Lecture 25

Instructor's Comments: First part is to recall the definition of congruence. This is extremely important. Get students to do this on their own

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 $a = b + kn$.

Instructor's Comments: This is the 5 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: Write on the board and get students to prove. These are follow your nose proofs

Congruence is an Equivalence Relation (CER)
Let $n \in \mathbb{N}$. Let $a, b, c \in \mathbb{Z}$. Then

(i) (Reflexivity) $a \equiv a \pmod{n}$.

(ii) (Symmetry) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.

(iii) (Transitivity) $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.

Proof:

(i) Since $n \mid 0 = (a - a)$, we have that $a \equiv a \pmod{n}$.

(ii) Since $n \mid (a - b)$, there exists an integer k such that $nk = (a - b)$. This implies that $n(-k) = b - a$ and hence $n \mid (b - a)$ giving $b \equiv a \pmod{n}$.

(iii) Since $n \mid (a - b)$ and $n \mid (b - c)$, by Divisibility of Integer Combinations, $n \mid ((a - b) + (b - c))$. Thus $n \mid (a - c)$ and hence $a \equiv c \pmod{n}$

Instructor's Comments: This is the 20 minute mark

Example: Without a calculator, determine if $167 \equiv 2015 \pmod 4$ is true.

Solution: Since $2015 \equiv 3 \pmod 4$ (valid as $4 \mid 2012 = 2015 - 3$) and $167 \equiv 3 \pmod 4$ (valid as $4 \mid 164 = 167 - 3$), we see by symmetry that $3 \equiv 2015 \pmod 4$ and hence by transitivity that $167 \equiv 2015 \pmod 4$.

Alternate Solution: Does $4 \mid (2015 - 167) = 1848$?

Instructor's Comments: This is the 25 minute mark

Handout or Document Camera or Class Exercise

Instructor's Comments: Write on board and get students to prove on their own

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

(i) $a + b \equiv a' + b' \pmod{m}$

(ii) $a - b \equiv a' - b' \pmod{m}$

(iii) $ab \equiv a'b' \pmod{m}$

Proof:

(i) Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid (a - a' + (b - b'))$. Hence $m \mid ((a + b) - (a' + b'))$ and so $a + b \equiv a' + b' \pmod{m}$.

(ii) Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid (a - a' - (b - b'))$. Hence $m \mid ((a - b) - (a' - b'))$ and so $a - b \equiv a' - b' \pmod{m}$.

(iii) Since $m \mid (a - a')$ and $n \mid (b - b')$, we have by Divisibility of Integer Combinations $m \mid ((a - a')b + (b - b')a')$. Hence $m \mid ab - a'b'$ and so $ab \equiv a'b' \pmod{m}$.

Instructor's Comments: This is the 40 minute mark

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

Example: Since $2 \equiv 6 \pmod 4$, we have that
$2^2 \equiv 6^2 \pmod 4$, that is, $4 \equiv 36 \pmod 4$.

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.

Instructor's Comments: This is the 50 minute mark. Some things to note above: In computations, we often don't cite every single time a basic proposition is used like PC or CER or the major corollary above. Be sure though while explaining to mention the use of the corollary above.