Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 4, March-2019, ISSN 2230-7540

A Study on the Applications of Number Theory in Mathematics

K. Gunasekar[1]* Dr. Ashwini Kumar Nagpal[2]

[1] Research Scholar (Part Time), OPJS University, Churu, Rajasthan

[2] Research Guide, Department of Mathematics, OPJS University, Churu, Rajasthan

Abstract – A few interesting applications have been made for Number Theory in Statistics. The reason for this overview paper is to feature certain significant uses of this sort. Prime numbers are an intriguing and testing field of mathematical hypothesis research. Diophantine conditions are the focal piece of number hypothesis. The condition that requires indispensable arrangements is known as the Diophantine condition. A few issues identified with prime numbers and the function of Diophantine conditions in Design Theory are talked about in the initial segment of this paper. The commitment of Fibonacci and Lucas numbers to the semi leftover plan of Metis is clarified. The Discrete Logarithm issue is a well-known issue identified with limited fields. The structure of Discrete Logarithm is examined in the second piece of this paper.

Keywords— Diophantine Equations, Design, Fibonacci and Lucas Numbers, Discreet Logarithm Problem

----------X----------

INTRODUCTION

The hypothesis of NUMBER is maybe the most seasoned part of arithmetic and, therefore, there are a few regions of examination in the field of number hypothesis. Methods from different parts of information may demonstrate valuable in tackling a portion of the issues in mathematical hypothesis and the other way around. The point of this paper is to pressure the significance of an interdisciplinary way to deal with research , specifically the linkages between number hypothesis and insights. Certain particular issues are examined to represent the utilizations of mathematical hypothesis in insights and to feature the level of association between the two subjects.

PRIME NUMBERS

For an itemized record of prime numbers, kindly allude to P. Ribenboim. The most confounding conduct of numbers is that of prime numbers. In spite of the best endeavors made by various analysts, understanding the different attributes of prime numbers keeps on introducing impossible challenges. This is because of varieties in the properties of prime numbers. The dissemination of expenses is an intriguing region of examination. Let Δ(X) indicate a prime number not surpassing x. We have the accompanying table of qualities:

x	1	2	3	4	5	6	7	8	9	10
$\pi(x)$	0	1	2	2	3	3	4	4	4	4

x	11	12	13	14	15	16	17	18	19	20
$\pi(x)$	5	5	6	6	6	6	7	7	8	8

Let P_n denote the n^{th} prime. With this notation, we have

$$\pi(p_n) = n \qquad (1)$$

Coming up next are notable outcomes on primes:

- Prime number hypothesis: The quantity of prime's not surpassing x is asymptotic to.
- Tchebychef's hypothesis: The significant degree of is π(X) = .

A fascinating inquiry is to discover how the prime pair's p, p+2 are dispersed

THE POLYNOMIAL OF EULER

A few endeavors have been made by specialists to discover polynomials that would just yield prime numbers. Leonhard Euler (1707-1783) considered the polynomial f(x)=x2+x+41 where x is accepted to take basic qualities as it were. Shockingly, this polynomial uses fundamental qualities just for a few successive necessary estimations of x,

beginning from 0, as appeared in the accompanying tables:

x	0	1	2	3	4	5	6	7	8	9	10
f(x)	41	43	47	53	61	71	83	97	113	131	151

x	11	12	13	14	15	16	17	18	19	20
f(x)	173	197	223	251	281	313	347	383	421	461

x	21	22	23	24	25	26	27	28	29	30
f(x)	503	547	593	641	691	743	797	853	911	971

x	31	32	33	34	35	36	37	38	39
f(x)	1033	1097	1163	1231	1301	1373	1447	1523	1601

In any case, when x = 40, we have f(x) =402 +40+41= 40(40+1)+41 =412 , partner a composite incentive for f(x). Euler's polynomial is a guide to show that there can't be a polynomial taking prime qualities in particular.

Like Euler's polynomial, the accompanying polynomials likewise accept prime qualities just for the back to back estimations of x gave inside brackets.

2x2+11 (x=0, 1,...,10), 2x2 +29 (x=0, 1,...,28), x2+x+17 (x=0, 1,...,15), 3x2+39x+37 (x=0, 1,...,174 +4x+59 (x=0, 1,...,13), x3+x2 +17 (x=0, 1,...,10) x4+29x2+101 (x=0, 1,...,19)

At the point when x is a characteristic number, it has been demonstrated that no polynomial f(x) with vital coefficients, not a steady, can be prime for all x, or for adequately enormous x (see for example G.H. Strong and E.M. Right). It is noticed that probabilistic appraisals of sequential prime (or composite) values accepted by Euler's polynomial for x > 39 or by different polynomials determined above for x surpassing the predetermined fundamental worth would be a fascinating issue.

