Chapter 1

1.1 Divisibiliy

By Natural numbers we mean the numbers 1, 2,3,......

Integers are Natural numbers, 0 and the negative numbers ...-3,-2,-1. The set of integers will be denoted by Z such that

Z = {....,-3,-2,-1, 0, 1, 2, 3,....}.

Definition ***1.1.1***

If a and b are Integers with $a \neq 0$, we say that a divides b if there is an integer c such that b=ac.

If a divides b, then a is a divisor or factor of b.

If a divides b we write $a \mid b$, if a doesn't divide b then $a \nmid b$.

Example (1):

The following illustrate the concept of divisibility of integers :

$13 \mid 182$, $-5 \mid 30$, $6 \nmid 44$, $7 \nmid 50$ and $17 \mid 0$.

Example (2):

The divisors of 6 are ±1, ±2, ±3, ±6.

The divisors of 17 are ±1, ±17..

The divisors of 100 are ±1, ±2, ±4, ±5, ±10, ±20, ±25, ±50 and ±100.

Note that:

Every non-zero integer is a divisor of 0 and 1 is a divisor of every integer or equivalently every integer is a multiple of 1.

1.3 The Euclidean Algorithm

The gcd of two integers can be found by listing all +ve divisors and picking out the largest one common to each , but this is not suitable for large numbers.

A more efficient process involving repeated application of the division algorithm goes by the name of

Euclidean Algorithm . The E.A. may be described as follows :

Let a , b be two integers whose gcd is desired , we can find unique integers q_1 , r_1 such that

$$a = bq_1 + r_1 \qquad 0 \le r_1 < b$$

if $r_1 \ne 0$ we divide b by r_1 so

$$b = r_1 q_2 + r_2 \qquad 0 \le r_2 < r_1.$$

if $r_2 \ne 0$ we divide r_1 by r_2 so

$$r_1 = r_2 q_3 + r_3 \qquad 0 \le r_3 < r_2.$$

Similarly if $r_3 \ne 0$

$$r_2 = r_3 q_4 + r_4 \qquad 0 \le r_4 < r_3$$

.

.

.

$$r_{k-2} = r_{k-1} q_k + r_k \qquad 0 < r_k < r_{k-1}$$

$$r_{k-1} = r_k q_{k+1} + 0 \qquad r_{k+1} = 0.$$

By the repeated application of Theorem 1.2.5 , we can show that r_k , the last non-zero reminder which appears in this manner is equal to (a , b),

3(-6) + 6.6 = 18
3(10) + 6(-2) = 18.
where as the equation 2x + 10y = 17 which has no solution .
so its reasonable to ask about the conditions under which a
solution is possible . The answer is given by the following theorem .

Theorem ***1.5.2:***

Let a , b be integers with d = (a , b) . The equation ax + by = c has no integral solution if $d \nmid c$.
If d | c then there are infinitely many integral solutions . Moreover , if $x = x_0$, $y = y_0$ is a particular solution of the equation , then all solutions are given by
$x = x_0 + (b/d)n$, $y = y_0 - (a/d)n$, where n is an integer .

Proof :

Assume that x and y are integers such that ax+ by = c . Then since d | a and d | b so d | c .
Hence if $d \nmid c$, there are no integral solutions of the equation.
Assume that d\c. Since (a,b)=d ∃ s,t Z, such that
d = as + bt ....(*)
Since d | c there is e ∈ Z such that de = c.
Multiply both sides of (*) by e we get
c = de = (as + bt) e = a(se) + b(te).

Let $k = 4n + 1$, $k' = 4m + 1$

Then $kk' = (4n + 1)(4m + 1)$

$= 16mn + 4n + 4m + 1$

$= 4(4mn + n + m) + 1$

$= 4L + 1$, where $L = 4mn + n + m$.

Which is of the desired form.

Theorem ***2.2.5:***

There is an infinite number of primes of the form 4n + 3.

Proof :

In anticipation of a contradiction , let us assume that there exist only finitely many primes of the form 4n+3 , call them $q_1, q_2, \ldots\ldots, q_s$. Consider the positive integer

$N = 4 q_1 q_2 \ldots\ldots q_s - 1 = 4(q_1 q_2 \ldots\ldots q_s - 1) + 3$,

and let $N = r_1.r_2\ldots.\ r_t$ be its prime factorization .

Because N is an odd integer, we have $r_k \neq 2$ for all k , so that each r_k is either of the form 4n+1 or 4n+3.By the lemma above the product of any number of primes of the form $4n + 1$ is again an integer in this type for N take the form 4n+3 as its clearly dose, N must contain at least one prime factor r_i of the form 4n+3. But r_i cannot be found among the listing $q_1, q_2, \ldots.., q_s$, for this would lead to a contradiction that $r_i \mid 1$.

The only possible conculosion is that there are infinitly many primes of the form 4n+3 .

Theorem ***2.2.6:*** ***<u>(Dirichlet)</u>***

If a and b are relatively prime positive integers i.e (a, b) = 1 , then the arithmetic progression

a, a + b, a + 2b, a + 3 b

contains infinitely many primes.

<u>**Example(6)**</u>:

(3, 4) = 1 , therefore the arithmetic progression is

3, 3 + 4 , 3+ 2(4) ,3+ 3(4) , 3 + 4(4), 3 + 5(4),...........

i.e, the arithmetic progression is 3, 7, 11, 15, 19, 23, ...

contains infinitely many primes all of them are of the form 4n + 3.

Similarly (1, 4) = 1 therefore the arithmetic progression is :

1, 1 + (4) , 1+ 2(4), 1 + 3(4), 1 + 4(4), 1 + 5(4) ,......... ,i.e. 1, 5, 9, 13, 17, 21,......

contains infinite number of primes of the form 4n + 1 .

Theorem ***2.2.7:***

No Arithmetic progression of the form a, a + b , a + 2b,......, contains only primes.

Proof :

Let a + nb = p where p is a prime.

If we put $n_k = n + kp$, $k = 1, 2, 3, \ldots$, then the n_k^{th} term in the progression is

$a + n_k b = a + (n + kp) b$

$$\varphi(720) = \varphi(2^4.3^2.5) = 720(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 192$$

$$\varphi(450) = \varphi(2.3^2.5^2) = 450(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 120$$

Example (22)

If f is an arithmatic function ,then

$$\sum_{d/12} f(d) = f(1)+f(2)+f(3)+f(4)+f(6)+f(12)$$

for example

$$\sum_{d/12} d^2 = 1^2+2^2+3^2+4^2+6^2+12^2$$

$$= 1+4+9+16+36+144 = 210.$$

The following result which states that n is the sum of values of the phi-function at all the

positive divisors of n will be useful.

Theorem ***4.3.13***

Let n be positive integer,then $\sum_{d/n} \varphi(d) = n.$

Let $n = p^\alpha$, then the divisor of p^α are $,1, p, p^2, \ldots, p^\alpha$. Therefore

$$\sum_{d/n} \varphi(d) = \varphi(1)+\varphi(p)+\varphi(p^2)+\ldots+\varphi(p^\alpha)$$

$$= 1+p-1+p^2-p+\ldots\ldots+p^\alpha-p^{\alpha-1}$$

$$= p^\alpha = n.$$

Hence the result is true for $n = p^\alpha$.