# Homework:

READ CHAPTER 26!

Q1. I enjoy trying to discover and write MATH 135 proofs.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q2. When I have difficulties with MATH 135 proofs, I know I can handle them.

A) Strongly disagree

B) Disagree

C) Neither agree nor disagree

D) Agree

E) Strongly agree

Q3. Which of the following satisfies $x \equiv 40 \pmod{17}$ ?

$x \equiv 6 \bmod 17$

(Do not use a calculator.)

A) $x = 173 \equiv 3 \bmod 17$

B) $x = 15^5 + 19^3 - 4 \equiv (-2)^5 + 2^3 - 4 \equiv -32 + 8 - 4 \equiv 2 + 4 \equiv 6 \bmod 17$

C) $x = 5 \cdot 18^{100} \equiv 5(1)^{100} \equiv 5 \bmod 17$

D) $x = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 6 \cdot 35 \cdot 143 \equiv (-6)(-4) \equiv 6 \cdot 1 \cdot 24 \equiv 6 \cdot 7 \equiv 42 \equiv 8 \bmod 17$

E) $x = 17^0 + 17^1 + 17^2 + 17^3 + 17^4 + 17^5 + 17^6 \equiv 1 \bmod 17$

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

Soln: Reduce mod 10.

$$5^{32}\cdot 3^{10} + 9^{22} \equiv (5^2)^{16}(9)^5 + (-1)^{22} \mod 10$$
$$\equiv 5^{16}(-1)^5 + 1 \mod 10$$
$$\equiv (5^2)^8(-1) + 1 \mod 10$$
$$\equiv -5^8 + 1 \mod 10$$
$$\equiv -(5^2)^4 + 1 \mod 10$$
$$\equiv -5^4 + 1 \mod 10$$
$$\equiv -5^2 + 1 \mod 10$$
$$\equiv -5 + 1 \mod 10$$
$$\equiv -4 + 10 \mod 10$$
$$\equiv 6$$

# Linear Congruences.

Q: Solve $ax \equiv c \mod m$
(for $a, c \in \mathbb{Z}$, $m \in \mathbb{N}$) for $x \in \mathbb{Z}$.

Compare to $ax = c$ (sol'n when $a|c$).

Ex: $4x \equiv 5 \mod 8$

Sol'n 1: By defn $\exists y' \in \mathbb{Z}$ s.t.
$4x - 5 = 8y' \iff \exists y' \in \mathbb{Z}$ s.t.
$4x - 8y' = 5$.
Let $y = -y'$. Thus, the original question is equivalent to solving the LDE

$$4x + 8y = 5$$

Since $\gcd(4,8) = 4 \nmid 5$, by LDET1, this LDE has no sol'n.

$4x \equiv 5 \bmod 8$

Soln 2: Try all numbers from 0 to 7.

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| $4x \bmod 8$ | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |

Now, let $x \in \mathbb{Z}$. By the Div Alg'm

$$x = 8q + r$$

for some $0 \leq r \leq 7$. By CISR

$4x \equiv 5 \bmod 8 \iff 4r \equiv 5 \bmod 8$

Above we tried all numbers from 0 to 7 and saw that there was no solution.

Soln 3: Assume towards a contradiction that $\exists x \in \mathbb{Z}$ s.t. $4x \equiv 5 \bmod 8$.

Multiply both sides by 2 to get (by PC)

$$0 \equiv 0_x \equiv 8x \equiv 10 \bmod 8$$

Thus $8 \mid 10$. BUT $8 \nmid 10$ #. So there are no integer solutions to $4x \equiv 5 \bmod 8$.

Ex: $5x \equiv 3 \mod 7$

Soln 1:

| $x$ | 0 | 1 | **2** | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| $5x \bmod 7$ | 0 | 5 | **3** | 1 | 6 | 4 | 2 |

$\therefore$ $x \equiv 2 \mod 7$ gives the solutions.

Soln 2: Equivalent to solving the LDE

$$5x + 7y = 3.$$

By LDE T2 $x = 2 + 7n$ $y = -1 - 5n$

$\forall n \in \mathbb{Z}$ gives the solutions.

Soln 3: $5x \equiv 3 \mod 7 \iff x \equiv 2 \mod 7$

(mult. by 5 / mult. by 3)

Ex: $2x \equiv 4 \mod 6$

Soln

| $x$ | 0 | 1 | **2** | 3 | 4 | **5** |
|---|---|---|---|---|---|---|
| $2x \bmod 6$ | 0 | 2 | **4** | 0 | 2 | **4** |

$\therefore$ $x \equiv 2, 5 \mod 6 \iff x \equiv 2 \mod 3$

Summary: LCT1 (Linear Congruence Theorem 1)

Let $a, c \in \mathbb{Z}$, $m \in \mathbb{N}$ and $\gcd(a,m) = d$ Then

$ax \equiv c \bmod m$ has a solution $\iff d \mid c$.

NB: Have $d$ solutions modulo $m$.
Have $1$ solution modulo $\frac{m}{d}$.

Moreover, if $x = x_0$ is a solution, then

$x \equiv x_0 \bmod \frac{m}{d}$ forms the complete sol'n

OR $x = x_0 + \frac{m}{d} n$ forall $n \in \mathbb{Z}$

OR $x \equiv x_0, x_0 + \frac{m}{d}, x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d} \bmod m$

Pf: Read p. 180.