

Mathematical Applications in Computer Science: A Review

Atul Jagannath Bhawsar and Vikas Sahebrao Ghorpade

Lecturer

Shri. H. H. J. B. Polytechnic, Chandwad, Maharashtra, India

Abstract: *Arithmetic has been an important intellectual preoccupation of man for a long term. Pc technology as a proper subject is ready seven many years younger. However, one thing in common among all customers and manufacturers of mathematical idea is the almost involuntary use of computing. In this text, we deliver to fore the many close connections and parallels among the two sciences of mathematics and computing. We display that, unlike inside the other branches of human inquiry where arithmetic is merely utilized or applied, computer technological know-how also returns additional price to mathematics via introducing positive new computational paradigms and methodologies and additionally through posing new foundational questions. We emphasize the strong interplay and interactions via searching at some thrilling present day results from quantity idea and combinatorial arithmetic and algorithms of pc technology.*

Keywords: Computer Science, Computational Paradigm, Combinatorial Mathematics.

I. INTRODUCTION

Mathematics has been an crucial intellectual pre occupation of guy for a long term. It is stated that the mathematics of the not unusual man or the mathematics of the thousands and thousands does no longer possess the esoteric abstractions and expressions of the arithmetic of the expert mathematician or the millennium arithmetic problems. But, one thing in not unusual between all customers and producers of mathematical idea is the almost involuntary use of computing. The nature, intensity and volume of the actual computing may additionally range quite extensively among those exclusive sorts of engagements with mathematics and computing. The simple processes of empirical verification, development of abstractions from concrete times inherent in mathematical questioning has a whole lot in commonplace with algorithmic or computational thinking. Mathematics is as old as humanity, while laptop technological know-how is a young field, approximately seven many years old. The sturdy interplay between arithmetic and computer science is at its peak nowadays. A lot has been written by way of philosophers on the nature of human inquiry. But, it is quite hard to outline a term such as mathematics in a complete and succinct manner. A fanciful, round definition states that mathematics is what is practiced by using mathematicians. It isn't always viable to strive even such an indicative definition of the discipline of Laptop science. Laptop science is perceived as an inter- disciplinary area with clean tracks of contributions from electrical and electronic engineering way of wondering and a clean track of contributions from the mathematical manner of wondering. In addition, these tracks ramify into many different sub-tracks and rejoin after a few complicated interactions. At a vast degree computer technology hence straddles simultaneously medical, engineering and technological standards. The term computing technological know-how seems to refer to the act of computing while the time period pc technological know-how appears to consult the ideas of architecting and engineering a pc. Indeed, it is true as visible from the preceding sentence; laptop technology every now and then refers to all of those and more. We will use fairly synonymously the terms, laptop science and computing technological know-how. The alternative terms computational science, science of computing, clinical computing, mathematics of computation, computational arithmetic all have slightly distinct specialized meanings and on occasion permit a few overlap. We are able to be aware that we sometimes increase our barriers. The motive of this article is not to delineate and distinguish clean demarcations. On the other hand the intent is to carry out the beautiful connections, similarities and parallels among the 2 disciplines of arithmetic and computer technology. In our paintings we take into account

handiest the aspect of theoretical underpinnings of computer technological know-how leaning on the technological know-how of algorithms. We do no longer consider the meta-physical, cognitive connections and subsequently do not make forays into subjects of formal logics, computational linguistics, synthetic intelligence, systemgaining knowledge of and different associated fields. Also we do now not discuss the exciting new possibilities of computing machines primarily based at the quantum mechanical or organic processes, that could render as beside the point some of the deep theoretical and practical troubles we take a look at here. The early formalisms in pc technological know-how have made clean the connections most of the 3 entities of machines, languages and computation. In addition they installed those connections via formalisms based on various sorts of automata, the corresponding formal language training and the generative mechanisms of grammars. Machines are synonymous with algorithms in a formal sense. From these theoretical underpinnings arose the formal specifications of algorithms and applications. The evolution of the theoretical foundations of computing science came about along these two clean tracks algorithms and applications.

