

HW 2.

1. if $\{xy: x \in [a], y \in [b]_n\} = [ab]_n$
 then $\{xy: x \in [a], y \in [b]_n\} \subseteq [ab]_n$
 and $[ab]_n \subseteq \{xy: x \in [a]_n, y \in [b]_n\}$

We can disprove that as follows:

$$\forall x \in [a]_n \quad y \in [b]_n$$

$$\text{let } x = k_1n + a \quad y = k_2n + b$$

$$xy = (k_1n + a)(k_2n + b) = k_1k_2n^2 + (ak_2 + bk_1)n + ab$$

$$\text{so } xy \in [ab]_n$$

$$\text{so } [ab]_n \supseteq \{xy: x \in [a]_n, y \in [b]_n\}$$

On the other side:

$$\forall x \in [ab]_n \quad \text{let } x = k_3n + ab$$

$$\text{let } n=5 \quad a=2 \quad b=3. \quad ab=6 \quad [b]_5 = [1]_5 \quad \text{so } x = 5k_3 + 1$$

$$\text{let } x = 5m_1 + 2 \quad y = 5m_2 + 3$$

$$\text{let } k_3 = 6. \quad \text{so } x = 5 \times 6 + 1 = 31$$

$$\text{if } [ab]_n \subseteq \{xy: x \in [a]_n, y \in [b]_n\}.$$

$$\Rightarrow 31 = xy = (5m_1 + 2)(5m_2 + 3).$$

$$\text{but } 31 \text{ is a prime, } 31 = 1 \times 31.$$

$$\Rightarrow \begin{cases} 5m_1 + 2 = 1 \\ 5m_2 + 3 = 31 \end{cases} \quad \text{or} \quad \begin{cases} 5m_1 + 2 = 31 \\ 5m_2 + 3 = 1 \end{cases} \quad \text{or} \quad \begin{cases} 5m_1 + 2 = -1 \\ 5m_2 + 3 = -31 \end{cases} \quad \text{or} \quad \begin{cases} 5m_1 + 2 = 31 \\ 5m_2 + 3 = -31 \end{cases}$$

but m_1, m_2 are integers. *lead to distraction!*

$$\text{so } [ab]_n \not\subseteq \{xy: x \in [a]_n, y \in [b]_n\}$$

$$\begin{aligned}
2. \quad & [1]_{23} = ([1]_{23})^{-1} \quad [2]_{23} = ([12]_{23})^{-1} \quad [3]_{23} = ([8]_{23})^{-1} \\
& [4]_{23} = ([6]_{23})^{-1} \quad [5]_{23} = ([14]_{23})^{-1} \quad [6]_{23} = ([4]_{23})^{-1} \\
& [7]_{23} = ([10]_{23})^{-1} \quad [8]_{23} = ([3]_{23})^{-1} \quad [9]_{23} = ([18]_{23})^{-1} \\
& [10]_{23} = ([7]_{23})^{-1} \quad [11]_{23} = ([21]_{23})^{-1} \quad [12]_{23} = ([2]_{23})^{-1} \\
& [13]_{23} = ([16]_{23})^{-1} \quad [14]_{23} = ([5]_{23})^{-1} \quad [15]_{23} = ([20]_{23})^{-1} \\
& [16]_{23} = ([13]_{23})^{-1} \quad [17]_{23} = ([11]_{23})^{-1} \quad [18]_{23} = ([9]_{23})^{-1} \\
& [19]_{23} = ([17]_{23})^{-1} \quad [20]_{23} = ([15]_{23})^{-1} \quad [21]_{23} = ([11]_{23})^{-1} \\
& [22]_{23} = ([22]_{23})^{-1}
\end{aligned}$$

$$\begin{aligned}
3. \quad (1) \quad & 1 \cdot 1 \equiv 1 \pmod{p} \\
& (p-1)(p-1) \equiv 1 \pmod{p}
\end{aligned}$$

suppose that $k \cdot k \equiv 1 \pmod{p}$ $1 < k < p-1$

$$k^2 - 1 \equiv 0 \pmod{p}$$

so. $p \mid k^2 - 1$ $p \mid (k-1)(k+1) \Rightarrow p \mid k-1$ or $p \mid k+1 \Rightarrow k+1 \geq p$

but $0 < k-1, k+1 < p$. Contradict!

(2) (lemma 引理) if p is a prime, $\forall a, \exists b$ s.t. $ab \equiv 1 \pmod{p}$ ($a, p = 1$)

prove: $\because (a, p) = 1 \quad \exists m, n. \quad am + pn = 1.$

$$\Rightarrow am \equiv 1 \pmod{p} \quad \text{let } b = m.$$

let $A = \{ [2]_p, [3]_p, \dots, [p-2]_p \}$

$$\forall m \in A, \quad m \cdot 1 \equiv m \not\equiv 1 \pmod{p} \quad m \cdot (p-1) \equiv -m \not\equiv 1 \pmod{p}$$

so. $\exists n \in A$, s.t. $mn \equiv 1 \pmod{p}$.

suppose that $\exists m_1, m_2 \quad m_1 n \equiv m_2 n \equiv 1 \pmod{p}$

i.e. $(m_1 - m_2)n \equiv 0 \pmod{p} \Rightarrow p \mid m_1 - m_2$ or $p \mid n$ contradict!

so. $\forall m \in A, \exists$ unique n s.t. $mn \equiv 1 \pmod{p}$

also because p is an odd prime

$$[2]_p \cdot [3]_p \cdots [p-1]_p \equiv 1 \pmod{p}$$

even num (有偶数), 可以一一配对

and $1 \cdot (p-1) \equiv -1 \pmod{p}$

so $[1]_p \cdot [2]_p \cdots [p-1]_p \equiv [-1]_p$

(3) Call by (2), $(p-1)! \equiv -1 \pmod{p}$

4. because $p \notin \{2, 5\}$ $(p, 10) = 1$

Fermat: $10^{p-1} \equiv 1 \pmod{p} \Rightarrow (10^{p-1})^t \equiv 1 \pmod{p}$

so $p \mid 10^{t(p-1)} - 1$

let $t = 1, 2, 3, \dots$ and $10^{t(p-1)} - 1 \in \{9, 99, -999, \dots\}$

$\Rightarrow p$ divides infinitely many elements of the set. \square

5. $M = \{0, 1, \dots, N-1\}$ if $\gcd(m, N) = 1$ \checkmark

else $\gcd(m, N) = p \Rightarrow m_1 = \frac{m}{p}$ $N_1 = \frac{N}{p} \Rightarrow \gcd(m_1, N_1) = 1$

Euler: $m_1^{\phi(N_1)} \equiv 1 \pmod{N_1}$

$N = pq$. let $m = m_1 \cdot p$

so $(m, q) = 1$ $m^{\phi(q)} \equiv 1 \pmod{q}$

$\begin{cases} N = pq \\ \phi(N) = \phi(p)\phi(q) \end{cases}$

$m^{\phi(q)} = iq + 1$
and $n \mid qm$

so $c^d = m^{ed} = m^{c\phi(N)+1} \pmod{n}$
 $= m^{c\phi(p)\phi(q)+1} \pmod{n}$
 $= (iq+1)^{c\phi(q)} \cdot m \pmod{n}$

hence $iqm \equiv 0 \pmod{n}$, $(iq+1)^{c\phi(q)} \cdot m \equiv m \pmod{n}$