A. Some Unsolved Problems Pertaining To Primes

- Are there boundlessly numerous primes given by the polynomial f(x)=x2+1?
- Is there consistently a prime between x2and (x2+1) ?

It is beneficial to attempt the above issues with probabilistic methodology.

A PROBLEM RELATED TO EULER'S ARITHMETIC FUNCTION

Let n be a given common number> 1. Euler's ∅-work partners with n the quantity of positive numbers not exactly and prime to n. By convention∅(n), is taken as 1. We have the accompanying table of qualities:

n	1	2	3	4	5	6	7	8	9	10
∅(n)	1	1	2	2	4	2	6	4	6	4

n	11	12	13	14	15	16	17	18	19	20
∅(n)	10	4	12	6	8	8	16	6	18	8

Consider the prime factorization of n. If .$n=p^{\alpha}q^{\beta}$.. where p, q ... are distinct primes, then

$$\emptyset(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\ldots. \qquad (2)$$

Uh, P.T. Bateman[1] considered the distribution of Euler 's validation-function values. It took am as the number of positive integers n with an acronym (n)=m and defined the function.

$$A(x) = \sum_{m\le x} a_m. \qquad (3)$$

i.e., A(s) is the number of positive integer's n with∅(n)≤x . He considered the function$\frac{A(x)}{x}$. The following values were obtained by him:

X	100	200	300	400	500
A(x)	198	395	588	790	971
$\frac{A(x)}{x}$	1.980	1.975	1.960	1.975	1.942

X	600	700	800	900	1000
A(x)	1174	1357	1569	1759	1941
$\frac{A(x)}{x}$	1.957	1.939	1.961	1.954	1.941

He conjectured that $\frac{A(x)}{x}$ has a finite limit of 1.9435964... as x→∞. In [1], he has presented several techniques to obtain the estimates for the error term in $\frac{A(x)}{x}$.

DIOPHANTINE EQUATIONS

The condition that requires indispensable arrangements is known as the Diophantine condition. Diophantus of Alexandria was keen on the indispensable arrangements of arithmetical conditions and subsequently the classification of Diophantine conditions. These conditions are the focal piece of the number hypothesis. L.J. is the standard reference for Diophantine conditions. It's Mordell.

Square-Free Natural Number A characteristic number n is supposed to be without square in the

event that it isn't detachable by a square with a number > 1. Thusly n is sans square if and just on the off chance that it is the result of unmistakable charges. An intriguing issue is to decide the likelihood that a given common number n is sans square. Gauss has seen that the likelihood that two whole numbers ought to be generally prime is . The likelihood that a number should be sans square is .

Pell's Equation Let D be a given without square common number. The condition

$$x^2 - Dy^2 = 1 \qquad (4)$$

It's known as Pell 's condition. For a given without square regular number d, this condition consistently has number arrangements in x and y, and the quantity of arrangements is unending. There are other general types of Pell 's condition

$$x^2 - Dy^2 = -1 \text{ and} \qquad (5)$$

$$x^2 - Dy^2 = N \qquad (6)$$

N is a non-zero number. These overall structures might not have indispensable answers for a given N or a without square D. It is fascinating to take note of that Pell 's condition for an exceptional estimation of D is identified with the plan as appeared in the grouping.

PLAN THEORY

Plan Theory is a significant part of insights. A plan can be considered as a point in R5. The boundaries related with a plan structure a quintuple (v, b, r, k, ambi as depicted underneath: let V mean a limited set comprising of v components. By block we mean a subset of V. We consider b blocks. It is expected that every component of V is in r blocks where r≤ b. We allude to r as the replication number of the plan. Let k mean the quantity of varietie blocks.

$$vr = bk \qquad (7)$$

$$\lambda(v-1) = r(k-1) \qquad (8)$$

The contribution of the number theory to the designs will be considered in the sequence. To this end, we consider a special type of design.

Metis Design By Metis design, we mean a block design with a parameter set (v, b, r, k, etc.) satisfying the additional relationship.

$$v = r + k + 1 \qquad (9)$$

Quasi-Residual Metis Design Quasi-Residual Metis design has additional properties

$$r = k + \lambda \qquad (10)$$

Consider equations (7) to (10). From (10) we've got the same = r-k. Using this in (8), we'll get rv-kv+k = kr. Substituting v from (9), we shall obtain a relationship

Since k can't take negative values, we're going to get it.

