RESEARCHERID
THOMSON REUTERS

ISSN: 2277-9655
[Devi* *et al.*, 6(6): June, 2017] Impact Factor: 4.116
IC™ Value: 3.00 CODEN: IJESS7

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DISCRETE MATHEMATICS/NUMBER THEORY

Mrs. Manju Devi*
*Assistant professor in mathematics, S.D. (P.G.) College, panipat

DOI: 10.5281/zenodo.817972

ABSTRACT

Discrete mathematics is the study of mathematical structures that are fundamentally discrete rather than continuous. In contrast to real numbers that have the property of varying "smoothly", the objects studied in discrete mathematics such as integers, graphs, and statements do not vary smoothly in this way, but have distinct, separated values. Discrete mathematics therefore excludes topics in "continuous mathematics" such as calculus and analysis. Discrete objects can often be enumerated by integers. More formally, discrete mathematics has been characterized as the branch of mathematics dealing with countable sets(sets that have the same cardinality as subsets of the natural numbers, including rational numbers but not real numbers). However, there is no exact, universally agreed, definition of the term "discrete mathematics." Indeed, discrete mathematics is described less by what is included than by what is excluded: continuously varying quantities and related notions.

The set of objects studied in discrete mathematics can be finite or infinite. The term finite mathematics is sometimes applied to parts of the field of discrete mathematics that deals with finite sets, particularly those areas relevant to business.

Although the main objects of study in discrete mathematics are discrete objects, analytic methods from continuous mathematics are often employed as well.

I. INTRODUCTION

Unlike real analysis and calculus which deals with the dense set of real numbers, number theory examines mathematics in discrete sets, such as **N** or **Z**.

Number Theory, the study of the integers, is one of the oldest and richest branches of mathematics. Its basic concepts are those of divisibility, prime numbers, and integer solutions to equations -- all very simple to understand, but immediately giving rise to some of the best known theorems and biggest unsolved problems in mathematics. The Theory of Numbers is also a very interdisciplinary subject. Ideas from combinatorics (the study of counting), algebra, and complex analysis all find their way in, and eventually become essential for understanding parts of number theory.

II. DIVISIBILITY

Note that in **R**, **Q**, and **C**, we can *divide* freely, except by zero. This property is often known as *closure* -- the quotient of two rationals is again a rational, etc.. However, if we move to performing mathematics purely in a set such as **Z**, we come into difficulty. This is because, in the integers, the result of a division of two integers might not be another integer. For example, we can of course divide 6 by 2 to get 3, but we *cannot* divide 6 by 5, because the fraction 6/5 is not in the set of integers.

However we can introduce a new relation where division **is** defined. We call this relation *divisibility*, and if $\frac{b}{a}$ is an integer, we say:

- a is a factor of b
- b is a multiple of a
- b is divisible by a

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Formally, if there exists an integer q such that $b = qa$ then we say that a **divides** b and write $a \mid b$. If a does not divide b then we write $a \nmid b$:

III. QUOTIENT AND DIVISOR THEOREM

For any integer *n* and any *k* > 0, there is a unique *q* and *r* such that:
n = *qk* + *r* (with 0 ≤ *r* < *k*)

We call *q* the *quotient*, *r* the *remainder*, and *k* the *divisor*.

IV. MODULAR ARITHMETIC

Using the division theorem above

0 = 8*0 + 0
1 = 8*0 + 1
2 = 8*0 + 2
:
8 = 8*1 + 0
:
and so on

We have a notation for the remainders, and can write the above equations as

0 mod 8 = 0
1 mod 8 = 1
2 mod 8 = 2
3 mod 8 = 3
4 mod 8 = 4
5 mod 8 = 5
6 mod 8 = 6
7 mod 8 = 7
8 mod 8 = 0

WeThese notations are all short for
a = 8*k*+*r* for some integer *k*.

