Unit-4

Number Theory

Division

When one integer is divided by a second non-zero integer, the quotient may or may not be an integer. As for example, 12/3=4 is an integer where as 11/4=2.75 is not integer. This leads to definition 1.

Definition 1

If a & b are integers with a≠0.We can say that a divides b if there is an integer c such that b=ac (or if b/a is an integer).When a divides b, we say that a is a factor or divisor of b & that b is a multiple of a. The notation a/b denotes that a divides b. We write a ∤ b does not divide when a does not divide b.

Example 1

Determine whether 3/7 & whether 3/12.

Solution: We say that $3 \nmid 7$, because $7/3$ is not an integer. On the other hand, $3/12$ because $12/3=4$.

The division Algorithm

Theorem 2 The division Algorithm

The division algorithm states that for any integer a and any positive integer d, there exists unique integers q and r with 0<=r<=d such that a = dq + r.

Definition 2

A/to division algorithm, d is called the divisor, q is called the quotient & r is called the remainder.

q=a div d, r=a mod d.

Example 3

What are the quotient & remainder when 101 is divided by 11?

Solution:

101=11.9+2

The quotient when 101 is divided by 11 is 9=101 div 11 & the remainder is 2=101 mod 11.

Example 4

What are the quotient & remainder when -11 is divided by 3?

Solution: We have

-11=3(-4)+1

The quotient when -11 is divided by 3 is -4=-11 div 3 & the remainder is 1=-11 mod 3.

-11=3(-3)-2.

Because r=-2 does not satisfy 0<=r<3.

Modular Arithmetic

Modular arithmetic is the branch of arithmetic mathematics related with the "mod" functionality. Basically, modular arithmetic is related with computation of "mod" of expressions. Expressions may have digits and computational symbols of addition, subtraction, multiplication, division or any other.

Modulo Arithmetic m

Definition 3

If a & b are integers & m is a positive integer, then a is congruent to b modulo m if m divides a-b.

a ≡ b (mod m) is indicate that a is congruent to b modulo m. We say that a ≡ b (mod m) is a congruence & that m is its modulus (plural moduli). If a &b are not congruent modulo m, we write a ≠ b (mod m).

Theorem 3

Let a & b be integers & let m be a positive integer. Then, a ≡ b (mod m) if & only if a mod m=b mod m.

Solution:

(do itself)

Example 5

Determine whether 17 is congruent to 5 modulo 6 & whether 24 & 14 are congruent modulo 6.

Solution: 6 divides 17-5=12.We see that 17≡5 (mod 6)

24-14=10 is not divisible by 6.

24≠ 14 (mod 6).

Theorem 5

Let m be a positive integer. If a ≡ b(mod m) & c ≡ d (mod m),then a+c=b+d (mod m)

& ac=bd (mod m).

Proof:

a ≡ b (mod m) c≡d (mod m),by theorem 4 there are integers s & t with b=a+sm & d=c+tm.

Hence, b+d=(a+sm)+(c+tm)

=(a+c)+m(s+t)

& bd=(a+sm)(c+tm)=ac+m(at+cs+stm)

Hence,

a+c=b+d(mod m) & ac ≡ bd(mod m)

Example 6

7 ≡ 2 (mod 5) & 11≡1 (mod 5), it follows that theorem 5 that 18=7+11≡2+1=3 (mod 5) & that 77=7.11≡2.1=2 (mod 5).

Primes & Greatest Common Division

Primes

Positive integers that have exactly two different positive integer factors are called primes.

Definition 1

An integer p greater than 1 is called prime if the only positive factors of p are 1 & p. A positive integer that is greater than 1 & is not prime is called composite.

Theorem 1

The fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes, where the prime factors are written in order of non-decreasing size. As for example,

Example 2

The prime factorizations of 100,641,999 & 1024 are given by

$100=2.2.5.5=2^2.5^2$

$641=641$

$999=3.3.3.37=3^3.37$

$1024=2.2.2.2.2.2.2.2.2.2=2^{10}$

Trial division

It is important to show that a given integer is prime. It follows that an integer is prime if it is not divisible by any prime less than or equal to its square root. This leads to the brute-force algorithm known as trial division.

Example 3

Show that 101 is prime.

Solution:

The only primes not exceeding $\sqrt{101}$ are 2, 3, 5 & 7.Because 101 is not divisible by 2, 3, 5 or 7.It follows that 101 is prime.

Example 4

Find the prime factorization of 7007.

Solution:

First perform divisions of 7007 by successive prime, beginning with 2.None of the primes 2, 3 & divides 7007.However, 7 divides 7007, with 7007/7=1001.Next, divide 1001 by successive primes, beginning with 7.7 also divides 1001 because 1001/7=143.Continue by dividing 143 by successive primes, beginning with 7.Although 7 does not divide 143 & 143/11=13. 13 is prime, the procedure is completed.

$7007=7.1001=7.7.143=7.7.11.13$

The prime factorization of 7007 is $7.7.11.13=7^2.11.13$ Ans.