$$k^2 + kr = r^2 + r \qquad (11)$$

Treating (11) as a quadratic equation in k, we are led to the relation

$$k = \frac{-r \pm \sqrt{(5r^2 + 4r)}}{2}$$

Since k cannot take negative values, we get

$$k = \frac{\sqrt{(5r^2+4r)} - r}{2} \qquad (12)$$

In order for k to assume integral values, it is necessary to have the square of a natural number. Let g denote the largest common divider of $5r^2+4r$ and r. Then g /4. This implies that is a $\frac{5r^2+4r}{g^2}$ square. Hence each one of $\frac{5r+4}{g}$ and r/g shall be perfect squares. Considering modulo 4, it is seen that g cannot take the value of 2. Hence g = 1 or 4. In either case 5r+4 and r are both squares. Therefore there exist natural numbers x and y such that

$$5r + 4 = x^2 \text{ and} \qquad (13)$$

$$r = y^2 \qquad (14)$$

Thus we see that x and y are related by the following equation

$$x^2 - 5y^2 = 4 \qquad (15)$$

Equation (15) is the Pell's equationx^2-d^{y2}-=N – with D = 5 and N = 4.Thus a quasi-residual Metis design is related to the Pell's equation.

Relationship with Fibonacci and Lucas Numbers Fibonacci numbers {Fs} and Lucas numbers {Ls} are recursively defined as follows (see e.g. G.H.Hardy and E.M.Right[3]).

$$F_0 = 0, F_1 = 1 \text{ and } F_{s+2} = F_{s+1} + F_s, \qquad (16)$$

$$L = 0, L_1 = 1 \text{ and } L_{s+2} = L_{s+2} + L_s \qquad (17)$$

The first few Fibonacci and Lucas numbers are furnished in the following table:

s	0	1	2	3	4	5	6	7	8
F_s	0	1	1	2	3	5	8	13	21
L_s	2	1	3	4	7	11	18	29	47

s	9	10	11	12	13	14	15
F_s	34	55	89	144	233	377	610
L_s	76	123	199	322	521	843	1364

One can observe that the successive pairs of Fibonacci and Lucas numbers have the following properties:

$$2^2 - 5.0^2 = 4, 1^2 - 5.1^2 = -4,$$
$$3^2 - 5.1^2 = 4, 4^2 - 5.2^2 = -4 \; etc.$$

These specific results lead us to try out an induction approach in order to have a general outcome. By induction, we can see that

$$L_{2s}^2 - 5F_{2s}^2 \text{ and } L_{2s+1}^2 - 5F_{2s+1}^2 = -4$$

The corresponding even-subscribed terms in the Lucas and Fibonacci sequences thus satisfy the Pell equation (15) and therefore lead to a quasi-residual design of the Metis. In view of this result, the parameters of the quasi-residual design of the Metis are obtained in the Lucas and Fibonacci numbers as follows:

$$v = F_{2s}F_{2s+1} + 1, b = F_{2s}F_{2s+2}, r = F_{2s}^2,$$
$$k = F_{2s-1}F_{2s} \text{ and } \lambda = F_{2s-2}F_{2s}.$$

THE PROBLEM OF DISCRETE LOGARITHM

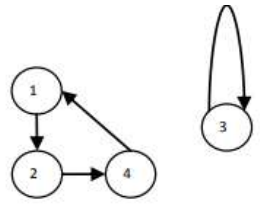
Leave p alone an odd prime. The discrete logarithm issue is to discover x = logb(y) in the limited field Zp, for example to discover the value(s) x in Zp, for example, bx = y (mod p). There is right now no calculation accessible for this issue. Applications are made to this issue in cryptography, which is the subject of mystery sending of messages, guaranteeing the security of the data (see for example A. M. Odlyzko[6]).

D. Cloutier and J. Holden have considered the issue of planning discrete logarithm[2]. The structure of the discrete logarithm has been concentrated by A. Hoffman[4]. The cautious logarithm can be seen as a capacity. The issue is to decide the reverse of x-apairbx (mod p). A utilitarian chart can be utilized to tackle this issue. The estimations of x can be spoken to by hubs of the diagram and the bolts can be drawn for every one of the mappings. A practical diagram is a coordinated chart with the goal that every vertex must have precisely one edge coordinated out of it. The m-ary work chart is a useful diagram where every hub has an in-level of precisely zero or m.

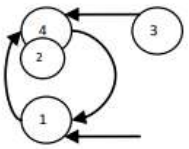
Let us think about a couple of explicit cases to delineate the system being referred to. For the utilitarian diagram of 2 (mod 5), consider the progressive essential forces of 2 and diminish them to modulo 5.

We have 21≡ (mod 5),22 ≡4 (mod 5), 23≡ 3 (mod 5),24 ≡1 (mod 5).Taking into account the type and the outcome subsequent to diminishing modulo 5, we get the forward correspondence

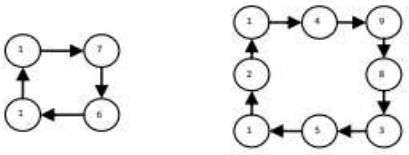
From this correspondence, we separate the cycles and get . Each cycle is spoken to by methods for a coordinated chart. The useful diagram for this case and a couple of different models are demonstrated as follows.



