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:

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

let $x = k_1 n + a \quad y = k_2 n + b$

$xy = (k_1 n + a)(k_2 n + b) = k_1 k_2 n^2 + (ak_2 + bk_1)n + ab$

so $xy \in [ab]_n$

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

On the other side:

$\forall\ t \in [ab]_n \quad$ let $t = k_3 n + ab$

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

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

let $k_3 = 6. \quad$ so $t = 5 \times 6 + 1 = 31$

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

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

but 31 is a prime. $31 = 1 \times 31$.

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

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

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

D

2. $[1]_{23}=([1]_{23})^{-1}$ $[2]_{23}=([12]_{23})^{-1}$ $[3]_{23}=([8]_{23})^{-1}$

$[4]_{23}=([6]_{23})^{-1}$ $[5]_{23}=([14]_{23})^{-1}$ $[6]_{23}=([4]_{23})^{-1}$

$[7]_{23}=([10]_{23})^{-1}$ $[8]_{23}=([3]_{23})^{-1}$ $[9]_{23}=([18]_{23})^{-1}$

$[10]_{23}=([7]_{23})^{-1}$ $[11]_{23}=([21]_{23})^{-1}$ $[12]_{23}=([2]_{23})^{-1}$

$[13]_{23}=[16]_{23}$ $[14]_{23}=([5]_{23})^{-1}$ $[15]_{23}=([20]_{23})^{-1}$

$[16]_{23}=([13])^{-1}$ $[17]_{23}=([19]_{23})^{-1}$ $[18]_{23}=([9]_{23})^{-1}$

$[19]_{23}=([17]_{23})^{-1}$ $[20]_{23}=([15]_{23})^{-1}$ $[21]_{23}=([11]_{23})^{-1}$

$[22]_{23}=([22]_{23})^{-1}$

3. (1) $1\cdot 1\equiv 1 \pmod p$

$(p-1)\cdot(p-1)\equiv 1 \pmod p$

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

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

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

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

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

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

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

$\square$

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

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

so. $\exists\ n\in A,$ $\quad$ 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 $p\mid n$ $\quad$ 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 (有偶数个,可以一一配对)

and $\quad 1\cdot(p-1) \equiv -1 \pmod p$

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

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

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

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

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

let $t = 1,2,3,\cdots,$ $\quad$ and $10^{t(p-1)}-1 \in \{9, 99, \cdots 999\cdots9, \cdots\}$

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

5. $\quad M = \{0,1,\cdots,N-1\}$ $\quad$ if $\gcd(m,N)=1$ ✓.

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

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

$$\begin{cases} \varphi(N) = N \cdot \prod_{p\mid N}\left(1-\frac{1}{p}\right) \\ \varphi\left(\frac{N}{k}\right) = \frac{N}{k} \cdot \prod_{p\mid \frac{N}{k}}\left(1-\frac{1}{p}\right) \end{cases}$$

$\Rightarrow \varphi\left(\frac{N}{k}\right) \mid \varphi(N)$

$m_1^{\varphi(N_1)} = tN_1 + 1 = t\frac{N}{k} + 1$

$m^{\varphi(N_1)} = m_1^{\varphi(N_1)} \cdot k^{\varphi(N_1)} = t \cdot k^{\varphi(N_1)-1} N + k^{\varphi(N_1)}$

$m^{\varphi(N)} = \left(m^{\varphi(N_1)}\right)^{\frac{\varphi(N)}{\varphi(N_1)}} = \left(tk^{\varphi(N_1)-1} N + k^{\varphi(N_1)}\right)^{\frac{\varphi(N)}{\varphi(N_1)}}$

二项式展开. 右边只有一项不含$N$, 即 $k^{\varphi(N)}$ 也即 $m^{\varphi(N)} \equiv k^{\varphi(N)} \pmod N$.

继续上述操作. 若 $\gcd(k,N)=1$, 则 $k^{\varphi(N)} \equiv 1^{\varphi(N)} \equiv 1 \pmod N$

否则 若 $\gcd(k,N)=k_1$ 则 $k^{\varphi(N)} \equiv k_1^{\varphi(N)} \pmod N$

又 ∵ $N$ 有限, $\gcd$ 递减, 则上述操作有限次后, $\exists k_t$ $\gcd(k_t, N)=1$

则 $\quad m^{\varphi(N)} \equiv k^{\varphi(N)} \equiv k_1^{\varphi(N)} \equiv \cdots \equiv k_t^{\varphi(N)} \equiv 1^{\varphi(N)} \equiv 1 \pmod N$

回到本题,

$$m^e \equiv c \pmod N$$

$$ed \equiv 1 \pmod{\phi(N)} \qquad ed = c\phi(N)+1$$

$$\Rightarrow \quad c^d \equiv (m^e)^d = m^{ed} = m^{c\phi(N)+1} = m^{c\phi(N)} \cdot m$$

$$m^{c\phi(N)} \equiv (m^{\phi(N)})^c \equiv 1^c = 1 \pmod N$$

So. $c^d \equiv 1 \cdot m = m \pmod N$. $\square$