INTRODUCTION TO NUMBER THEORY

EUCLID'S ALGORITHM :-

{ on input a, b where a, b are z such that $a \geq b \geq 0$ }

The algorithm follows three steps :

Step 1 : If $b=0$, then return the value of a.

step 2 : Otherwise, divide a by b and store the remainder in some variable r.
[which is nothing but modulo operation]

Step 3 : Let $b=r$ and $a=b$ and return to step.

Step 4 : Continue this process until $b=0$.

FOR EXAMPLE :-

Let us consider the inputs as

$a = 25$ $\quad$ $b = 10$

$r = a \% b$ $\quad := r = 5$

$b = 5$ $\quad a = 10$

$r = a \% b$ $\quad := r = 0$

$b = 0$ $\quad a = 5$

$\therefore gcd(25, 10) = a = 5$

```
int gcd (int a, int b)
{   int r;
    if (b == 0)
        return a;
    else
        r = a % b;
        gcd (b, r);
}
```

} a=b and b=r

Time complexity

The euclidean algorithm computes gcd(a,b), where $a \geq b \geq 0$.

* The no. of divisions with remainder is $O(\text{len}(b))$
* The rough estimate of the total time is $O(\text{len}(b)^2 \text{len}(a))$
* Moreover it can be proved that the Euclidean algorithm only needs $O(\text{len}(b)\text{len}(a))$ time.