V. NUMBER BASES

The numbers that are generally used in transactions are all in base-10. This means that there are 10 digits that are used to describe a number. These ten digits are {0,1,2,3,4,5,6,7,8,9}.

Similarly, base-4 has 4 digits {0,1,2,3} and base-2 has two digits {0,1}. Base two is sometimes referred to as Binary.

There are also bases greater than 10. For these bases, it is customary to use letters to represent digits greater than 10. An example is Base-16 (Hexadecimal). The digits used in this base are {0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F}.

To convert from decimal to another base one must simply start dividing by the value of the other base, then dividing the result of the first division and overlooking the remainder, and so on until the base is larger than the result (so the result of the division would be a zero). Then the number in the desired base is the remainders read from end to start.

The following shows how to convert a number (105) which is in base-10 into base-2

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Operation	Remainder
105 / 2 = 52	1
52 / 2 = 26	0
26 / 2 = 13	0
13 / 2 = 6	1
6 / 2 = 3	0
3 / 2 = 1	1
1 / 2 = 0	1

Answer : 1101001

After finishing this process, the remainders are taken and placed in a row (from bottom to top) after the final quotient (1101001, in this example) is shown as the base-2 equivalent of the number 105.

This works when converting any number from base-10 to any base. If there are any letters in the base digits, then use the letters to replace any remainder greater than 9. For example, writing 11(of base-10) in base 14.

Operation	Remainder
11 / 14 = 0	B (=11)

Answer: B

As 11 is a single remainder, it is written as a single digit. Following the pattern {10=A, 11=B, 12=C...35=Z}, write it as B. If you were to write "11" as the answer, it would be wrong, as "11" Base-14 is equal to 15 in base-10!

In order to convert from a number in any base back to base ten, the following process should be used:
Take the number 3210 (in base-10). In the units place (10^0), there is a 0. In the tens place (10^1), there is a 1. In the hundreds place (10^2), there is a 2. In the thousands place (10^3), there is a 3.

The formula to find the value of the above number is:
$3\times10^3 + 2\times10^2 + 1\times10^1 + 0\times10^0 = 3000 + 200 + 10 + 0 =$ **3210**.

The process is similar when converting from any base to base-10. For example, take the number 3452 (in base-6). In the units place (6^0), there is a 2. In the sixths place (6^1) there is a 5. In the thirty-sixths place (6^2), there is a 4. In the 216th place (6^3), there is a 3.

The formula to find the value of the above number (in base-10) is:
$3\times6^3 + 4\times6^2 + 5\times6^1 + 2\times6^0 = 648 + 144 + 30 + 2 =$ **824**.

The value of 3452 (base-6) is **824** in base-10.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

VI. PRIME NUMBERS

Prime numbers are the building blocks of the integers. A prime number is a positive integer greater than one that has only two divisors: 1, and the number itself. For example, 17 is prime because the only positive integers that divide evenly into it are 1 and 17. The number 6 is not a prime since more than two divsors 1, 2, 3, 6 divide 6. Also, note that 1 is not a prime since 1 has only one divisor.

Testing for primality

There are a number of simple and sophisticated primality tests. We will consider some simple tests here. In upper-level courses we will consider some faster and more sophisticated methods to test whether a number is prime.

The most immediate and simple test to eliminate a number n as a prime is to inspect the units digit or the last digit of a number.If the number n ends in an even number 0, 2, 4, 6, 8 we can show that number n cannot be a prime. For example, take n = 87536 = 8753(10) + 6. Since 10 is divisible by 2 and 6 is divisible by 2 then 87536 must be divisible by 2. In general, any even number can be expressed in the form n = a*10 + b, where b = 0, 2, 4, 6, 8. Since 10 is divisible by 2 and b is divisible by 2 then n = a*10 + b is divisible by 2. In a similar type of argument, if a number n ends in a 5 we can show the number n cannot be a prime. If the last digit of n, call it b, is a 5 we can express n in the form n = a*10 + b, where b = 5. Hence, any number n which ends in a 5 such as 93475 is divisible by 5 so n is not a prime.. Consequently, if a number ends in a 1, 3, 7, or 9 we have to test further.