The older form of the phrase algorithm is algorism. This time period refers to the manner of doing mathematics the use of arabic numerals. Mathematical historians hint the etymology of the word set of rules to the word algorism. The term comes from the call of a persian writer, abu musa al-khowarizmi (c. 825 ad)¹, who wrote a celebrated ebook, kitab al jabr w'al-muqabala (rules of recovery and discount). The word algebra stems from the name of this e book. The ancient city of khowarizm is the current city of khiva in russia. An set of rules is a compact, particular description of the stairs to solve a hassle. It's miles a finite, precise, effective method taking an input and producing an output. A application is a specific set of statements expressed the usage of the syntactic, semantic and linguistic constructs of a programming language that embodies the steps of an set of rules. The amazing evolution and applications of computers is due to the big range of traits in the technology of algorithms and applications. The 2 main troubles in the have a look at of algorithms and packages are correctness and computational complexity. Many theoretical and pragmatic ideas alongside these guidelines have brought about terrific advances. We talk the belief of proofs in arithmetic and the position of computer systems and computing in this context. We discuss the troubles of correctness and computational complexity in the context of design and evaluation of algorithms. Its miles right here that many captivating connections between mathematics and computing science seem in many sudden ways. These connections have caused very exciting developments in both fields of inquiry. We do not talk on this paper, the formal methods for reasoning about applications and their intrinsic relationship with sure abstract structures of mathematical good judgment and algebraic systems. We simply cite the notable works and treatises of the pioneers dijkstra² on the technology of programming, of worth on the notion of statistics structures which collectively with algorithms ends in the belief of applications and of manna⁴ on the logics used to reason about the correctness of applications.

II. ALGORITHMS AND COMPUTATIONAL COMPLEXITY

A lot has been stated and written on the topic of design and analysis of algorithms. There are a big quantity of top notch textual content books, superior monographs and high quality specialized journals and conferences on this area. They cowl a number of troubles associated with design techniques (including grasping, divide and conquer, branch and sure, binary doubling, and many others.), implementation (choice of information structures to store and procedure data), and analysis (version of computation, asymptotics, decrease bounds, structures in complexity, etc.). We cognizance best on the bigger macro stage capabilities and their relationships with arithmetic. A lovely precis of the common functions shared by way of algorithmic questioning and mathematical thinking is made with the aid of knuth⁵. The two styles of questioning are characterised with the aid of functions which include system manipulation, representation of fact, discount to simpler issues, summary reasoning. The amazing differences in functions are the manner of dealing with the uncountable continuum in mathematics and the manner of dealing with the belief of size of proof (computational complexity) in pc technological know-how. The set of rules of euclid (factors, e book 7) for calculating the greatest not unusual divisor (gcd) of integers is a first-rate example of the current perception of algorithm. It displays all of the houses and Features associated with establishing the correctness and computational complexity. One measures the computational complexity of an algorithm through expressing the quantity of primary steps taken with the aid of the set of rules to solve a trouble, in terms of the sizes of the input (and the sizes of a l of the

