APPLICATION : ALGORITHMS

The Division Algorithm :

Based on quotient remainder theorem,

$$a = dq + r \quad \text{and} \quad 0 \leq r < d$$

Algorithm :

```
r := 0 , q := 0
while (r ≥ d)
    r := r - d
    q := q + 1
end while
  return (q, r)
```

($GCD(a,b) * LCM(a,b) = a * b$)

Euclidean Algorithm :

Premises

- If $r \in \mathbb{Z}^+$, $GCD(0, r) = r$
- If $a, b \in \mathbb{Z}$ and $a, b \neq 0$

$$a = bq + r$$

$$\gcd(a, b) = \gcd(b, r)$$

(Lemma on which Euclid algorithm is based)

GCD(A, B) :

$A, B \geq 0$

```
a := A , b := B , r := B
  while (b ≠ 0)
     r := a mod b
     a := b
     b := r
  end while
   return a
```