

Let's say that there are two numbers,  $a$  and  $b$ . Let's say  $\text{GCD}(a,b)=x$ .

Surely one number must be greater than the other. Let's say that  $a$  is greater than  $b$ .

If we divide  $a$  by  $b$  then, we get  $q$  as quotient and  $r$  as remainder.

Now,

$$a=bq+r$$

$\text{GCD}(a,b)=x$  must divide both  $a$  and  $b$ .

$a$  must be divisible by  $x$ , leaving remainder as 0.

By the equation,  $(bq+r)$  must be divisible by  $x$ , since  $a=bq+r$ .

By definition,  $x$  should divide  $b$ . So,  $x$  also divides  $bq$ , since  $q$  is just another integer.

Now, for  $(bq+r)$  to be divisible by  $x$ , it's intuitive and clear that  $r$  should be divisible by  $x$ .

Now the theorem follows,  $\text{GCD}(a,b)=\text{GCD}(b,r)=\text{GCD}(a,r)$

Usually,  $\text{GCD}(b,r)$  is taken, since  $b$  is smaller than  $a$ , thereby making life easy.

Now again,  $\text{GCD}(b,r)$  is treated as like the mirror  $\text{GCD}(a,b)$  and this process continues until the remainder  $r$  becomes zero.

The last non-zero remainder  $r$  is the value of the GCD of the original numbers,  $\text{GCD}(a,b)$ .