intermediate outcomes). In well known, the most wide variety of steps taken over all viable inputs over asymptotically huge-sized inputs is used as an upper certain and serves to represent the behaviour of the algorithm. This degree, expressed as a feature of the enter size is called the worst case asymptotic (time) complexity of the set of rules. The dimensions of an element is generally the quantity of binary bits needed to encode the element. Permit the sizes of the two input integers x, y be n bits. The euclidean gcd set of rules to obtain the $\gcd(x, y)$ calls for wide variety of steps (or equivalently time) proportional to $o(n^3)$. Therefore the computational complexity of the euclidean gcd set of rules is said to be cubic in input size. An set of rules whose complexity is polynomial within the input size is taken into consideration top. A problem that admits a polynomial time set of rules is said to be tractable or clean. Alternatively there are a large range of problems, that do not appear to be smooth (i. E. They do not seem to be solvable with the aid of a polynomial time algorithm). Consider the mathematical structure graph. Allow $g = (v, e)$ be a graph, in which v is a fixed of n vertices, and e is a collection of edges (a subset of the set of $n(n - 1)/2$ pairs of vertices). The size of the enter inside the case of a graph is proportional to the quantity of vertices and edges and is bounded by using $o(n^2)$. For example, the problem of determining whether a graph g has a hamiltonian cycle (a cyclic traversal of the edges of the graph travelling each vertex exactly as soon as), does not appear to be easy inside the above technical sense. Certainly, with the aid of list all feasible $n!$ Variations of the vertices and checking whether the graph can be traversed alongside the rims as in line with the vertex permutation, you can actually resolve the trouble. It is apparent that this set of rules, adopts a brute-force approach of exhaustive enumeration of all possible solutions. The computational complexity is exponential within the quantity of vertices because the characteristic $n!$ Grows about as $o(n n + 1/2 \exp - n)$.

III. PROOFS IN MATHEMATICS AND COMPUTER SCIENCE

In the previous section, we mentioned how we investigate the computational complexity of an set of rules. There may be the other element of checking the answer produced. How do we recognize that the solution produced by way of an algorithm or the realization of the set of rules is correct? Is there a easy mechanism, a components, an expression into which we will plug in the solution and check the answer? For a simple instance, keep in mind the problem of subtraction of integer b from integer a . We right away understand that we ought to upload the end result of subtraction to b and test for fit with a . Now, what is the complexity of sporting out this verification? In this case, addition and subtraction are both linear in the period of the operands a and b and hence the verification can be completed in polynomial time and hence we are saying that the verification is straightforward. Here we confirmed the correctness of an set of rules by using the use of another algorithm. Of Route we assumed that the opposite set of rules produced accurate solutions and that the result of that can be established effortlessly. The answers to issues that have polynomial time algorithms for generating the solutions seem to be verifiable in polynomial time (see the subtraction hassle) by running every other complementary algorithm. Another pair of simple, complementary algorithms are the multiplication and division algorithms with quadratic strolling time. This situation prevails in a non-apparent way in lots of conditions. The nonobvious nature comes from the position of the mathematical theorems that characterize the state of affairs. For example, in the case of the finest common divisor of integers, there may be a theorem because of bezout, that states that if $\gcd(x, y) = g$, then there exist two integers u, v such that $ux + vy = g$. The euclidean set of rules may be prolonged to decide the constants u, v except g , given x, y . At the same time as the bezout relation can be used to test if the gcd g is correct, assuming the portions u, v are accurate. The catch is that u, v also are received by using the equal algorithm. But, there may be any other way. From the fundamental theorem of arithmetic and the resultant specific factorization theorem the $\gcd(x, y)$ is on the spot from the high factorizations of x and y . Now we've got a exclusive seize. Factorization of an integer isn't always acknowledged to be polynomial time solvable. Much of our contemporary studies is centered round this trouble. In the subsequent segment, we speak the formal systems that address these sorts of conditions. The principle message right here is that unbiased characterizations allow the willpower and verification of an answer. It isn't at all clear whether or not or more impartial characterizations might be to be had for a problem. It isn't proper that the specific characterizations will result in the improvement of polynomial time algorithms to supply the solution. Such conditions are treated in problems of optimization, by using a selection of duality, reciprocity and min-max theorems. We discuss those in a next segment. Despite the fact that the initial formal

