21PC22

Basic Results in congruences :-

Theorem 1: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a \pm c \equiv b \pm d \pmod{n}$

Proof :

We prove that $a - c \equiv b - d \pmod{n}$

$a - b = n\alpha$, $c - d = n\beta$ for some $\alpha, \beta \in Z$

$$(a-c)-(b-d) = (a-b)-(c-d)$$
$$= n\alpha - n\beta = n(\alpha - \beta)$$
$$\Rightarrow a - c \equiv b - d \pmod{n}$$

similarly we can prove $a + c \equiv b + d \pmod{n}$

Theorem 2: If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$

$a - b = n\alpha$, $c - d = n\beta$ for some $\alpha, \beta \in Z$

$$ac - bd = (ac - bc) - (bd - bc)$$
$$= n\alpha c - b(-n\beta)$$
$$= n(\alpha c + b\beta)$$

$\therefore ac \equiv bd \pmod{n}$

Applying the previous two results we get,

If $a \equiv b \pmod{n}$ and $f(x)$ is a polynomial with integer coefficients then

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