

CHAPTER 4: SOME NUMBER THEORY

MORE ON THE NATURAL NUMBERS

Theorem. *Every non-empty set of natural numbers has a least, or smallest, element.*

Definition. *If a and b are natural numbers we say that a divides b , and write $a|b$, if there is a natural number q such that $b = aq$. We say that a is a divisor of b .*

Definition. *We say that a natural number p is a prime number if the only divisors of p are 1 and p . We do not consider the number 1 to be a prime number. It is a unit. Numbers which are not units or prime numbers are called composite.*

These definition also can be extended to the integers. In this case the numbers 1 and -1 are the units in the set of integers. The units in a Ring (the integers are an example of a Ring) are those elements which have multiplicative inverses.

Theorem. *If a natural number q is composite then there are integers $1 < m < q$ and $1 < n < q$ such that $q = mn$.*

Theorem. *Every natural number $n > 1$ is either a prime number or can be expressed as a product of prime numbers.*

Theorem: The division algorithm. *If m and n are integers and $m > 0$ then there are unique integers q and $0 \leq r < n$ such that*

$$m = nq + r.$$

Given two integers m and n define

$$I(m, n) = \{ma + nb : a, b \in \mathbf{Z}\}.$$

Put

$$S(m, n) = I(m, n) \cap \mathbf{N}.$$

Theorem. *With the definitions above let r be the least element of $S(m, n)$. Then if $d|m$ and $d|n$ then $d|r$. Further $r|m$ and $r|n$. r is the greatest common divisor or m and n .*

Corollary. *If r is the greatest common divisor or m and n then there exist integers a and b such that*

$$r = ma + nb.$$