notions of set of rules and computational complexity figured most prominently inside the computer science literature at some point of the 1970s, the notion made its first appearance in a traditional paper through Edmonds⁶ on maximum matchings in graphs. Then again, many problems have the extraordinary function that the solutions can be established in polynomial time; but they do no longer seem to admit polynomial time algorithms to locate the solution (see the hamiltonian cycle problem). It's far clear that the yes answer to the question of hamiltonicity of a graph may be proven in linear time once a hamiltonian cycle is given. This case prevails within the case of many issues of various nature (decision, search, optimization, and so forth.), arising in unique domain names (sets, integers, graphs, and so on.) and from many different software areas (scheduling, data retrieval, operations studies, and so on.). Laptop scientists found out quite early, that there's a philosophic distinction between the computational complexity of an algorithm used to resolve a hassle and the computational complexity of verification of the answer. They also placed on a firm formal footing those notions of algorithmic production of an answer and that of verification. In addition they set up, inside the spirit of mathematical abstraction, equivalence training of problems categorized in step with their computational complexity. The equivalence magnificence of troubles whose answers might be validated in polynomial time become called np and the former elegance p . Truly p is contained in np . An crucial result was the postulate of an equivalence class of tough issues within np known as the np -whole class. An interesting state of affairs in the realm of computational complexity is that there does not appear to be effortlessly verifiable succinct certificate to the no solutions to choice variations of many problems. As an instance, it is not at all regarded the way to provide a short polynomial time verifiable proof to the answer that a given graph does not have a hamiltonian cycle. PC scientists have built many thrilling sub-systems within np . The fundamental meta-clinical query is whether p is same to np . This question has engaged computer scientists for the final three decades, in growing formalisms and loads of technical hair-splitting. We cannot pass into further details of this fascinating query from the principles of theoretical laptop science. We refer the reader to the classic book on this situation with the aid of Garey and Johnson⁷. We just make a few feedback on the modern-day perspectives on this subject which borders on meta arithmetic. I might borrow the quaint little word meta-magical themes used by Douglas Hofstadter as the identify for his column within the magazine scientific american, to describe those questions. Interestingly, this word was coined through Hofstadter, a laptop scientist, as an anagram of the identify mathematical video games utilized by Martin Gardner for decades as the identify of his column in scientific american. The Clay Mathematics Institute of Massachusetts, United States of America, named seven prize issues, each wearing a cash award of one million dollars, in can also 2000. Those encompass the distinguished Riemann speculation, and some different notable conjectures of twentieth century arithmetic. These problems are toasted to be at the identical magnificence of issues stated by means of d. Hilbert within the yr 1900. The eminent french mathematician, j. P. Serre, commenting on those issues, said that the choice by means of the clay institute became very apt. He hoped that the $p = np$ query might not become undecidable. This question possibly, is a meta query and is on the same footing as sure axiomatic questions within the foundations of set theory upon which the whole edifice of current mathematics rests. Hence the belief of speedy verifiable succinct proof or a brief certificates to the correctness of the answer determined with the aid of an set of rules, is a cornerstone contribution of PC technology to mathematical idea. Inside the following sections we observe the notion proofs in arithmetic and a few near connections with computational notion.

IV. MANY PROOFS AND MANY ALGORITHMS

In mathematics the perception of proof is a crucial ingredient of all outcomes. No mathematical statement is made without a aware try to establish or prove the assertion. Mathematicians are taught and trained within the course in their development from a student to a professional practitioner, the science of proving statements. Mathematical statements include a hard and fast of axioms, hypotheses, antecedents and consequents. The statements are set up by means of a chain of logical outcomes from the hypotheses and antecedents to the consequents by a chain of logical deductions. Of path, arithmetic is not to be construed as an insignificant set of dry, mechanical deductions. If that have been so, such a human endeavour might no longer have survived. There is a sure innate beauty in many mathematical statements and theorems and very often inside the many twists and turns of the proofs. One wonders at times if this innate fine Of