VII. TRIAL DIVISION METHOD

To test if a number n that ends in a 1, 3, 7, or 9 is prime, we could simply try the smallest prime number and try to divide it in n. If that doesn't divide, we would take the next largest prime number and try again etc. Certainly,if we took all primes numbers in this manner that were less than n and we could not divide n then we would be justified in saying n is prime. However, it can be shown that you don't have to take all primes smaller than n to test if n is prime. We can stop earlier by using the Trial Division Method.

The justification of the Trial Division Method is if a number n has no divisors less than or equal to $\sqrt{n}$ then n must be a prime.

Trial Division Method is a method of primality testing that involves taking a number n and then sequentially dividing it by primes up to $\sqrt{n}$.

For example, is 113 prime? $\sqrt{113}$ is approximately 10.63... We only need to test whether 2, 3, 5, 7 divide 113 cleanly (leave no remainder, i.e., the quotient is an integer).

113/2 is not an integer since the last digit is not even.
113/3 (=37.666...) is not an integer.
113/5 is not an integer since the last digit does not end in a 0 or 5.
113/7 (=16.142857...) is not an integer.

So we need not look at any more primes such as 11, 13, 17 etc. less than 113 to test, since 2, 3, 5, 7 does not divide 113 cleanly, 113 is prime.

VIII. THE FUNDAMENTAL THEOREM OF ARITHMETIC

The theorem basically states that every positive integer can be written as the product of prime numbers in a unique way.

In particular, **The Fundamental Theorem of Arithmetic** means any number such as 1,943,032,663 is either a prime or can be factored into a product of primes. If a number such as 1,943,032,663 can be factored into primes such as 11×13×17×19×23×31×59 it is futile to try to find another different combination of prime numbers that will also give you the same number.To make the theorem work even for the number 1, we think of 1 as being the product of zero prime numbers.

More formally,

For all $n \in \mathbf{N}$
$n = p_1 p_2 p_3 ...$
where the p_i are all prime numbers, and can be repeated.

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

LCM

The lowest common multiple, or the least common multiple, for two numbers a and b is the smallest number designated by LCM(a,b) that is divisible by both the number a and the number b. We can find LCM(a,b) by finding the prime factorization of a and b and choosing the maximum power for each prime factor.

In another words, if the number a factors to $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, and the number b factors to $p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, then LCM(a,b) = $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ where $\gamma_i = Maximum(\alpha_i, \beta_i)$ for *i = 1 to n.*

GCD

The greatest common divisor for two numbers a and b is the biggest number designated by GCD(a,b) that divides both the number a and the number b. In a similar process to finding LCM(a,b), we can find GCD(a,b) by finding the prime factorization of a and b but choosing the minimum power for each prime factor instead.

In other words, if the number a factors to $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, and the number b factors to $p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$, then GCD(a,b) = $p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_n^{\gamma_n}$ where $\gamma_i = Minimum(\alpha_i, \beta_i)$ for *i = 1 to n.*

IX. THE EUCLIDEAN ALGORITHM

The Euclidean algorithm is such that we can find the gcd of two numbers without finding the factorization*. The Euclidean algorithm consists of only addition and multiplication, and uses the above properties of gcd as its basis.

Factorization is a "hard" process, that is, to factor a number takes a long time depending on the length of the number. This is why later, when you need to find the gcd of a pair of numbers, you will most likely *never* factorize the numbers and use the properties of the primes but will use the Euclidean algorithm instead.

