

§4.2 #32 case $r=2$ only.

$$x \equiv a_1 \pmod{m_1} \quad \text{and} \quad x \equiv a_2 \pmod{m_2} \quad \dots (*)$$

Since $(m_1, m_2) = 1$, $\exists b_1, b_2 \in \mathbb{Z} \Rightarrow m_1 b_1 + m_2 b_2 = 1$.

$$\begin{aligned} \therefore m_1 b_1 &= 1 - m_2 b_2 \equiv 1 \pmod{m_2} & \& \\ m_2 b_2 &= 1 - m_1 b_1 \equiv 1 \pmod{m_1} \end{aligned} \quad \dots \textcircled{1}$$

$$\begin{aligned} \text{Clearly, } m_1 b_1 &\equiv 0 \pmod{m_1} & \& \\ m_2 b_2 &\equiv 0 \pmod{m_2} \end{aligned} \quad \dots \textcircled{2}$$

Define $x_0 = m_1 b_1 a_2 + m_2 b_2 a_1$.

$$\text{Then } x_0 = m_1 b_1 a_2 + m_2 b_2 a_1 \stackrel{\text{by } \textcircled{2}}{\equiv} 0 \cdot a_2 + m_2 b_2 a_1 \stackrel{\text{by } \textcircled{1}}{\equiv} 1 \cdot a_1 = a_1 \pmod{m_1}$$

$$\& \quad x_0 = m_1 b_1 a_2 + m_2 b_2 a_1 \stackrel{\downarrow}{\equiv} m_1 b_1 a_2 + 0 \cdot a_1 \stackrel{\downarrow}{\equiv} 1 \cdot a_2 = a_2 \pmod{m_2}$$

$\therefore x_0$ is a common solution of $(*)$

If x_0 and x_1 are both common solutions of $(*)$, then

$$x_0 \equiv a_1 \equiv x_1 \pmod{m_1} \quad \& \quad x_0 \equiv a_2 \equiv x_1 \pmod{m_2}.$$

$$\Rightarrow m_1 \mid x_1 - x_0 \quad \& \quad m_2 \mid x_1 - x_0$$

$$\Rightarrow m_1 m_2 \mid x_1 - x_0$$

Since $(m_1, m_2) = 1$

$$\Rightarrow x_1 \equiv x_0 \pmod{m_1 m_2}$$

$$\begin{aligned} \S 5.2 \# 18. \quad & (a-1)(1+a+a^2+\dots+a^{o(a)-1}) \\ &= (a+a^2+a^3+\dots+a^{o(a)-1} + a^{o(a)}) - (1+a+a^2+\dots+a^{o(a)-1}) \\ &= a^{o(a)} - 1 - 1 - 1 - \dots - 1 \end{aligned}$$

Since $a \neq 1$, $1+a+a^2+\dots+a^{o(a)-1} \equiv 0 \pmod{p}$.

$\S 5.2 \# 24.$

(\Rightarrow) Suppose n is even. i.e. $n=2k$ for $k \in \mathbb{Z}$

$$\text{Since } 1^2 \equiv 1, 2^2 \equiv 1 \pmod{3}, \quad (x^2)^k + (y^2)^k = 1+1=2 \not\equiv 1 = (z^2)^k.$$

for nonzero x, y, z .

Contradiction! $\therefore n$ is odd.

(\Leftarrow) Assume n is odd i.e. $n=2k+1$ for $k \in \mathbb{Z}$.

$$\text{Then } 1^n + 1^n = 1^{2k} + 1^{2k} = 1+1=2 = 1 \cdot 2 \equiv 2^{2k} \cdot 2 = 2^{2k+1} = 2^n$$

$\therefore (x, y, z) = (1, 1, 2)$ nonzero solution in \mathbb{Z} .

$\S 5.4 \# 2$

$$\text{By thm 5.12, } \phi(n) = \prod_{i=1}^k (p_i^{m_i} - p_i^{m_i-1})$$

$$= \prod_{i=1}^k p_i^{m_i-1} (p_i - 1).$$

if $p_i = 2$ then $p_i - 1 = 1$ & $p_i^{m_i-1} = 2^{m_i-1}$ $\therefore \phi(n)$ is even.

if $\nexists i \ni p_i = 2$, then p_i 's are odd.

Since $p_i - 1$ is even, $\phi(n)$ is even.

$\therefore \phi(n)$ is even.

§5.4 #6.

i) $n = p^m$ where p is prime.

divisors of p^m are $1, p, p^2, \dots, p^m$

$$\begin{aligned} \therefore \sum_{d|p^m} \varphi(d) &= \sum_{r=0}^m \varphi(p^r) = 1 + \sum_{r=1}^m (p^r - p^{r-1}) = 1 + (p^1 - p^0) + (p^2 - p^1) + \dots + (p^m - p^{m-1}) \\ &= p^m = n. \end{aligned}$$

ii) general case.

$n = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}$ where p_1, \dots, p_k are distinct prime numbers & m_1, \dots, m_k are positive integers.

Every divisor d of n is of the form $d = p_1^{r_1} \dots p_k^{r_k}$ where $0 \leq r_i \leq m_i$

for $i = 1, \dots, k$.

By thm 5.12, $\varphi(d) = \varphi(p_1^{r_1}) \varphi(p_2^{r_2}) \dots \varphi(p_k^{r_k})$

$$\begin{aligned} \therefore \sum_{d|n} \varphi(d) &= \sum_{r_1=0}^{m_1} \dots \sum_{r_k=0}^{m_k} \varphi(p_1^{r_1} \dots p_k^{r_k}) \\ &= \sum_{r_1=0}^{m_1} \dots \sum_{r_k=0}^{m_k} \varphi(p_1^{r_1}) \varphi(p_2^{r_2}) \dots \varphi(p_k^{r_k}) \\ &= \prod_{i=1}^k \sum_{r_i=0}^{m_i} \varphi(p_i^{r_i}) \\ &= \prod_{i=1}^k p_i^{m_i} = n. \end{aligned}$$