MTH26001- Elementary Number Theory.

Student ID: 20202026

Student Name: Nguyen Minh Duc

ASSIGNMENT 3

Sec 4.2.

Problem 3.

⊗ Since $a \equiv b \pmod{n}$, $a - b = nk$ $(k \in \mathbb{Z})$

$\Rightarrow a = b + nk$.

⊗ Note that $\gcd(b,n) \mid b$ and $\gcd(b,n) \mid n$.

$\Rightarrow b + nk \equiv 0 \pmod{\gcd(b,n)}$.

$\Rightarrow a \equiv 0 \pmod{\gcd(b,n)}$.

$\left.\begin{array}{l}\Rightarrow \gcd(b,n) \mid a. \\ \text{Moreover, } \gcd(b,n) \mid n\end{array}\right\} \Rightarrow \gcd(b,n)$ is a divisor of both a and n.

$\Rightarrow \gcd(b,n) \leq \gcd(a,n)$. — ①.

⊗ Similarly, we have: $b = a - nk$ $(\because a - b = nk, k \in \mathbb{Z})$.

Note that $\gcd(a,n) \mid b$ and $\gcd(a,n) \mid n$.

$\Rightarrow a - nk \equiv 0 \pmod{\gcd(a,n)}$.

$\Rightarrow b \equiv 0 \pmod{\gcd(a,n)}$.

$\left.\begin{array}{l}\Rightarrow \gcd(a,n) \mid b. \\ \text{Moreover, } \gcd(a,n) \mid n\end{array}\right\} \Rightarrow \gcd(a,n)$ is a divisor of both b and n.

$\Rightarrow \gcd(a,n) \leq \gcd(b,n)$. — ②.

⊗ ① and ② $\Rightarrow \gcd(a,n) = \gcd(b,n)$

Problem 5.

⊗ Prove $53^{103} + 103^{53} \equiv 0 \pmod{39}$.

Note that: $53^2 = 2704 = 72 \times 39 + 1$. $\Rightarrow 53^2 \equiv 1 \pmod{39}$

$\Rightarrow 53^{102} \equiv 1 \pmod{39}$

$\Rightarrow 53^{103} \equiv 53 \equiv 14 \pmod{39}$.

Note that: $103^2 = 10609 = 272 \times 39 + 1$ $\Rightarrow 103^2 \equiv 1 \pmod{39}$

$\Rightarrow 103^{52} \equiv 1 \pmod{39}$

$\Rightarrow 103^{53} \equiv 103 \equiv 25 \pmod{39}$.

Thus, $53^{103} + 103^{53} \equiv 14 + 25 \equiv 39 \equiv 0 \pmod{39}$

$\Rightarrow 53^{103} + 103^{53}$ is divisible by 39.

⊛ Prove $111^{333} + 333^{111} \equiv 0 \pmod 7$.

Note that $111^2 = 12321 = 1760 \times 7 + 1 \Rightarrow 111^2 \equiv 1 \pmod 7$

$\Rightarrow 111^{332} \equiv 1 \pmod 7$

$\Rightarrow 111^{333} \equiv 111 \equiv 6 \pmod 7$.

Note that $333 = 47 \times 7 + 4 \Rightarrow 333 \equiv 4 \pmod 7$.

$\Rightarrow 333^3 \equiv 4^3 \pmod 7$

$\Rightarrow 333^3 \equiv 64 \equiv 1 \pmod 7$.

$\Rightarrow 333^{111} \equiv 1 \pmod 7$

Thus, $111^{333} + 333^{111} \equiv 6 + 1 \equiv 7 \equiv 0 \pmod 7$

$\Rightarrow 111^{333} + 333^{111}$ is divisible by 7.

Problem 11.

⊛ We have the following table:

x	0	1	2	$2^2=4$	$2^3=8$	$2^4=16$	$2^5=32$	$2^6=64$	$2^7=128$	$2^8=256$	$2^9=512$
x mod 11	0	1	2	4	8	5	10	9	7	3	6

All of the "x mod 11" are distinct and ranging from 0 to 10.

$\Rightarrow \{0, 1, 2, 2^2, 2^3, \ldots, 2^9\}$ forms a complete set of residues modulo 11.

⊛. Consider~~ing~~ the following table:

x	0	$1^2=1$	$2^2=4$	$3^2=9$	$4^2=16$	$5^2=25$	$6^2=36$	$7^2=49$	$8^2=64$	$9^2=81$	$10^2=100$
x mod 11	0	1	4	9	5	3	3	5	9	4	1

There are missing 2, 6, 7 and 8 in "x mod 11" row.

