2. $n \in \mathbb{N}$

$a, b \in \mathbb{Z}$

$a \equiv b \pmod{n}$

$f(x) = C_d x^d + C_{d-1} x^{d-1} + \cdots + C_1 x + C_0$

$\rightarrow f(a) \equiv f(b) \pmod{n}$

이것을 $d \geq 1$ 에 대해 귀납법으로 증명.

i) $d = 1$

$f(x) = C_1 x^1 + C_0$

$a \equiv b \pmod{n} \longrightarrow n \mid a-b \longrightarrow a-b \neq 0$, $a-b = n \cdot g$

$f(a) = C_1 a + C_0$

$f(b) = C_1 b + C_0$ $\rightarrow f(a) - f(b) = C_1 (a-b)$

$n \mid a-b$ 이고 $a-b \mid C_1 (a-b)$ 이므로

$n \mid C_1 (a-b)$ ($\because$ Thm 12)

$\rightarrow n \mid f(a) - f(b)$

$\rightarrow f(a) \equiv f(b) \pmod{n}$ ∎

ii) Assume that assertion holds for every $d = 1, 2, 3, \cdots, k$ (≥ 1)

(ii) Now, consider the case where $d=k+1$

$d=k$,

$$\left.\begin{aligned} f(a) &= C_k a^k + C_{k-1}a^{k-1} + \cdots + C_1 a + C_0 \\ f(b) &= C_k b^k + C_{k-1} b^{k-1} + \cdots + C_1 b + C_0 \end{aligned}\right]$$

$$f(a)-f(b) = C_k(a^k-b^k) + C_{k-1}(a^{k-1}-b^{k-1}) + \cdots + C_1(a-b)$$

$$\frac{a^k-b^k}{a-b} = a^{k-1}+a^{k-2}\cdot b + a^{k-3}\cdot b^2 + \cdots + ab^{k-2} + b^{k-1} \quad \text{이므로}$$

$$f(a)-f(b) = (a-b)\left\{ C_k\left(a^{k-1}+a^{k-2}\cdot b + \cdots + ab^{k-2}+b^{k-1}\right) + C_{k-1}\left(a^{k-2}+a^{k-3}\cdot b + \cdots + a\cdot b^{k-3}+b^{k-2}\right) \right.$$
$$\left. + C_{k-2}\left(a^{k-3}+a^{k-4}\cdot b + \cdots + ab^{k-4}+b^{k-3}\right) + \cdots + C_2(a'+b') + C_1 \right\}$$

$$= (a-b)\cdot Q \quad \text{s.t. } Q\in\mathbb{Z} \qquad \cdots\cdots\cdots\cdots (1)$$

$n \mid (a-b)$ 이고 $(a-b) \mid (a-b)Q$

$\rightarrow n \mid (a-b)\cdot Q$ ($\because$ Thm 12)

$\rightarrow n \mid f(a)-f(b) \rightarrow f(a) \equiv f(b) \pmod n$

$d=k+1$ 일 때,

$$f(x) = C_{k+1}x^{k+1} + C_k x^k + C_{k-1}x^{k-1} + \cdots + C_1 x + C_0$$

$a \equiv b \pmod n \longrightarrow n \mid (a-b)$

$$f(a) = C_{k+1}a^{k+1} + C_k a^k + C_{k-1}a^{k-1} + \cdots + C_1 a + C_0$$

$$f(b) = C_{k+1}b^{k+1} + C_k b^k + C_{k-1}b^{k-1} + \cdots + C_1 b + C_0$$

$$f(a)-f(b) = C_{k+1}a^{k+1} - C_{k+1}b^{k+1} + (a-b)Q \quad (\because (1))$$

$$= (a-b)\cdot C_{k+1}\left(a^k + a^{k-1}b + \cdots + ab^{k-1} + b^k\right) + (a-b)\cdot Q$$

$$= (a-b)\left\{ C_{k+1}\left(a^k + a^{k-1}b + \cdots + ab^{k-1} + b^k\right) + Q \right\}$$

$$= (a-b)\cdot P \quad \text{s.t. } P\in\mathbb{Z}$$

$n \mid (a-b)$ 이고 $(a-b) \mid (a-b)P$

$\rightarrow n \mid (a-b)\cdot P$ ($\because$ Thm 12)

$\rightarrow n \mid f(a)-f(b)$

$\rightarrow f(a) \equiv f(b) \pmod n$, Thus the assertion is True for $d=k+1$

IV) Therefore we conclude that the assertion is true for every $d \geq 1$ ∎