY: Solve the congruence $5x \equiv 4 \pmod{17}$

EFY: Solve the congruence $55x \equiv 34 \pmod{89}$

EFYs

Solving Congruences

EFY: Solve the congruence $55x \equiv 34 \pmod{89}$

Solution: First we check that 55 and 89 are relatively prime

$$
\begin{aligned}
89 &= 1 \cdot 55 + 34 \\
55 &= 1 \cdot 34 + 21 \\
34 &= 1 \cdot 21 + 13 \\
21 &= 1 \cdot 13 + 8 \\
13 &= 1 \cdot 8 + 5 \\
8 &= 1 \cdot 5 + 3 \\
5 &= 1 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1
\end{aligned}
$$

Solving Congruences

They are, now work backwards to find the inverse of 55 modulo 89

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 = 3 - 1 \cdot (5 - 3) = 2 \cdot 3 - 5 \\
&= 2 \cdot (8 - 1 \cdot 5) - 5 = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) = 5 \cdot 8 - 3 \cdot 13 \\
&= 5 \cdot (21 - 1 \cdot 13) - 3 \cdot 13 = 5 \cdot 21 - 8 \cdot 13 \\
&= 5 \cdot 21 - 8 \cdot (34 - 1 \cdot 21) = 13 \cdot 21 - 8 \cdot 34 \\
&= 13 \cdot (55 - 1 \cdot 34) - 8 \cdot 34 = 13 \cdot 55 - 21 \cdot 34 \\
&= 13 \cdot 55 - 21 \cdot (89 - 1 \cdot 55) \\
&= 34 \cdot 55 - 21 \cdot 89
\end{aligned}
$$

Thus the inverse of 55 mod 89 is 34

Solving Congruences

EFY: Solve the congruence $55x \equiv 34 \pmod{89}$

Multiplying both sides of the congruence by the inverse of 55 modulo 89 gives

$$\begin{aligned} x &\equiv 34 \cdot 34 \pmod{89} \\ &\equiv 1156 \pmod{89} \\ &\equiv 12 \cdot 89 + 88 \pmod{89} \\ &\equiv 88 \pmod{89} \end{aligned}$$

Thus $x \equiv 88 \pmod{89}$ is the solution

$$\begin{aligned} \textbf{Check}: 55 \cdot 88 \equiv 4840 \pmod{89} &\equiv 54 \cdot 89 + 34 \pmod{89} \\ &\equiv 34 \pmod{89} \quad \checkmark \end{aligned}$$

Solving Congruences

EFY: Solve the congruence $5x \equiv 4 \pmod{17}$

Solution: First we check that 5 and 17 are relatively prime, and if so, find the inverse of 5 modulo 17

$$\begin{aligned} 17 &= 3 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

We've shown that gcd$(5, 17) = 1$, so an inverse exists. To find it we work backwards through the Euclidean Algorithm

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2 \cdot (17 - 3 \cdot 5) = 7 \cdot 5 - 2 \cdot 17 \end{aligned}$$

Thus the inverse of 5 mod 17 is 7

Solving Congruences

EFY: Solve the congruence $5x \equiv 4 \ (\mathbf{mod}\ 17)$

Solution: Multiplying both sides of the congruence by 7 gives

$$\begin{aligned} x &\equiv 7 \cdot 4 \ (\mathbf{mod}\ 17) \\ &\equiv 28 \ (\mathbf{mod}\ 17) \\ &\equiv 1 \cdot 17 + 11 \ (\mathbf{mod}\ 17) \\ &\equiv 11 \ (\mathbf{mod}\ 17) \end{aligned}$$

So the solution to the linear congruence is $x = 11 \ (\mathbf{mod}\ 17)$

Check: $5 \cdot 11 \equiv 55 \ (\mathbf{mod}\ 17)$

$$\equiv 3 \cdot 17 + 4 \ (\mathbf{mod}\ 17) = 4 \ (\mathbf{mod}\ 17) \quad \checkmark$$

Solving Congruences

EFY: Solve the congruence $5x \equiv 4 \pmod{17}$

Solution: Multiplying both sides of the congruence by 7 gives

$$\begin{aligned} x &\equiv 7 \cdot 4 \pmod{17} \\ &\equiv 28 \pmod{17} \\ &\equiv 1 \cdot 17 + 11 \pmod{17} \\ &\equiv 11 \pmod{17} \end{aligned}$$

So the solution to the linear congruence is $x = 11 \pmod{17}$

Check: $5 \cdot 11 \equiv 55 \pmod{17}$

$$\equiv 3 \cdot 17 + 4 \pmod{17} = 4 \pmod{17} \quad \checkmark$$