There are not a complete set of residues modulo 11.

$\Rightarrow \{0, 1^2, 2^2, \ldots, 10^2\}$ does not form a complete set of residues modulo 11.

Sec 4.3

Problem 3.

⊗ From the hint $\begin{cases} 9^9 \equiv 9 \pmod{10} \Rightarrow 9^9 = 10k+9,\ k \in \mathbb{Z}. \\ 9^9 \equiv 89 \pmod{100}. \end{cases}$

⊗ Consider: $9^{9^9} = 9^{10k+9} = (9^{10})^k \times 9^9 = (9 \times 9^9)^k \times 9^9 \cancel{\equiv (9\times 89)^k \times 89}$

$$\equiv (9 \times 89)^k \times 89 \pmod{100}$$
$$\equiv (801)^k \times 89 \pmod{100}$$
$$\equiv 1^k \times 89 \pmod{100}$$
$$\equiv 89 \pmod{100}$$

Thus, the last two digits of 9^{9^9} are 89.

Problem 10.

⊗ Let N be such integer. Decimal representation of N:

$$N = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 10 + a_0.$$

Note that $10 \equiv 1 \pmod 9 \Rightarrow 10^x \equiv 1 \pmod 9\ \forall x \in \mathbb{N}$.

Hence, $N \equiv a_n + a_{n-1} + \dots + a_0 \pmod 9$.

$\Rightarrow N \equiv 15 \pmod 9$ ($\because$ sum of digits of N is 15).

$\Rightarrow N \equiv 6 \pmod 9$.

⊗. From the hint, $a^3 \equiv 0, 1$ or $8 \pmod 9$ $\forall a \in \mathbb{Z}$. $\Rightarrow$ Any cube is congruent to 0, 1 or 8 modulo 9. However, $N \equiv 6 \pmod 9$. Thus, N can't be a cube —— (1).

⊗ Let $a \in \mathbb{Z}$, $a = 9q + r$ ($q \in \mathbb{Z}$, $0 \le r < 9$). $\Rightarrow a \equiv r \pmod 9$.
$\Rightarrow a^2 \equiv r^2 \pmod 9$.

For $r = 1$, $a^2 \equiv 1 \pmod 9$
For $r = 2$, $a^2 \equiv 2^2 \equiv 4 \pmod 9$
For $r = 3$, $a^2 \equiv 3^2 \equiv 9 \equiv 0 \pmod 9$
For $r = 4$, $a^2 \equiv 4^2 \equiv 16 \equiv 7 \pmod 9$
For $r = 5$, $a^2 \equiv 5^2 \equiv 25 \equiv 7 \pmod 9$
For $r = 6$, $a^2 \equiv 6^2 \equiv 36 \equiv 0 \pmod 9$
For $r = 7$, $a^2 \equiv 7^2 \equiv 49 \equiv 4 \pmod 9$
For $r = 8$, $a^2 \equiv 8^2 \equiv 64 \equiv 1 \pmod 9$.
For $r = 0$, $a^2 \equiv 0 \pmod 9$

$\Rightarrow a^2 \equiv 0, 1, 4$ or $7 \pmod 9$.

Thus, any square is congruent to 0, 1, 4 or 7 modulo 9. However, $N \equiv 6 \pmod 9$.
$\Rightarrow N$ can't be a square —— (2).

⊗ From (1) and (2), N can't be a square or a cube.

Problem 11.

- $\overline{273x49y5} = 273\times10^5 + x\times10^4 + 49\times10^2 + y10 + 5$.

Note that $10 \equiv 10 \pmod{495} \Rightarrow 10^2 \equiv 100 \pmod{495}$

$\Rightarrow 10^4 \equiv 10000 \equiv 20\times495+100 \equiv 100 \pmod{495}$

$\Rightarrow 10^5 \equiv 10^4\times10 \equiv 1000 \equiv 10 \pmod{495}$.

- Hence, $\overline{273x49y5} \equiv 273\times10 + 100x + 49\times100 + 10y + 5 \pmod{495}$

$\equiv 100x + 10y + 7635 \pmod{495}$

$\equiv 100x + 10y + 210 \pmod{495}$.

$\equiv \overline{xy0} + 210 \pmod{495}$.

- Since $\overline{273x49y5}$ is divisible by 495, $\overline{xy0} + 210 \equiv 0 \pmod{495}$.

$\Rightarrow \overline{xy0} + 210 = 495k,\ k\in\mathbb{Z}$.

- Note that $0 < \overline{xy0} + 210 \leq 990 + 210 = 1200$.

