Lecture 27

Instructor's Comments: An important announcement. Students should probably read the textbook but I anticipate most don't just due to timing restrictions. However, I would strongly advise students read Chapter 26 to get practice with the plethora of notation.

Handout or Document Camera or Class Exercise

What is the last digit of $5^{32}3^{10} + 9^{22}$?

Solution: Want the remainder when we divide by 10. Hence reduce modulo 10 and use Congruent If and Only If Same Remainder.

$$\begin{aligned} 5^{32} \cdot 3^{10} + 9^{22} &\equiv (5^2)^{16} \cdot 9^5 + (-1)^{22} \pmod{10} \\ &\equiv 5^{16}(-1)^5 + 1 \pmod{10} \\ &\equiv (5^2)^8(-1) + 1 \pmod{10} \\ &\equiv -5^8 + 1 \pmod{10} \\ &\equiv -(5^2)^4 + 1 \pmod{10} \\ &\equiv -5^4 + 1 \pmod{10} \\ &\equiv -625 + 1 \pmod{10} \\ &\equiv -4 \pmod{10} \\ &\equiv 6 \pmod{10} \end{aligned}$$

Hence the last digit is 6. ■

Instructor's Comments: This is the 10 minute mark.

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: We associate a linear Diophantine equation to this linear congruence. By definition, there exists a $z \in \mathbb{Z}$ such that $4x - 5 = 8z$, that is, $4x - 8z = 5$. Now, letting $y = -z$. gives the linear Diophantine equation

$$4x + 8y = 5$$

Instructor's Comments: From now on I will jump straight to this version of the LDE without mentioning it so make sure they understand this change of variables trick to translate to an LDE quickly. This is why I go through this here.

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: 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.

Instructor's Comments: Again make a note that this explanation is not needed anymore to do these problems and is included here only for clarity.

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: 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 $4x \equiv 5 \pmod{8}$. ■

Instructor's Comments: This is the 25 minute mark. Take your time with the previous argument. Encourage students to be creative with how they argue! If they find a solution encourage them to find another!

Example: $5x \equiv 3 \pmod{7}$.

Solution: Look Modulo 7. Then there are only 7 possibilities to consider for x. Trying them gives

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

Therefore, $x \equiv 2 \pmod{7}$ gives the complete set of solutions. ■

Solution 2: This is equivalent to solving the LDE

$$5x + 7y = 3$$

A solution is given by $(x, y) = (2, -1)$. By LDET2, $x = 2 + 7n$ and $y = -1 + 5n$ for all n gives the complete set of solutions. Hence $x \equiv 2 \pmod{7}$ gives the complete solutions. ■

Solution 3: $5x \equiv 3 \pmod{7} \Leftrightarrow x \equiv 2 \pmod{7}$. We see this by multiplying by 5 to go in reverse and multiplying by 3 to go from the left to the right. Something like:

$$\begin{aligned}
5x &\equiv 3 \pmod{7} \\
(3)5x &\equiv (3)3 \pmod{7} \\
15x &\equiv 9 \pmod{7} \\
x &\equiv 2 \pmod{7}
\end{aligned}$$

and multiply by 3 to go in reverse.

Instructor's Comments: Mention that this is related to something called finding an inverse for 5.

Example: $2x \equiv 4 \pmod{6}$.

Solution: Trying all 6 possibilities yields,

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

Hence, $x \equiv 2, 5 \pmod 6$ give solutions. These solutions are captured by $x \equiv 2 \pmod 3$. (It is not a coincidence that $3 = 6/\gcd(2, 4)$). ■

Instructor's Comments: Try to make this the 35 minute mark.

Summarizing the above give the following theorem:

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:

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

Proof: Read p. 180. ■

Instructor's Comments: This is the 40-45 minute mark.

Handout or Document Camera or Class Exercise

Solve $9x \equiv 6 \pmod{15}$.

Solution: Notice that $9(4) = 36 \equiv 6 \pmod{15}$. Hence, by LCT1, all solutions are given by $x \equiv 4 \pmod{15/\gcd(9,15)}$, or $x \equiv 4 \pmod{5}$. This is equivalent to $x \equiv 4, 9, 14 \pmod{15}$.

Alternate Solution: Equivalent to solving the LDE

$$\begin{aligned} & 9x + 15y = 6 \\ \implies & 3x + 5y = 2 \end{aligned}$$

By LDET2, since $(x, y) = (-1, 1)$ is a solution, all solutions are given by

$$\begin{aligned} x &= -1 + 5n \\ y &= 1 - 3n \end{aligned}$$

for all $n \in \mathbb{Z}$. Therefore, a solution is given by $x \equiv -1 \pmod{5}$ or $x \equiv 4 \pmod{5}$. Equivalently, $x \equiv 4, 9, 14 \pmod{15}$.

Instructor's Comments: This is the 50 minute mark.