Thm The necessary & sufficient condition that a non-zero element a in a Euclidean ring R is unit is that $d(a) = 1$.

Proof Let a is unit in Euclidean ring R

We have $d(1a) \geq d(1)$

$\Rightarrow d(a) \geq d(1)$ —— ①

Since a is unit in $R \Rightarrow a^{-1} \in R$ such that

$aa^{-1} = 1$.

$\Rightarrow d(1) = d(aa^{-1}) \geq d(a)$

i.e $d(1) \geq d(a)$ —— ②

From ① & ② $d(a) = d(1)$.

Conversely: Let $d(a) = d(1)$

We want to show that a is unit in R.

If a is not a unit in R (

then $d(1a) > d(1)$

$\Rightarrow d(a) > 1$ (Contradiction)

Hence a must be a unit in R

Thm: Let R be a Euclidean ring. Then every non-zero element in R is either a unit in R or can be written as a product of finite number of primes element of R.

Proof We will prove this theorem by induction on $d(a)$

We have $a = 1a$.

$\therefore d(a) \geq d(1)$

Thus 1 is an element in R which has minimal d-value. Also if $d(a) = d(1)$ then a is unit in R.

Thus result of this theorem is true for $d(a) = d(1)$.

Let us assume inductively that the statement of theorem is true for all non-zero element x in R such that $d(x) < d(a)$

We shall now show that theorem is true for a also.

If a is prime then theorem is true for a also

If a is not prime then we can write $a = bc$ where neither b nor c is unit in R.

$\therefore d(bc) > d(b)$ & $d(bc) > d(c)$

$\Rightarrow d(b) < d(a)$ & $d(c) < d(a)$ $(\because a = bc)$

$\therefore$ By induction hypothesis b & c can be written as a product of a finite numbers of prime elements in R.

Let $b = p_1 p_2 \cdots p_m$ and $c = q_1 q_2 \cdots q_n$

$\Rightarrow a = bc = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n$

Thus we have a as a product of a finite numbers of primes elements of R.

Hence by induction, theorem is proved.

Unique factorisation theorem

Let R be a Euclidean ring and a be a non-zero non-unit element in R. Suppose that

$$a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

where p_i's and q_j's are prime elements of R. Then $m = n$ and each p is an associate of some q and each q is an associate of some p.

Proof We have $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ ——— (1)

$\Rightarrow p_1$ is divisor of $q_1 q_2 \cdots q_n$

$\Rightarrow p_1$ is divisor of at least one of $q_1, q_2, \cdots q_n$

Since R is commutative ring, wiltous loss of generality we may suppose that $p_1 \mid q_1$

Since p_1 & q_2 bolt are prime elements

$\Rightarrow p_1$ & q_1 must be associates.

ie $\exists$ a unit $u_1 \in R$ such that $p_1 = u_1 q_1$

So from (1) we have

$$p_1 p_2 \cdots p_m = u_1 p_1 q_2 q_3 \cdots q_n$$

$$\Rightarrow p_2 p_3 \cdots p_m = u_1 q_2 q_3 \cdots q_n \quad \text{——— (2)}$$

We repeat the same argument in (1) with p_2 and so on If $n > m$ then after m steps left hand side becomes 1 while right hand side reduces to product of some units in R and certain number of q_j's. But q_j's are prime elements of R, so product of some units and certain number of q_j's can not be equal to 1.

So n can not be greater than m

$$\Rightarrow n \leq m. \quad \text{——— (1)}$$

Also we have ~~some~~ shown that each p_i is an associate of some q_j.

Interchanging the role of p_i & q_j we can show that $m \leq n$ and also each q_j is associate of some q_i ——— (2)

From (1) & (2) $m = n$

Hence theorem is established.

Note: Combination of previous two theorem. We can say that in a Euclidean ring every non-zero element can be uniquely written (upto associates) as a product of prime elements in R or unit in R.

Therefore a Euclidean ring is UFD.