$\Rightarrow 0 < 495k \leq 1200$

$\Rightarrow 0 < k \leq \frac{1200}{495} \approx 2.42$

$\Rightarrow k \in \{1, 2\}$ ($\because k\in\mathbb{Z}$).

- For $k=1$, $\overline{xy0} + 210 = 495 \Rightarrow \overline{xy0} = 285 \Rightarrow \begin{cases} x=2 \\ y=8 \\ 0=5 \end{cases}$ (constradiction)

$\Rightarrow$ No solution.

For $k=2$, $\overline{xy0} + 210 = 495\times2 = 990 \Rightarrow \overline{xy0} = 780 \Rightarrow \begin{cases} x=7 \\ y=8 \\ 0=0 \end{cases}$ (satisfy).

Therefore, $(x,y) = (7,8)$.

Problem 25.

- For a prime $p>3$, p has the form of $6k+1$ or $6k+5$, $k\in\mathbb{Z}$.
- Consider: $10^5 = 7692\times13+4 \equiv 4 \pmod{13}$.

$\Rightarrow 10^6 \equiv 40 \equiv 1 \pmod{13}$

$\Rightarrow 10^{6k} \equiv 1 \pmod{13}$

$\Rightarrow \begin{cases} 10^{6k+1} \equiv 10 \pmod{13} \\ 10^{6k+5} \equiv 4 \pmod{13}. \end{cases}$

- For $p=6k+1$, $10^{2p}+10^p+1 = 10^{2(6k+1)} - 10^{6k+1} + 1 \equiv 10^2 - 10 + 1 \pmod{13}$

$\equiv 91 \pmod{13}$

$\equiv 0 \pmod{13}$.

$\hookrightarrow 13 \mid 10^{2p}+10^p+1$.

⊗ For $p = 6k+5$, $10^{2p} - 10^{p} + 1 = 10^{2(6k+5)} - 10^{6k+5} + 1 \equiv 4^2 - 4 + 1 \pmod{13}$
$\equiv 13 \pmod{13}$
$\equiv 0 \pmod{13}$

$\hookrightarrow 13 \mid 10^{2p} - 10^{p} + 1$.

⊗ Therefore, $13 \mid 10^{2p} - 10^{p} + 1$, for any prime $p > 3$.

Sec 4.4.

Problem 2 (b). $12x + 25y = 331$.

$$\Rightarrow \begin{cases} 12x = -25y + 331 \\ 25y = -12x + 331 \end{cases} \Rightarrow \begin{cases} 12x \equiv 331 \pmod{25} & (1) \\ 25y \equiv 331 \pmod{12} & (2). \end{cases}$$

⊗ Consider equation (1), $12x \equiv 331 \pmod{25}$.

$\Rightarrow 12x \equiv 6 \pmod{25}$

$\Rightarrow 24x \equiv 12 \pmod{25}$

$\Rightarrow -x \equiv 12 \pmod{25}$ $(\because 24 \equiv -1 \pmod{25})$.

$\Rightarrow x \equiv -12 \equiv 13 \pmod{25} \Rightarrow x = 13 + 25t, t \in \mathbb{Z}$.

⊗ Consider equation (2), $25y \equiv 331 \pmod{12}$.

$\Rightarrow y \equiv 7 \pmod{12}$ $(\because 25 \equiv 1 \pmod{12})$

$\Rightarrow y = 7 + 12s, s \in \mathbb{Z}$.

⊗ Now, we obtain: $12x + 25y = 331 \Rightarrow 12(13+25t) + 25(7+12s) = 331$.

$\Leftrightarrow 300t + 300s + 331 = 331$.

$\Leftrightarrow t + s = 0 \Leftrightarrow s = -t$.

⊗ General solution: $\begin{cases} x = 13 + 25t \\ y = 7 - 12t \end{cases}, t \in \mathbb{Z}$.

Problem 3. $3x - 7y \equiv 11 \pmod{13}$.

⊗. Check the solvability: $\gcd(3, 7, 13) = 1 \mid 11$.

$\Rightarrow$ The equation has a solution.

⊗. $3x - 7y \equiv 11 \pmod{13} \Rightarrow 3x \equiv 11 + 7y \pmod{13}$.

$\Rightarrow 12x \equiv 44 + 28y \pmod{13}$

$\Rightarrow -x \equiv 5 + 2y \pmod{13}$ $(\because 12 \equiv -1 \pmod{13})$

$\Rightarrow x \equiv -5 - 2y \pmod{13}$

$\Rightarrow x \equiv 8 + 11y \pmod{13}$.

