Remainder theorem: If $f(x) \in F[x]$ and $a \in F$, for any field F, then $f(a)$ is the remainder when $f(x)$ is divided by $(x-a)$

Proof By division algorithm $\exists$ polynomial $q(x)$ & $r(x)$ such that $f(x) = (x-a)\cdot q(x) + r(x)$ where either $r(x) = 0$ or $r(x)$ is a polynomial whose degree is less than that of $x-a$. Since degree of $(x-a)$ is one so degree of $r(x)$ must be of zero or no degree. Hence $r(x)$ is constant polynomial ie $r(x) = r \in F$

Thus $f(x) = q(x)(x-a) + r$.

Putting $x = a$ we get

$$f(a) = q(a).(a-a) + r$$

$$\Rightarrow f(a) = r. \quad \text{Proved}$$

Factor theorem If $f(x) \in F[x]$ and $a \in F$, for a field F then $x-a$ divides $f(x)$ if & only if $f(a) = 0$

Proof By remainder theorem, $f(a)$ is remainder when $f(x)$ is divided by $(x-a)$ Therefor if $f(a) = 0$ then $(x-a)$ divides $f(x)$.

Conversely if $x-a$ divides $f(x)$, then we get

$$f(x) = (x-a).q(x)$$

Putting $x = a$ we get

$$f(a) = (a-a).q(x) = 0$$

Proved

Thm In a unique factorisation domain (UFD) every pair of non-zero elements has a HCF and LCM.

Proof Let R be UFD. and $a, b \in R$ s.t. $a \neq 0$ $b \neq 0$

Case I When either a or b is unit

Without loss of generality let us assume that a is unit.

$\Rightarrow a^{-1} \in R$.

Now $b = aa^{-1}b$

$\Rightarrow a|b$ also $a|a$

So a is common factor of a & b

Let $d \in R$ be such that $d|a$ & $d|b$

So in particular $d|a$.

$\Rightarrow a$ is HCF of a & b (By def^n of HCF)

Also $a|b$ also $b|b$

$\Rightarrow b$ is common multiple of a & b

Let $c \in R$ be such that $a|c$ & $b|c$.

So in particular $b|c$.

$\Rightarrow$ b is LCM of a & b (By def^n of LCM)

Case II If neither a nor b are unit.

Let us write $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$

$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$ (By def^n of UFD)

as product of powers of set of distinct primes.

((Note: Here we allow zero powers as well.
i.e Like $2 = 2^1 \times 3^0$
& $3 = 3^0 \times 3^1$))

Let $\gamma_i = \max(\alpha_i, \beta_i)$ & $\xi_i = \min(\alpha_i, \beta_i)$ $i = 1, 2, 3, \ldots n$

Let $c = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ & $d = p_1^{\xi_1} \cdot p_2^{\xi_2} \cdots p_n^{\xi_n}$

Clearly $c, d \in R$ and c is LCM and d is HCF of a & b

Thm: If R is principal ideal domain (PID), then every pair of non-zero elements a & b of R has HCF and LCM. Further if $d(a,b)$, then $d = ax + by$ for some $x, y \in R$. Proved

Proof Since R is principal ideal ring
$\Rightarrow$ Every ideal of R is principal ideal
Let a, b be two non-zero elements of R.
Clearly (a) & (b) are two principal ideals of R generated by a & b respectively
Since sum of two ideals & intersection of two ideals are again ideal.
$\Rightarrow (a)+(b)$ and $(a) \cap (b)$ are ideals of R
Since R is PID
$\Rightarrow \exists$ d and $\ell \in R$ such that
$(a)+(b) = (d)$ and $(a) \cap (b) = (\ell)$.
Now we will prove that d is HCF & ℓ is LCM of a & b.

At first we will prove that d is HCF of a & b

Since $(a) \subseteq (a)+(b)$ & $(b) \subseteq (a)+(b)$

$\Rightarrow (a) \subseteq (d)$ & $(b) \subseteq (d)$

$\Rightarrow d|a$ and $d|b$

Also let $q \neq 0$ be an element of R such that

$q|a$ and $q|b$

$\Rightarrow (a) \subseteq (q)$ & $(b) \subseteq (q)$

$\Rightarrow (a)+(b) \subseteq (q)$

$\Rightarrow (d) \subseteq (q)$

$\Rightarrow q|d$

Hence by defn of HCF, d is HCF of a & b.

Again since $(d) = (a)+(b)$

$\Rightarrow d \in (a)+(b)$

$\Rightarrow \exists\ x, y \in R$ such that

$d = ax+by$. (Proved)

Now we will prove that l is LCM. of a & b.

Since $(a) \cap (b) \subseteq (a)$ & $(a) \cap (b) \subseteq (b)$

$\Rightarrow (l) \subseteq (a)$ & $(l) \subseteq (b)$

$\Rightarrow a|l$ and $b|l$.

Also let $m \neq 0$ be an element of R such that

$a|m$ and $b|m$

$\Rightarrow (m) \subseteq (a)$ & $(m) \subseteq (b)$

$\Rightarrow (m) \subseteq (a) \cap (b)$

$\Rightarrow (m) \subseteq (l)$.

$\Rightarrow l|m$

By defn of LCM l is LCM of a & b (Proved)