Carmen's Core Concepts (Math 135)

Carmen Bruni

University of Waterloo

Week 7

1. Congruence Definition
2. Congruence is an Equivalence Relation (CER)
3. Properties of Congruence (PC)
4. Example
5. Congruences and Division (CD)
6. Congruent iff Same Remainder (CISR)
7. Example 2
8. Linear Congruences
9. Solution 1 to "Solve $4x \equiv 5 \pmod 8$".
10. Solution 2 to "Solve $4x \equiv 5 \pmod 8$"
11. Solution 3 to "Solve $4x \equiv 5 \pmod 8$"
12. Linear Congruence Theorem 1
13. Simplifying Congruences

Congruence Definition

Congruence Definition

Definition: Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then a is congruent to b modulo n if and only if $n \mid (a - b)$ and we write $a \equiv b \pmod{n}$. This is equivalent to saying there exists an integer k such that $a - b = kn$ or $a = b + kn$.

Example: $5 \equiv 11 \pmod{6}$, $723 \equiv -17 \pmod{20}$

Congruence is an Equivalence Relation (CER)

Theorem: Congruence is an Equivalence Relation (CER)

Let $n \in \mathbb{N}$. Let $a, b, c \in \mathbb{Z}$. Then

1. (Reflexivity) $a \equiv a \pmod{n}$.
2. (Symmetry) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.
3. (Transitivity) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Properties of Congruence (PC)

Theorem: Properties of Congruence (PC) Let $a, a', b, b' \in \mathbb{Z}$. If $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$, then

1. $a + b \equiv a' + b' \pmod{m}$
2. $a - b \equiv a' - b' \pmod{m}$
3. $ab \equiv a'b' \pmod{m}$

Corollary If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for $k \in \mathbb{N}$.

Example

Example: Is $5^9 + 62^{2000} - 14$ divisible by 7?

Example

Example: Is $5^9 + 62^{2000} - 14$ divisible by 7?

Solution: Reduce modulo 7. By Properties of Congruence, we have

$$\begin{aligned} 5^9 + 62^{2000} - 14 &\equiv (-2)^9 + (-1)^{2000} - 0 \pmod 7 \\ &\equiv -2^9 + 1 \pmod 7 \\ &\equiv -(2^3)^3 + 1 \pmod 7 \\ &\equiv -(8)^3 + 1 \pmod 7 \\ &\equiv -(1)^3 + 1 \pmod 7 \\ &\equiv 0 \pmod 7 \end{aligned}$$

Therefore, the number is divisible by 7.

Congruences and Division (CD)

Proposition: (Congruences and Division (CD)). Let $a, b, c \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Congruences and Division (CD)

Proposition: (Congruences and Division (CD)). Let $a, b, c \in \mathbb{Z}$ and let $n \in \mathbb{N}$. If $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

Proof: By assumption, $n \mid (ac - bc)$ so $n \mid c(a - b)$. Since $\gcd(c, n) = 1$, by Coprimeness and Divisibility (CAD), $n \mid (a - b)$. Hence $a \equiv b \pmod{n}$.

Congruent iff Same Remainder (CISR)

Proposition: (Congruent iff Same Remainder (CISR)) Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder after division by n.

Congruent iff Same Remainder (CISR)

Proposition: (Congruent iff Same Remainder (CISR)) Let $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod{n}$ if and only if a and b have the same remainder after division by n.

Proof: By the Division Algorithm, write $a = nq_a + r_a$ and $b = nq_b + r_b$ where $0 \leq r_a, r_b < n$. Subtracting gives

$$a - b = n(q_a - q_b) + r_a - r_b$$

($\Rightarrow$) First assume that $a \equiv b \pmod{n}$, that is $n \mid a - b$. Since $n \mid n(q_a - q_b)$, we have by Divisibility of Integer Combinations that $n \mid (a - b) + n(q_a - q_b)(-1)$ and thus, $n \mid r_a - r_b$. By our restriction on the remainders, we see that the difference is bounded by $-n + 1 \leq r_a - r_b \leq n - 1$. However, only 0 is divisible by n in this range! Since $n \mid (r_a - r_b)$, we must have that $r_a - r_b = 0$. Hence $r_a = r_b$.

($\Leftarrow$) Assume that $r_a = r_b$. Noting that the difference $a - b$ yields $a - b = n(q_a - q_b) + r_a - r_b = n(q_a - q_b)$, we see that $n \mid (a - b)$ and hence $a \equiv b \pmod{n}$. ■

Example 2

What is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4?

Example 2

What is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4?