An example

We will see how this works by calculating gcd(44,458)
First, divide 458 by 44 and obtain the remainder:

458 = 44 × 10 + 18

Now suppose that a number is a common divisor of 458 and 44. Then it must also be a divisor of 18. To see this, rearrange the above equation to:

458 - 44×10 =18

When this equation is divided by a common divisor of 44 and 458, an integer is obtained on the left, and so must also be obtained on the right. This, by definition, means that the number is also a divisor of 18. By the same reasoning, any common divisor of 18 and 44 is also a divisor of 458. Since all of the common divisors of 458 and 44 are equal to common divisors of 44 and 18, then in particular the greatest common divisors are equal. So we have gcd(458,44)=gcd(44,18)

The next step in the algorithm is to divide 44 by 18 and find the remainder.

$44 = 18 \times k + r$

44 = 18 × 2 + 8

Repeat this process; keep dividing the previous divisor by the previous remainder:

18 = 8 × 2 + 2
8 = 2 × 4 + 0

Our gcd is the last remainder before the zero, in this case, 2. This is because the reasoning that proved gcd(458,44)=gcd(44,18) applies at every step, so gcd(458,44)=gcd(44,18)=gcd(18,8)=gcd(8,2)=gcd(2,0)=2.
The extended Euclidean algorithm

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Draw up a table with four columns, label these from left to right *q*, *r*, *u*, *v*. For convenience label a column *i* representing the step we're currently up to. Place *a* and *b* with the greater of these on top in the column *r*, and place 1s and 0s accordingly:

i	q	r	u	v
-1	.	b	0	1
0	.	a	1	0

Now iterate downwards by taking the quotient of *b*/*a* and putting it in the next space in the *q* column, then of *b*-*aq* in the *r* column.
To update *u* and *v*, take

$u_i = u_{i-2} - u_{i-1}q_i$
$v_i = v_{i-2} - v_{i-1}q_i$

Indeed, you are looking for *u* and *v* such that $au + bv = \gcd(a,b)$. At some point, gcd (a,b) is in fact the remainder at the ith stage, so you might as well compute u_i and v_i such that $au_i + bv_i = r_i$, at EACH stage.

Deriving the recurrences found above results from these three equations (the second equation is Euclid's algorithm's basic property, the other two are constraints we set to attain our desired goal):

$au_{i-1} + bv_{i-1} = r_{i-1}$
$r_{i-2} = q_i r_{i-1} + r_i$
$au_i + bv_i = r_i$

The trick is to then appropriately express r_{i-2}.
Stop writing when you obtain a 0 in the *r* column.

Finding then, gcd(450,44) (this is the same as gcd(44,450)

i	q	r	u	v
-1	.	450	0	1
0	.	44	1	0
1	10	10	-10	1
2	4	4	41	-4
3	2	**2**	-92	9
4	2	0	–	–

The bold number is the gcd. Observe (9)×450+(-92)×44=2 Clearly these *u* and *v* are very special.

Bezout's identity
In the above case we have 9×450+(-92)×44=gcd(450,44). So the greatest common divisor of 450 and 44 can be written as a linear combination of 450 and 44 with integer coefficients. This turns out to be true of any pair of integers. This result is known as "Bezout's Identity" and can be stated as follows:

For any pair of nonzero integers, *a* and *b*, there exists integers *u* and *v* such that
au+bv=gcd(a,b)

X. SOLVING LINEAR MODULAR EQUATIONS - BACK TO BEZOUT

Bezout's identity above provides us with the key to solving equations in the form
$ax \equiv b \pmod{m}$

Coprime case - gcd(*a*, *m*) is 1
Consider the case where
$ax \equiv b \pmod{m}$
but with $\gcd(a, m)=1$

ISSN: 2277-9655
Impact Factor: 4.116
CODEN: IJESS7

Because of Bezout's identity

$$1 = au+mv$$

When we calculate u, this number is special.

XI. REFERENCES

[1] www.en.wikipedia/wiki/discrete_ mathematics.
[2] www.wikibooks/wikin/number theory

CITE AN ARTICLE

Devi, M., Mrs. (2017). DISCRETE MATHEMATICS/NUMBER THEORY . *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *6*(6), 600-606. doi:10.5281/zenodo.817972