Greatest Common Divisors (GCD) & Least Common Multiples (LCM)

GCD

The largest integer that divides both of two integers is called the greatest common divisor of these integers.

Definition 2

Let a & b be integers, not both zero. The largest integer d such that d/a & d/b is called the greatest common divisor of a & b. The greatest common divisor a & b is denoted by gcd (a,b).

Example 10

What is the greatest common divisor of 24 & 36?

Solution:

GCD of 24 & 36 are 1, 2,3,4,6 & 12.Hence, GCD (24, 36) =12.

Example 11

What is the greatest common divisor of 17 & 22?

Solution: The integers 17 & 22 have no positive common divisors other than 1, so that gcd (17, 22) = 1(Definition 3).

Definition 3

The integers a & b are relatively prime if their greatest common divisor is 1.

Example 12

By example 11, it follows that the integers 17 & 22 are relatively prime, because gcd (17, 22) =1(Definition 4)

Definition 4

The integers $a_1, a_2, \ldots\ldots, a_n$ are pair wise relatively prime if gcd $(a_i, a_j)=1$ whenever $1<=i<j<=n$.

Example 13

Determine whether the integers 10, 17 & 21 are pairwise relatively prime & whether the integers 10, 19 & 24 are pair wise relatively prime.

Solution: gcd(10, 17) = 1, gcd(10,21)=1.We conclude that 10,17 & 21 are pair wise relatively prime.

gcd(10,24)=2>1.We see that 10,19 & 24 are not pair wise relatively prime.

Example 14

Prime factorization of 120 & 500 are $120=2^3.3.5$ & $500=2^2.5^3$, the greatest common divisor is

$\gcd(120,500)=2^{\min(3,2)}{}_3{}^{\min(1,0)}{}_5{}^{\min(1,3)}$

$= 2^2.3^0.5^1=20$

Prime factorizations can be also used to find the least common multiple of two integers.

LCM

Definition 5

The least common multiple of the positive integers a & b is the smallest positive integer that is divisible by both a & b. It is denoted by LCM (a,b).

lcm(a,b)=$P_1^{max(a1,b1)}$ $P_2^{max(a2,b2)}$ $P_n^{max(a_n,b_n)}$.

Example 15

What is the least common multiple of $2^3\,3^5\,7^2$ & $2^4\,3^3$

Lcm ($2^3\,3^5\,7^2\,2^4\,3^3$)= $2^{max(3,4)}3^{max(5,3)}7^{max(2,0)}$

$=2^4\,3^5\,7^2$

Theorem 5

Let a & b be positive integers. Then, ab=gcd(a,b).lcm(a,b).

The Euclidean Algorithm

Efficient method of finding the greatest common divisor called the Euclidean Algorithm.

It is named after the ancient Greek Mathematician Euclid.

Find gcd (91,287)

287=91.3+14

Any divisor of 91 & 287 must also be a divisor of 287-91.3=14.Also, any divisor of 91 & 14 must be a divisor of 287=91.3+14.

Gcd of 91 & 287 is the same as gcd of 91 & 14.

Next, divide 91 by 14 to obtain 91=14.6+7.

Any common divisor of 91 & 14 also gcd(14,7)=7,gcd(287,91)=gcd(91,14)=gcd(14,7) =7.

Example 16

Find the GCD of 414 & 662 using the Euclidean Algorithm.

Solution:

662=414.1+248

414=248.1+66

248=166.1+82

166=82.2+2

82=2.41

Hence, GCD (414,662) =2, because 2 is the last non-zero remainder.

We can summarize in tabular form.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}
0	662	414	1	248
1	414	248	1	166
2	248	166	1	82
3	166	82	2	2
4	82	2	41	0

The Euclidean Algorithm

Procedure gcd (a,b: positive integers)

x:=a

y:=b

while y ≠ 0

r:=x mod y

x:=y

y:=r

return x{gcd(a,b) is x}

Example 17
Page 286
Example 18
Page 287

Gcd as linear combinations

Gcd of two integers a & b can be expressed in the forms
sa+tb where s & t are integers.
Gcd(a,b) can be expressed as a linear combination with integer coefficients of a & b. As for example,gcd(6,14)=2 & 2=(-2).6+1.14(Theorem 6)
Theorem 6 **BEZOUT'S THEOREM**
If a & b are positive integers, then there exist integers s & t such that gcd(a,b)=sa+tb.

Applications of Number Theory

Theorem 1
If a & m are relatively prime integers & m>1,then an inverse of a modulo m exists.This inverse is unique modulo m.
Proof:
By Theorem 6,gcd(a,m)=1,there are integers s & t such that
sa+tm=1
sa+tm≡1(mod m)
sa≡1(mod m)
s is an inverse of a modulo m.
Example 2
Find the inverse of 101 modulo 4620.
4620=45.101+75
101=1.75+26
75=2.26+23
26=1.23+3
23=7.3+2
3=1.2+1
2=2.1
Gcd(101,4620)=1