Solution: Notice that

$$6 = 4(1) + 2 \qquad 77 = 19(4) + 1 \qquad 999 = 249(4) + 3$$

Hence, by (CISR), we have $6 \equiv 2 \pmod 4$, $77 \equiv 1 \pmod 4$ and $999 \equiv 3 \pmod 4$. Thus, by (PC),

$$\begin{aligned} 77^{100}(999) - 6^{83} &\equiv (1)^{100}(3) - 2^{83} \pmod 4 \\ &\equiv 3 - 2^2 \cdot 2^{81} \pmod 4 \\ &\equiv 3 - 4 \cdot 2^{81} \pmod 4 \\ &\equiv 3 - 0(2^{81}) \pmod 4 \\ &\equiv 3 \pmod 4 \end{aligned}$$

Once again by (CISR), 3 is the remainder when $77^{100}(999) - 6^{83}$ is divided by 4. ■

Linear Congruences

Question: Solve $ax \equiv c \pmod{m}$ where $a, c \in \mathbb{Z}$ and $m \in \mathbb{N}$ for $x \in \mathbb{Z}$.

Note: When we are solving $ax = c$ over the integers, we know that this has a solution if and only if $a \mid c$.

Example: Solve $4x \equiv 5 \pmod{8}$.

Solution 1 to "Solve $4x \equiv 5 \pmod 8$".

- By definition, there exists a $z \in \mathbb{Z}$ such that $4x - 5 = 8z$, that is, $4x - 8z = 5$. Now, let $y = -z$. Thus, the original question is equivalent to solving the Linear Diophantine Equation

$$4x + 8y = 5$$

- Since $\gcd(4, 8) = 4 \nmid 5$, by LDET1, we see that this LDE has no solution. Hence the original congruence has no solutions.

Solution 2 to "Solve $4x \equiv 5 \pmod 8$"

Let $x \in \mathbb{Z}$. By the Division Algorithm, $x = 8q + r$ for some $0 \leq r \leq 7$ and q, r integers. By Congruent If and Only If Same Remainder, $4x \equiv 5 \pmod 8$ holds if and only if $4r \equiv 5 \pmod 8$. Thus, if we can prove that no number from $0 \leq x \leq 7$ works, then no integer x can satisfy the congruence. Trying the possibilities

$$\begin{aligned}
4(0) &\equiv 0 \pmod 8 \\
4(1) &\equiv 4 \pmod 8 \\
4(2) &\equiv 0 \pmod 8 \\
4(3) &\equiv 4 \pmod 8 \\
4(4) &\equiv 0 \pmod 8 \\
4(5) &\equiv 4 \pmod 8 \\
4(6) &\equiv 0 \pmod 8 \\
4(7) &\equiv 4 \pmod 8
\end{aligned}$$

shows that $4x \equiv 5 \pmod 8$ has no solution. ■

Solution 3 to "Solve $4x \equiv 5 \pmod 8$"

Assume towards a contradiction that there exists an integer x such that $4x \equiv 5 \pmod 8$. Multiply both sides by 2 to get (by Properties of Congruence) that

$$0 \equiv 0x \equiv 8x \equiv 10 \pmod 8$$

Hence, $8 \mid 10$ however $8 \nmid 10$. This is a contradiction. Thus, there are no integer solutions to $4x \equiv 5 \pmod 8$. ■

Linear Congruence Theorem 1

Theorem: LCT1 (Linear Congruence Theorem 1). Let $a, c \in \mathbb{Z}$ and $m \in \mathbb{N}$ and $\gcd(a, m) = d$. Then $ax \equiv c \pmod{m}$ has a solution if and only if $d \mid c$. Further, we have d solutions modulo m and 1 solution modulo m/d. Moreover, if $x = x_0$ is a solution, then $x \equiv x_0 \pmod{m/d}$ forms the complete solution set or alternatively, $x = x_0 + \frac{m}{d}n$ for all $n \in \mathbb{Z}$ or for another alternative way to write the solution:

$$x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, ..., x_0 + (d-1)\frac{m}{d} \pmod{m}$$

This is a restatement of LDET1

Simplifying Congruences

If $x \equiv 2, 5 \pmod 6$, then $x \equiv 2 \pmod 3$ gives the same solution set.

Simplifying Congruences

If $x \equiv 2, 5 \pmod 6$, then $x \equiv 2 \pmod 3$ gives the same solution set.

This is true since if $x \equiv 2, 5 \pmod 6$, then $x = 2 + 6k$ or $x = 5 + 6k$ for some integer k. In either case, $3 \mid (x - 2)$ or $3 \mid (x - 5)$ since $3 \mid 6$. Hence, $x \equiv 2 \pmod 3$ or $x \equiv 5 \equiv 2 \pmod 3$. In reverse, if $x \equiv 2 \pmod 3$, then $x = 2 + 3k$ for some integer k. Now, since $6/3 = 2$, we look at the remainder of k when divided by 2. If the remainder is 0, then $k = 2\ell$ for some integer ℓ and hence $x = 2 + 6\ell$ and so $x \equiv 2 \pmod 6$. Now, if the remainder when k is divided by 2 is 1, then write $k = 2\ell + 1$ for some integer ℓ. Hence, $x = 2 + 3(2\ell + 1)$ giving $x = 5 + 6\ell$ and thus $x \equiv 5 \pmod 6$.