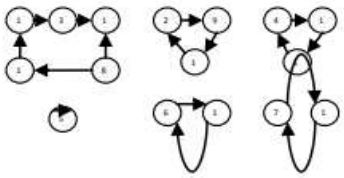
Functional graph for 2 (mod 5)



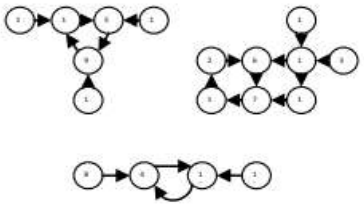
Functional graph for 4(mod 5)



Functional graph for 7 (mod 13)



Functional graph for 3 (mod 17)



Functional graph for 5 (mod 19)

In the capacity diagram for 4 (mod 5), hubs 2 and 3 are not part of any of the cycles. It is important to consider a useful chart in which every hub is

essential for a cycle. In this association, we need the accompanying:

Leave r alone the Zp component. Leave e alone the littlest normal number, for example, re= 1 (mod p). We state that r is a crude root modulo p e= p in the event that it is. Leave r alone any essential root modulo p and g = ra(mod p). D has been appeared. It's Cloutier and J. Holden [2] that the estimations of g which produce the m-ary diagram are accurately those for which gcd (5-007, p-1) = m is utilized. In the matter of discrete logarithm, A. Hoffman[4] accepting b as the essential root modulo p and considered three boundaries identified with the utilitarian chart, viz. The quantity of cycles, the most extreme length of the cycle and the weighted normal length of the cycle. It has been indicated that the structure of discrete logarithm can be broke down by factual examination of these three boundaries. It represented how examinations between irregular stages and those developed from an answer for a prudent logarithm issue can be made by thinking about the normal estimations of the three boundaries in the two cases. With the circulation of cycle lengths following the Poisson appropriation, it has been indicated how ANOVA tests can be performed for the mean number of cycle parts, the quantity of segments difference, the mean greatest cycle length, the most extreme cycle change, the mean normal cycle length and the normal cycle fluctuation. Choosing 30 primes in the reach 99991 – 106921 and utilizing the t-test and Anderson-Darling tests, he determined factual outcomes for the three boundaries of the useful charts identifying with the primes to show the structure in a cautious logarithm.

CONCLUSION

A portion of the connections between number hypothesis and measurements have been given in the above conversation. There is a lot of degree for investigating the uses of Number Theory in Statistics and the other way around. The circulation of prime numbers is a difficult territory for research. At the point when the boundaries in the plan become enormous, the plan investigation turns out to be very intricate , requiring more computational abilities. Understanding the properties of primes and taking care of a tactful logarithm issue utilizing useful designs requires very good quality processing power. With the computational abilities at present accessible because of innovative turns of events, future examination work is promising and unmistakable outcomes can be normal in this fascinating field of exploration.

REFERENCES

1. P.T. Bateman, “The distribution of values of Euler’s ø-function”, Acta Arith., Volume 21, Pp. 329 – 345, 1972
2. D. Cloutier and J. Holden, “Mapping the discrete logarithm”, Involve, Volume 3, Issue 2, Pp. 197 – 213, 2010
3. G.H. Hardy and E.M. Wright, “An introduction to the theory of numbers”, Oxford University Press, London, 1975.
4. A. Hoffman, “Statistical investigation of structure in the discrete logarithm”, Rose-Hulman Undergraduate Mathematics Journal, Volume10, Issue 2, Pp. 1 – 20, 2009
5. L.J. Mordell, “Diophantine equations”, Academic Press, London, 1969
6. A.M. Odlyzko, “Discrete logarithms in finite fields and their cryptographic significance” in “Advances in Cryptology: Proceedings of EUROCRYPT 84”, Lecture Notes in Computer Science, SpringerVerlag, Volume 209, Pp. 242 – 314, 1985
7. P. Ribenboim, “The new book of prime number records”, Springer Verlag, New York, 1996.
8. Yan Songyuan Number Theory and its Applications--Dedicated to Prof. Shiing-Shen Chern for his 90th Birthday [J]. Mathematics in Practice and Theory: 2002.03
9. Wang Shuhong the Early History of Algebraic Number Theory [J]. Journal of Northwest University (Natural Science Edition) 2010.6: P1120-
10. Xu Chong, Research and Implementation of Hierarchical Phrase-based translation Model in Statistical Machine Translation[D] Harbin Institute of Technology 2010

Corresponding Author

K. Gunasekar*

Research Scholar (Part Time), OPJS University, Churu, Rajasthan