⊗ We have the solution table: (mod 13)

y	0	1	2	3	4	5	6	7	8	9	10	11	12
x	8	6	4	2	0	11	9	7	5	3	1	12	10

Problem 4.

(a) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$. $N = 3 \times 5 \times 7 = 105$

$N_1 = \frac{105}{3} = 35$, $N_2 = \frac{105}{5} = 21$, $N_3 = \frac{105}{7} = 15$.

Now, we have 3 congruences: $35x \equiv 1 \pmod 3$, $21x \equiv 1 \pmod 5$, $15x \equiv 1 \pmod 7$

* $35x \equiv 1 \pmod 3$

$\Rightarrow -x \equiv 1 \pmod 3$ ($\because 35 \equiv -1 \pmod 3$)

$\Rightarrow x \equiv -1 \pmod 3$

$\Rightarrow x \equiv 2 \pmod 3$

* $21x \equiv 1 \pmod 5$

$\Rightarrow x \equiv 1 \pmod 5$ ($\because 21 \equiv 1 \bmod 5$)

* $15x \equiv 1 \pmod 7$

$\Rightarrow x \equiv 1 \pmod 7$ ($\because 15 \equiv 1 \bmod 7$).

* Thus, we obtain $(x_1, x_2, x_3) = (2, 1, 1)$.
* Solution: $x \equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 \pmod{105}$

$\Rightarrow x \equiv 157 \pmod{105}$

$\Rightarrow x \equiv 52 \pmod{105}$.

(b) $\begin{cases} x \equiv 5 \pmod{11} \\ x \equiv 14 \pmod{29} \\ x \equiv 15 \pmod{31} \end{cases}$. $N = 11 \times 29 \times 31 = 9889$

$N_1 = 899$, $N_2 = 341$, $N_3 = 319$.

$899x \equiv 1 \pmod{11}$

$\Rightarrow 8x \equiv 1 \pmod{11}$

$\Rightarrow 32x \equiv 4 \pmod{11}$

$\Rightarrow -x \equiv 4 \pmod{11}$

$\Rightarrow x \equiv -4 \pmod{11}$

$341x \equiv 1 \pmod{29}$

$\Rightarrow 22x \equiv 1 \pmod{29}$

$\Rightarrow -7x \equiv 1 \pmod{29}$

$\Rightarrow -28x \equiv 4 \pmod{29}$

$\Rightarrow x \equiv 4 \pmod{29}$

$319x \equiv 1 \pmod{31}$

$\Rightarrow 9x \equiv 1 \pmod{31}$

$\Rightarrow 63x \equiv 7 \pmod{31}$

$\Rightarrow x \equiv 7 \pmod{29}$

* Thus, we obtain $(x_1, x_2, x_3) = (-4, 4, 7)$.
* Solution: $x \equiv 5 \times 899 \times (-4) + 14 \times 341 \times 4 + 15 \times 319 \times 7 \pmod{9889}$

$\Rightarrow x \equiv 34611 \pmod{9889}$

$\Rightarrow x \equiv 4944 \pmod{9889}$.

(c) $\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 4 \pmod{11} \\ x \equiv 3 \pmod{17} \end{cases}$ $N = 6 \times 11 \times 17 = 1122$.

$N_1 = 187$, $N_2 = 102$, $N_3 = 66$.

$187x \equiv 1 \pmod 6$

$\Rightarrow x \equiv 1 \pmod 6$

$102x \equiv 1 \pmod{11}$

$\Rightarrow 3x \equiv 1 \pmod{11}$

$\Rightarrow 21x \equiv 7 \pmod{11}$

$\Rightarrow -x \equiv 7 \pmod{11}$

$\Rightarrow x \equiv -7 \pmod{11}$

$66x \equiv 1 \pmod{17}$

$\Rightarrow -2x \equiv 1 \pmod{17}$

$\Rightarrow 18x \equiv -9 \pmod{17}$.

$\Rightarrow x \equiv -9 \pmod{17}$

* Thus, we obtain $(x_1, x_2, x_3) = (1, -7, -9)$
* Solution: $x \equiv 5 \times 187 \times 1 + 4 \times 102 \times (-7) + 3 \times 66 \times (-9) \pmod{1122}$

$\Rightarrow x \equiv -3703 \pmod{1122}$

$\Rightarrow x \equiv 785 \pmod{1122}$.

