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 is equal to $[53]^{242} + [5]^{-1}$ in $\mathbb{Z}_7$?

(Do not use a calculator.)

$\boxed{\text{A) [5]}}$

B) [4]

C) [3]

D) [2]

E) [1]

$53^{242} \equiv 4^{242} \mod 7$

$\equiv (4^6)^{40} \cdot 4^2 \mod 7$

FLT $(\because \gcd(4,7)=1)$ $\equiv 1^{40} \cdot 16 \mod 7$

$\equiv 2$

$5 \cdot 3 = 15 \equiv 1 \mod 7$

$5^{-1} \equiv 3 \mod 7$

Sum: $5 \mod 7$

Theorem (Chinese Remainder Theorem (CRT)). *If* $\gcd(m_1, m_2) = 1$, *then for any choice of integers* a_1 *and* a_2, *there exists a solution to the simultaneous congruences*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \end{aligned}$$

Moreover, if $n = n_0$ *is one integer solution, then the complete solution is* $n \equiv n_0 \pmod{m_1 m_2}$.

Theorem (Generalized CRT (GCRT)). *If* $m_1, m_2, \ldots, m_k$ *are integers and* $\gcd(m_i, m_j) = 1$ *whenever* $i \neq j$, *then for any choice of integers* $a_1, a_2, \ldots, a_k$, *there exists a solution to the simultaneous congruences*

$$\begin{aligned} n &\equiv a_1 \pmod{m_1} \\ n &\equiv a_2 \pmod{m_2} \\ &\vdots \\ n &\equiv a_k \pmod{m_k} \end{aligned}$$

Moreover, if $n = n_0$ *is one integer solution, then the complete solution is*

$$n \equiv n_0 \pmod{m_1 m_2 \ldots m_k}$$

Solve $x \equiv 5 \mod 6$ (1)

$x \equiv 2 \mod 7$ (2)

$x \equiv 3 \mod 11$ (3)

From (1) $x = 5 + 6k$ for some $k \in \mathbb{Z}$.

Plug into (2) $5 + 6k \equiv 2 \mod 7$

$6k \equiv -3 \mod 7$

$-k \equiv -3 \mod 7$

$k \equiv 3 \mod 7$

$k = 3 + 7l$ for some $l \in \mathbb{Z}$

$\therefore x = 5 + 6(3 + 7l)$

$= 23 + 42l.$ (4)

$\therefore x \equiv 23 \mod 42$

Now we need to solve

$x \equiv 23 \mod 42$

$x \equiv 3 \mod 11$ (3)

Plug (4) into (3)

$$23+42l \equiv 3 \mod 11$$

$$-2l \equiv -20 \mod 11$$

Use CD valid $\because \gcd(-2,11)=1$

$$l \equiv 10 \mod 11$$

$\therefore l = 10+11m$ for some $m \in \mathbb{Z}$.

$\because x \equiv 23+\cancel{42}\,42l$,

$$\Rightarrow x = 23+42(10+11m)$$

$$= 443+462m$$

$$\therefore x \equiv 443 \mod 462$$

Twists

Solve $3x \equiv 2 \mod 5$

$2x \equiv 6 \mod 7$

Mult by 2 $6x \equiv 4 \mod 5$

$x \equiv 4 \mod 5$

mult. by 4 $8x \equiv 24 \mod 7$

$x \equiv 3 \mod 7$

Twist 2:

$x \equiv 4 \mod 6 \quad (1)$

$x \equiv 2 \mod 8 \quad (2)$

(1) $\Rightarrow$ $x = 4 + 6k$ for some $k \in \mathbb{Z}$.

Into (2): $4 + 6k \equiv 2 \mod 8$

$6k \equiv -2 \mod 8$

$6k \equiv 6 \mod 8$

Clearly $k = 1$ is a solution.

LCT1 says $k \equiv 1 \mod \frac{8}{\gcd(6,8)}$ gives ALL solutions

$k \equiv 1 \mod 4$

$k = 1 + 4l$ for some $l \in \mathbb{Z}$.

$\therefore x = 4 + 6(1 + 4l)$

$= 10 + 24l$

$\therefore x \equiv 10 \mod 24$

Example: Solve $x^2 \equiv 34 \mod 99$

This implies $99 \mid x^2 - 34$

Note $9 \mid 99$ $\therefore 9 \mid x^2 - 34$ by transitivity

$\Rightarrow x^2 \equiv 34 \mod 9$

Note $11 \mid 99$ $\therefore 11 \mid x^2 - 34$ by transitivity

$\Rightarrow x^2 \equiv 34 \mod 11$

$\Rightarrow x^2 \equiv 1 \mod 11$

$\Rightarrow x \equiv \pm 1 \mod 11$

Similarly $x^2 \equiv 34 \equiv 7 \mod 9 \Rightarrow x \equiv \pm 4 \mod 9$.

This gives 4 systems of equations:

$$\begin{cases} x \equiv 1 \mod 11 \\ x \equiv 4 \mod 9 \end{cases} \qquad \begin{cases} x \equiv 1 \mod 11 \\ x \equiv -4 \mod 9 \end{cases}$$

$$\begin{cases} x \equiv -1 \mod 11 \\ x \equiv 4 \mod 9 \end{cases} \qquad \begin{cases} x \equiv -1 \mod 11 \\ x \equiv -4 \mod 9 \end{cases}$$

Use CRT 4 times.

(Sol'n $x \equiv 23, 32, 67, 76 \mod 99$)

Splitting the Modulus (SM)

Let m, n be coprime positive integers. Then for any integers x, a,

$$\begin{matrix} x \equiv a \mod m \\ x \equiv a \mod n \end{matrix} \text{ (simultaneously)} \iff x \equiv a \mod mn$$