mathematics is similar to the surrealistic styles of human inquiry in area including the quality arts, literature, music, painting and sculpture. Certainly, the well-known mathematician littlewood as soon as described eloquently positive results of srinivasa ramanujan as evoking the experience of marvel produced through looking at a positive ecclesiastical architectural masterpiece. Many mathematicians and philosophers have contemplated over this innate satisfactory of mathematical notion. This innate great transcends the bodily international. Scientists in lots of disciplines have encounter a comparable phenomenon in explaining their technological know- how. Mathematical statements and proofs have an lifestyles of their very own, as pure figments of imagination. However, there may be glaring in a lot of these sorts of expressions of notion lovely perception into the shape of the arena of mathematical objects. In widespread, these gadgets are used to model the bodily world and the statements are about the way these objects interact to provide greater complex structures with real global effects. Nowa days, mathematicians and pc scientists have contributed many considerable thoughts that have all the features mentioned above. Within the last few a long time computer science has emerged as a mature foundational technological know-how, with its very own corpus of axioms, statements and body of effects. It's miles right here that the technology of algorithms, or now and again called algorithmics (specifically by means of the french research network), stands proud like a beacon proclaiming its reputation on par with arithmetic. The fraternity of mathematicians and computer scientists have come to recognize and well known with mutual respect sure top notch effects from their respective disciplines. Of direction, mathematics being a miles older technology has many extra theorems and consequences of superb beauty and importance than the algorithms of pc technological know-how. More and more, computer science is enriching mathematics in many approaches. This phenomenon is most seen inside the place of discrete mathematics. We study this phenomenon more carefully inside the next segment. We discussed above the conceptual parallels among the nature of proofs in arithmetic and the nature of algorithms in computer technology. We take this similarly to identify positive different similarities in our paper. We identify common characteristics. (i) many alternative proofs (ii) brief, succinct or stylish proofs. Each characteristics are found in abundance in the sciences of discrete mathematics and algorithms. In fact, these are precisely the reasons that make these subjects so charming. It's far tempting to quote and annotate the several examples to demonstrate those two features from the 2 disciplines. I shall restriction to just more than one illustrations to make the factor.

V. MANY PROOFS

The regulation of quadratic reciprocity of gauss is lauded as the gem of arithmetic through the mathematical historian, e. T. Bell. This law expresses the quadratic residuosity of a top integer p modulo another prime q , in terms of the quadratic residuosity of q modulo p within the form of a rather simple expression in phrases of the parities of p and q . As a mathematical statement that is indeed a gem. It's far stunning, easy and so herbal to think up. What's more, this law occupied the centre degree of variety theoretic research during a massive part of the 19th century. It is not sudden that gauss himself found eight proofs, and a 152nd proof of the law changed into published⁸ in 1976. The quest for a generalization of this regulation, which means higher order reciprocity.

Connecting solutions of better strength congruences modulo prime integers, occupied the mythical mathematicians gauss, kummer, jacobi, dirichlet. Ultimately, eisenstein received a proof of the law in 1865. What fascinates me except these exciting many proofs via many mathematicians is the various connections to many different problems which have caused unexpected new developments. Indeed, gauss, eisenstein, kummer, dirichlet and others have been all looking for proofs of higher electricity reciprocity legal guidelines (see edwards⁹ and lemmermeyer⁸) even as attempting to prove fermat's last theorem. Inside the route of this quest, kummer had a huge success in proving the fermat's final theorem for the elegance of abnormal top exponents and paved the way for the development of present day magnificence area idea. Mathematicians devise imaginative distinct proofs by using applying their instinct together with techniques and standards from diverse branches of arithmetic in surprising approaches. As an instance, the one-of-a-kind proofs of the regulation quadratic reciprocity referred to above draw upon principles from elementary enumerative combinatorial arguments to sophisticated use of algebraic systems and complicated analytic gear. To a specialist mathematician, the loads of proofs noted above could all fall into some categories. Despite the fact that, these

