

# NUMBER THEORY

Ariyadi Wijaya

# Prime Number

Definition:

A prime is positive integer greater than 1 that is divisible by no positive integers other than 1 and itself

Definition:

Positive integer greater than 1 that is not prime is called composite

# Prime Number

Lemma:

Every positive integer greater than 1 has a prime divisor.

Theorem:

If  $n$  is a composite number then it has a factor  $k$  so that  $1 < k \leq \sqrt{n}$

Theorem:

If  $n$  is a composite number, then  $n$  has a prime factor no greater than  $\sqrt{n}$

Theorem:

If  $p$  is a prime number and  $p|ab$  then  $p|a$  or  $p|b$

# The Fundamental Theorem of Arithmetic

Theorem (Fundamental Theorem of Arithmetic):

Every positive integer greater than 1 can be uniquely written as a product of prime.

Example:

$$26=2.13$$

$$100=2.2.5.5$$

Lemma:

If  $a$ ,  $b$  and  $c$  are positive integers such that  $(a,b)=1$  and  $a \mid bc$ , then  $a \mid c$

Proof:

$$(a,b)=1 \rightarrow ax+by=1$$

$$acx+bcy=c$$

Since  $a \mid acx$  and  $a \mid bcy$ ,  $a \mid c$

- $p|ab \rightarrow p|a \text{ or } p|b$