MTH26001 - Elementary Number theory.

Name: Nguyen Minh Duc

Student ID: 20202026.

I affirm that I will not give or recieve any unauthorized help on this exam, and that all work will be my own. Sign: MDuc

Final Exam

Problem 1.

~~We have: 5.28!≡~~

- Note that 31 is prime, by Wilson's theorem,

$$30! \equiv -1 \pmod{31}.$$

$$\Rightarrow 28! \cdot 29 \cdot 30 \equiv -1 \pmod{31}$$

$$\Rightarrow 28!(-2)(-1) \equiv -1 \pmod{31}$$

$$\Rightarrow 28! \cdot 2 \equiv -1 \pmod{31}$$

$$\Rightarrow 28! \cdot 30 \equiv -15 \pmod{31}$$

$$\Rightarrow 28!(-1) \equiv -15 \pmod{31}$$

$$\Rightarrow 28! \equiv 15 \pmod{31}$$

$$\Rightarrow 28! \cdot 5 \equiv 75 \pmod{31}$$

$$\Rightarrow 5 \cdot 28! \equiv 13 \pmod{31}.$$

- Thus, the remainder is 13.

Problem 2.

- Since 2 is a primitive root of 13, we have: $ord_{13}(2) = \phi(13) = 12$.

$$\Rightarrow 2^{\phi(13)} \equiv 2^{12} \equiv 1 \pmod{13}.$$

and $2^1, 2^2, \dots, 2^{11}, 2^{12}$ are incongruent and they are congruent to $1, 2, \dots, 12$ in some order.

- Note that $2^1 \equiv 2 \pmod{13} \Rightarrow 2^2 \equiv 4 \pmod{13} \Rightarrow ind_2 4 = 2$.

Now, $2^{12} \equiv 1 \pmod{13} \Rightarrow 2^{11} \cdot (2) \equiv 1 \pmod{13}$

~~$\Rightarrow 2^{11}$ ...~~

$$\Rightarrow 2^{11} \cdot (12) \equiv 6 \pmod{13}$$

$$\Rightarrow 2^{11} \cdot (-1) \equiv 6 \pmod{13}$$

$$\Rightarrow 2^{11} \equiv -6 \equiv 7 \pmod{13} \Rightarrow ind_2 7 = 11.$$

⊛. Consider the congruence:

$$4x^9 \equiv 7 \pmod{13}. \quad ; \ 13 \text{ is prime.}$$

Taking both side index of 2, we have:

$$\text{ind}_2 4 + 9\,\text{ind}_2 x \equiv \text{ind}_2 7 \pmod{12}.$$

$$\Rightarrow \quad 2 + 9\,\text{ind}_2 x \equiv 11 \pmod{12}$$

$$\Rightarrow \quad 9\,\text{ind}_2 x \equiv 9 \pmod{12}$$

$$\Rightarrow \quad \text{ind}_2 x \equiv 1 \pmod{12}.$$

$$\Rightarrow \quad x \equiv 2 \pmod{12}.$$

⊛ Therefore, the solution is $x \equiv 2 \pmod{12}$.

Problem 3.

⊛ Note that $109 = 9 + 100 \Rightarrow 109 = 3^2 + 10^2$.

⊛ Consider the congruence: $x^2 + 2x + 2 \equiv 0 \pmod{109}$

$$\Rightarrow (x+1)^2 + 1 \equiv 0 \pmod{109}$$

$$\Rightarrow (x+1)^2 \equiv -1 \pmod{109}.$$

⊛. Note that 109 is prime.

⊛ Euler criteria: $(-1)^{\frac{109-1}{2}} \equiv (-1)^{108/2} \equiv (-1)^{54} \equiv 1 \pmod{109}$

$\Rightarrow -1$ is a quadratic residue of 109.

⊛ Now, note that $33^2 = 1089 = 10 \times 109 - 1$.

$$\Rightarrow 33^2 \equiv -1 \pmod{109} \quad \text{— (1)}$$

$$\Rightarrow (109-33)^2 \equiv -1 \pmod{109}$$

$$\Rightarrow 76^2 \equiv -1 \pmod{109} \quad \text{— (2)}$$

⊛ From (1) and (2), we obtain the solution:

$x + 1 \equiv 33 \pmod{109}$ $\qquad$ $x + 1 \equiv 76 \pmod{109}$

$\Rightarrow x \equiv 32 \pmod{109}$ $\qquad$ $\Rightarrow x \equiv 75 \pmod{109}$

⊛ Therefore, solutions are:

$$x \equiv 32 \text{ or } 75 \pmod{109}.$$

Problem 4.

