# MATH 135: Final Review Session.

1. Prove the Freshman's Dream:

Let $n \in \mathbb{Z}$. Prove that $(a+b)^n \equiv a^n + b^n \pmod{n}$ $\forall a,b \in \mathbb{Z}$.

Proof By the Binomial Theorem

$$(a+b)^n \equiv \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \pmod{n}$$

$$\equiv \binom{n}{n} a^n b^0 + \binom{n}{0} a^0 b^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i b^{n-i} \pmod{n}$$

$$\equiv a^n + b^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i b^{n-i} \pmod{n}$$

$$\equiv a^n + b^n + \sum_{i=1}^{n-1} \frac{n!}{(n-i)!\, i!} a^i b^{n-i} \pmod{n}$$

$$\equiv a^n + b^n + \sum_{i=1}^{n-1} \left(\frac{(n-1)!}{(n-i)!\, i!}\right) n\, a^i b^{n-i} \pmod{n}$$

$$\equiv a^n + b^n + \sum_{i=1}^{n-1} 0 \pmod{n}$$

$$\equiv a^n + b^n \pmod{n}$$

$\square$

?. Solve the following system of linear congruences:

$$4x \equiv 7 \pmod 9$$
$$3x \equiv 2 \pmod{11}$$

Soln

$\Rightarrow$ $x \equiv 4^{-1} \cdot 7 \pmod 9$ $\qquad 4^{-1} \equiv 7 \pmod 9$
$x \equiv 3^{-1} \cdot 2 \pmod{11}$ $\qquad 3^{-1} \equiv 4 \pmod{11}$

$\Rightarrow$ $x \equiv 4 \pmod 9$ (1)
$x \equiv 8 \pmod{11}$ (2)

(1) $\Rightarrow$ $x = 4 + 9y$ for some $y \in \mathbb{Z}$.

Substituting into (2), we obtain

$$4 + 9y \equiv 8 \pmod{11}$$

$\Rightarrow$ $y \equiv 9^{-1} \cdot 4 \pmod{11}$ $\qquad 9^{-1} \equiv 5 \pmod{11}$

$\Rightarrow$ $y \equiv 9 \pmod{11}$

Thus $x = 4 + 9 \cdot 9 = 85$

$\therefore$ the complete set of solutions is $x \equiv 85 \pmod{99}$ by CRT.

3. Solve the following system of congruences.

$$x^3 \equiv 0 \pmod{8} \qquad (3)$$
$$3x^2 \equiv 3 \pmod{9} \qquad (2)$$
$$2x \equiv 0 \pmod{10} \qquad (1)$$

<u>Soln</u> (1) gives us $x \equiv 0 \pmod 5$

(3) gives us what? $x \equiv 0 \pmod 2$

Combining those, gives us $x \equiv 0 \pmod{10}$

$\Rightarrow x = 10y$ for some $y \in \mathbb{Z}$.

| $x$ | 0 | 1 | 2 | 3 | 4 | -4 | -3 | -2 | -1 |
|---|---|---|---|---|---|---|---|---|---|
| $3x^2$ | 0 | 3 | 3 | 0 | 3 | 3 | 0 | 3 | 3 |

(2) gives $x \equiv \pm 1, \pm 2, \pm 4 \pmod 9$

Substituting $x = 10y$ gives

$$10y \equiv \pm 1, \pm 2, \pm 4 \pmod 9$$

$$\Rightarrow y \equiv \pm 1, \pm 2, \pm 4 \pmod 9$$

$\therefore x \equiv 10, 20, 40, 50, 70, 80 \pmod{90}$ by GCRT

4. Define a sequence as follows:

$a_0 = 3$, $a_1 = 7$, $a_n = 5(a_{n-1} + a_{n-2}) + 4a_{n-1}^2 + 1$

Prove that $a_n \equiv 3 \pmod 4$ $\forall n \in \mathbb{N}$. Let $P(n)$ be the statement $a_n \equiv 3 \pmod 4$

Proof

Base Cases

$a_0 \equiv 3 \pmod 4$

$a_1 \equiv 7 \pmod 4$

$\Rightarrow a_1 \equiv 3 \pmod 4$

IH Suppose $P(k)$ is true $\forall k < n$, $n \geq 2$.

IS $a_n \equiv 5(a_{n-1} + a_{n-2}) + 4a_{n-1}^2 + 1 \pmod 4$

$\equiv a_{n-1} + a_{n-2} + 0 + 1 \pmod 4$

$\equiv 3 + 3 + 1 \pmod 4$ by (IH)

$\equiv 3 \pmod 4$.

Thus the result follows by POSI.

7. Prove that $n^7 - n$ is divisible by 42 $\forall n \in \mathbb{Z}$.

Proof $7 \cdot 3 \cdot 2 = 42.$

We examine
$$n^7 - n \mod 7$$
$$n^7 - n \mod 3$$
$$n^7 - n \mod 2$$

$$\Rightarrow \quad n^7 - n \equiv n - n \equiv 0 \pmod{7} \quad \text{by FLT}$$
$$n^7 - n \equiv n - n \equiv 0 \pmod{3}$$
$$n^7 - n \equiv n - n \equiv 0 \pmod{2}$$

$\therefore$ by SMT $n^7 - n \equiv 0 \pmod{42}$