(d) $\begin{cases} 2x \equiv 1 \pmod 5 \Rightarrow 4x \equiv 2 \pmod 5 \Rightarrow -x \equiv 2 \pmod 5 \Rightarrow x \equiv -2 \pmod 5 \\ 3x \equiv 9 \pmod 6 \Rightarrow x \equiv 3 \pmod 2 \\ 4x \equiv 1 \pmod 7 \Rightarrow 8x \equiv 2 \pmod 7 \Rightarrow x \equiv 2 \pmod 7 \\ 5x \equiv 9 \pmod{11} \Rightarrow 10x \equiv 18 \pmod{11} \Rightarrow -x \equiv 7 \pmod{11} \Rightarrow x \equiv -7 \pmod{11} \end{cases}$

New system: $\begin{cases} x \equiv -2 \pmod 5 \\ x \equiv 3 \pmod 2 \\ x \equiv 2 \pmod 7 \\ x \equiv -7 \pmod{11} \end{cases}$

$N = 5 \times 2 \times 7 \times 11 = 770.$

$N_1 = 154 \quad N_2 = 385$

$N_3 = 110 \quad N_4 = 70.$

$154x \equiv 1 \pmod 5$	$385x \equiv 1 \pmod 2$	$110x \equiv 1 \pmod 7$	$70x \equiv 1 \pmod{11}$
$\Rightarrow -x \equiv 1 \pmod 5$	$\Rightarrow x \equiv 1 \pmod 2$	$\Rightarrow 5x \equiv 1 \pmod 7$	$\Rightarrow 4x \equiv 1 \pmod{11}$
$\Rightarrow x \equiv -1 \pmod 5$		$\Rightarrow 15x \equiv 3 \pmod 7$	$\Rightarrow 12x \equiv 3 \pmod{11}$
		$\Rightarrow x \equiv 3 \pmod 7$	$\Rightarrow x \equiv 3 \pmod{11}$

- Thus, we obtain $(x_1, x_2, x_3, x_4) = (-1, 1, 3, 3)$.
- Solution: $x \equiv -2 \times 154 \times (-1) + 3(385) \times 1 + 2 \times 110 \times 3 + -7 \times 70 \times 3 \pmod{770}$

$\Rightarrow x \equiv 653 \pmod{770}$

Problem 11.

- ($\Rightarrow$) Let's suppose a solution exists.

Let $d = \gcd(n, m) \Rightarrow \begin{cases} n = dr \\ m = ds \end{cases}$ $(r, s \in \mathbb{Z})$.

we have: $\begin{cases} x \equiv a \pmod n \\ x \equiv b \pmod m \end{cases} \Rightarrow \begin{cases} x = a + nt \\ x = b + mk \end{cases}$ $(t, k \in \mathbb{Z})$.

$\Rightarrow a + nt = b + mk.$

$\Rightarrow a - b = mk - nt.$

$\Rightarrow a - b = drk - dst \quad (\because \begin{cases} n = dr \\ m = ds \end{cases})$.

$\Rightarrow a - b = d(rk - st).$

$\Rightarrow a - b = d(rk-st) \Rightarrow \gcd(n, m) \mid a - b.$ —— (1).

$\Rightarrow d \mid a - b$

- ($\Leftarrow$) Let $d = \gcd(n, m)$. Suppose $d \mid a - b$. $\Rightarrow a - b = dk, k \in \mathbb{Z}$.
- Since $d = \gcd(n, m)$, $\exists x_0, y_0 : nx_0 + my_0 = d$.

$\Rightarrow nx_0 k + my_0 k = dk = a - b.$

$\Rightarrow my_0 k + b = a - nx_0 k.$

Let $x = b + (y_0 k)m = a - (x_0 k)n.$ —— (2).

$\Rightarrow \begin{cases} x \equiv a \pmod n \\ x \equiv b \pmod m \end{cases}$. $\Rightarrow$ There is a simultaneous solution.

- Uniqueness: Let y be other solution, i.e. $\begin{cases} y \equiv a \pmod n \\ y \equiv b \pmod m \end{cases}$.

then, we have: $\begin{cases} x \equiv y \equiv a \pmod n \\ x \equiv y \equiv b \pmod m \end{cases}$

$$\Rightarrow \begin{cases} x-y \equiv 0 \pmod n \\ x-y \equiv 0 \pmod m \end{cases} \Rightarrow \begin{cases} n \mid x-y \\ m \mid x-y \end{cases}$$

$$\Rightarrow \operatorname{lcm}(n,m) \mid x-y.$$

$$\Rightarrow x-y \equiv 0 \pmod{\operatorname{lcm}(n,m)}$$

$$\Rightarrow x \equiv y \pmod{\operatorname{lcm}(n,m)}$$

- Thus, From ① and ①, ~~∃~~ there exists simultaneous solution iff $\gcd(n,m) \mid a-b$ and it is unique under modulo $\operatorname{lcm}(n,m)$.