* Note that $\tau(n)$ and $\phi(n)$ are multiplicative.

* Let $F(n) = \sum_{d|n} \tau(n)\phi(\frac{n}{d})$.

* Firstly, let's prove $F(n)$ is multiplicative:

  Let m and n be two coprime integers $\Rightarrow \gcd(m,n)=1$.

  Let d be a divisor of $mn \Rightarrow d \mid mn$

  $\Rightarrow d = r\cdot s$, where $r \mid m$ and $s \mid n$ $(\because \gcd(m,n)=1)$.

  Now, $F(mn) = \sum_{d|mn} \tau(d)\phi(\frac{mn}{d})$

  $= \sum_{\substack{r|m \\ s|n}} \tau(rs)\phi(\frac{mn}{rs})$

  $= \sum_{\substack{r|m \\ s|n}} \tau(r)\tau(s)\phi(\frac{m}{r})\phi(\frac{n}{s})$

  $= \sum_{r|m} \tau(r)\phi(\frac{m}{r}) \sum_{s|n} \tau(s)\phi(\frac{n}{s})$

  $= F(m)F(n)$.

  $\Rightarrow F(mn) = F(m)F(n)$ whenever $\gcd(m,n)=1$.

  $\Rightarrow F(n)$ is multiplicative.

* Consider $F(p^k) = \sum_{d|p^k} \tau(d)\phi(\frac{n}{d})$

  $= \tau(1)\phi(p^k) + \tau(p)\phi(p^{k-1}) + \ldots + \tau(p^{k-1})\phi(p) + \tau(p^k)\phi(1)$.

  $= 1(p^k - p^{k-1}) + 2(p^{k-1} - p^{k-2}) + \ldots + k(p-1) + (k+1)\cdot 1$.

  $= p^k - p^{k-1} + 2p^{k-1} - 2p^{k-2} + 3p^{k-3} - 3p^{k-3} + \ldots + kp - k + k + 1$.

  $= p^k + p^{k-1} + p^{k-2} + p^{k-3} + \ldots + p + 1$.

  $= \sigma(p^k)$.

* Therefore, by factorizing $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ where p_i is prime and $k_i \geq 1$, we have:

  $F(n) = F(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) = F(p_1^{k_1})F(p_2^{k_2})\cdots F(p_r^{k_r}) = \sigma(p_1^{k_1})\sigma(p_2^{k_2})\cdots\sigma(p_r^{k_r})$

  $= \sigma(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r})$ $(\because \sigma(n)$ is multiplicative$)$

  $= \sigma(n)$

* Thus, $\sum_{d|n} \tau(d)\phi(\frac{n}{d}) = \sigma(n)$.

Problem 5.

$$y^2 \equiv x^3 + x + 1 \pmod 7.$$

- Considering the following table:

$x \bmod 7$	0	1	2	3	4	5	6
$x^3+x+1 \bmod 7$	1	3	4	3	6	5	6

$\Rightarrow x^3+x+1 \in \{1, 3, 4, 5, 6\}$.

- Checking quadratic residue: $1^{\frac{7-1}{2}} \equiv 1 \pmod 7 \to$ ~~choose~~ Yes

$3^{\frac{7-1}{2}} \equiv 3^3 \equiv 27 \equiv 6 \equiv -1 \pmod 7 \to$ No

$4^{\frac{7-1}{2}} \equiv 4^3 \equiv 64 \equiv 1 \pmod 7 \to$ Yes

$5^{\frac{7-1}{2}} \equiv 5^3 \equiv 125 \equiv 6 \equiv -1 \pmod 7 \to$ No

$6^{\frac{7-1}{2}} \equiv 6^3 \equiv 216 \equiv 6 \equiv -1 \pmod 7 \to$ No.

- Thus, $y^2 \equiv 1$ or $4 \pmod 7$

$\Rightarrow y \equiv \pm 1$ or $\pm 2 \pmod 7$

- Therefore, the solutions are:

$(x, y) \in \{(0,1), (0,-1), (2,2), (2,-2)\}$.