Number Theory, Combinatoric and Cryptography

Abe Milton

INTRODUCTION

This essay aims at performing an analysis of three areas which include the number theory, combinatoric and cryptography. The number theory is used both in combinatoric and cryptography, and all the three areas find use in each other.

NUMBER THEORY

The branch of mathematics called number theory studies the properties exhibited by the natural numbers and all integers. Other words used interchangeably with number theory include; arithmetic, higher arithmetic and theory of numbers. The number theory tries to discover and establishes the relationships that exist between different numbers as well as to prove the truthiness of these relationships. The discovery of number theory was discovered by Pierre de Fermat in the 17th century. Integers can either be even or odd; however, these numbers are closed under multiplication, subtraction, and addition.

Relationship 1:

For an integer n to be considered even, then n must be equal to 2k (n=2a). While for an integer n to be considered odd, then n must be equal to 2a +1 (2a+1).

Proof:

If a = 2, then n = 4 where n= 2*2= 4 (an even integer)

If a= 2, then n= 5 where n= (2*2) +1= 5 (an odd integer)

Relationship 2:

It happens that if m and n are considered even integers, then mn is said to be divisible by 4

Proof:

By m and n being even implies that there are integers a and b in such a way that m=2a and n=2b.

In this regard, mn will be equal to 4ab (mn=4ab). And because ab is said to be an integer, mn is divisible by 4 since it is 4 times an integer.

Relationship 3:

Another relationship is that the sum of two odd integers can never be odd, but the sum of two even integers is even;

Proof:

Odd integers

An example to this is; taking 1 and 5 both odd numbers gives the following; 1+5= 6 Even integers

Recall that for an integer n to be considered even, then n must be equal to 2k (n=2k).

While for an integer n to be considered odd, then n must be equal to 2k +1 (2k+1).

Hence; if n and m are odd integers, there exist some integers a and b such that n=2a+1 and m=2b+1.

Hence sum of these two integers will yields; m+n = 2b+a+2a+1= 2(a+b+1). This implies that the summation of m and n must be even.

Relationship 4:

If n is a positive integer, then n will be even if and only if 3n2+8 is even.

Proof:

The first thing in this relationship is to show that n is even when 3n2+8 is even, and 3n2+8 is even when n is even.

n is even if n=2a and hence, 3n2+8 = 3(2a) 2+8= 12a2+8 = 2(6a2+4). This answer is even because the content of the bracket (6a2+4) is an integer

COMBINATORICS

Combinatoric refers to a branch of mathematics that deals with the study of combination, enumeration, as well as the permutation of sets of elements and mathematical relations which characterise their properties. In various cases, mathematicians use the word combinatoric to refer to a large subset of discrete mathematics such as graph theory. The topic finds its application in areas of mathematical optimisation, pure mathematics, ergodic theory, computer science and statistical physics. Combinatoric is related to number theory through which the two words are combined to form combinatoric number theory. Combinatoric number theory deals with classical problems that face number theory and also deals with issues such as cardinality of the largest subset.

The combinatoric concepts are proofed mathematically by use of the term combinatoric proof. This proof is divided into two; double counting and bijective proof. The double counting proves the combinatorial identity through counting the number of elements of those carefully chosen set of two different ways hence able to obtain various expressions in the identity. The condition is that the expressions must be the same since they count the same objects. This way the identity is established. When using the bijective proof, there are two sets that are shown to possess the same number of members via exhibiting a bijection such as one – to – one correspondence. Below is an example of the double counting proof for the known formula on the number of (n k) of k – combinations for an n – element set.

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1}.$$

In this set of k- combinations identity, a direct bijective proof cannot be used since the right-hand side has a fraction. The numerator of the identity counts the Cartesian products of k finite sets of sizes n, n-1… n -k+1. On the other hand, the denominator counts the permutations of k-element set.

Another example is C (n, k) = C (n, n - k), where one needs to observe the in the instances that items of k are selected, n-k items are left over. One can also introduce m=n-k to obtain k=n-m which translates to an equivalent form C (n, n-m) = C (n, m).)

CRYPTOGRAPHY

The term Cryptography refers to the study of information protection through encryption hence cannot be predicted by every user. This concept brings privacy in communication in many modern applications and communication platforms. The information is coded in an unreadable format referred to as cipher text and only the individuals who possess a secret key can be able to decrypt the information into a plain text. Albeit, most of the modern techniques used in cryptography are virtually unbreakable, the encrypted text can be broken by use of cryptanalysis (code breaking).

Cryptography is very important in providing secure and safe mailing in a system and hence able to offer quick and efficient messaging only within allowable permissions provided. The system provides integrity, confidentiality, non-repudiation and authentication. Fundamental principles of cryptography include freshness and redundancy. The basics of cryptography are plain text, cipher, encryption, decryption, private key, public key and public key. Cryptography is classified into private and public cryptography. The public cryptography is the most modern and forms a strong basis for digital signatures, digital certificates and data encryption. Examples of the private cryptography are Advanced Encryption Standard (AES), TDES, Blowfish and RC4. One of the suitable and superb cryptography systems used on the internet for the protection of data is Pretty Good Privacy. The two classifications of cryptography systems are public keys and symmetric – key systems.

Cryptography also uses the number theory concept as utilising the Fermat's little theorem. This theorem is stated as if p is said to be a prime number then a(p-1) ≡ 1 (mod p) for 1 ≤ a ≤ (p-1). A good example is that if p = 7 and a = 2 then 26 = 64 ≡ 1 (mod 7).

The concept of cryptography has shaped life through the study of hiding information.

CONCLUSION

The three areas of concern in this essay are related in that they all use connatural concepts in offering theories as well as mathematical solutions

REFERENCES

1. *Sharbaf, Mehrdad S.* "Quantum Cryptography: an Emerging Technology in Network Security." (2011): 13-19. Print.

2. *Bell, Eric T. Men of Mathematics.* New York: Simon and Schuster, 1937. Print.

3. *Kato, K.; Kurokawa, N.; and Saito, T. Number Theory 1: Fermat's Dream.* Providence, RI: Amer. Math. Soc., 2000

4. *Rosen, K. H. (Ed.). Handbook of Discrete and Combinatorial Mathematics.* Boca Raton, FL: CRC Press, 2000