few classes encompass notably one-of-a-kind concepts. That speaks for what's referred to as scientific serendipity with out which a good deal of the science of mathematics might lose its allure. The famous top quantity theorem states that the variety of primes much less than an integer x is about $x/\log(x)$. This easy declaration about the lore of integers has involved number theorists for a long time. The evidence of this theorem by hadamard and de los angeles vallee poussin is a conventional instance inside the global of arithmetic of a much less famous mathematician's call being associated with a remarkable result. Surprisingly, this and many other similar, associated results inside the fascinating branch of arithmetic referred to as range theory^{10,11}, invoke simultaneously techniques for dealing with the discrete and the non-stop. At a deeper stage, this isn't always too surprising. As kronecker, positioned it god made natural numbers, rest is the work of man. A herbal mathematical approach is to start modelling and analysing a finite, discrete world after which entering the continuum via adopting an asymptotic limiting process. I shall now not go into in addition reasons of this metaphor. I end with the comment approximately the opportunity evidence of the top wide variety theorem by means of erdos and selberg. This evidence used combinatorial arguments absolutely, and did no longer use any complicated evaluation techniques. The authors known as their proof an elementary proof. This proof is an example of what we term, elementary however not clean. It's miles primary in the experience that it does now not use superior techniques to be had only to the professionally educated mathematician. It isn't smooth within the experience that the arguments are worried and complicated. However, this proof is longer than the analytic proof. We use the adjective longer here, to indicate the diploma of difficulty in wading through the verification of several minute info. Mathematicians, like artists, every now and then talk to the pleasant of a proof with the aid of the term elegance. We are able to recall this belief of mathematical beauty within the subsequent sections .

VI. MANY ALGORITHMS

Mathematicians are coming round to the viewpoint that algorithms as studied in laptop science will be taken into consideration very close to the item they take a look at, called theorems. The premise for this reputation has been discussed above. We further add right here that within the ultimate a long time, many prestigious fora and awards that recognize extensive modern-day mathematical results have welcomed the fresh breath of thrilling mathematical outcomes from laptop technological know-how. Computer scientists have devised many thrilling algorithms for the identical trouble. In doing this, they've often combined super insights from the structures inside the problem area, the systems inherent in the enter facts and certain insightful generic algorithmic techniques. I give a few sophisticated examples later. Here we mention a few basic troubles for which computer scientists have come up with particularly unique methods of fixing them. These are: (i) sorting a hard and fast of elements¹², (ii) multiplication of polynomials, integers and matrices¹⁰, (iii) locating shortest paths in graphs¹³, (iv) speedy exponentiation in groups¹⁰. Some of the fantastic, and some distance accomplishing thoughts from the arena of algorithmics, which have enriched the mathematical global come from subjects which includes polynomial time interior point based algorithms for the linear optimization hassle, equivalence of combinatorial optimization troubles in phrases of computational complexity; the applicability of lattice foundation reduction for designing algorithms for optimization issues; the notions of approximation, randomized algorithms; algorithmic combinatorial geometry; polynomial time primality trying out set of rules for integers; modular exponentiation-based public key cryptographic algorithms, syndrome decoding set of rules in error correcting codes. What i set out to demonstrate in this segment is the situation of many algorithms for fixing a trouble, like the state of affairs of many proofs for the identical theorem in arithmetic. These distinctive algorithms for the identical hassle offer a massive repertoire of illustrative pedagogic, studies standards and techniques that liven up the technology of algorithms. They offer the chronic challenges to the scientists to give you higher, stylish, efficient and practical algorithms.

VII. ELEGANT PROOFS AND ELEGANT ALGORITHMS

The mythical 20th century mathematician paul erdos favored to talk approximately the e-book wherein god continues the most elegant or perfect proofs. The hungarian mathematician turned into referred to as the maximum prolific mathematician of all time, comparable to the other prolific mathematician, euler of an in advance generation.

Erdos maintained that even though one did no longer agree with inside the lifestyles of god, one must accept as true with in the life of the e-book. Aigner and ziegler¹⁴, made a diffusion of 30 items in a group posted in 1998. It's miles an unenviable project to bring together such

A set. A certain quantity of mathematical chauvinism is inevitable and so there are possibilities of omission in the choice. But, it's far irrefutable that what figures in such a diffusion is indeed elegant.

I cite a few from this collection.

- For any positive integer n there is a prime between n and $2n$.
- A natural number n is a sum of two squares if and only if every prime factor p of the form $4m + 3$ appears to an even power in n .
- p, p^2, \exp for rational r , are all irrational.
- If G is a connected, planar graph, then $n - e + f = 2$. Here n, e, f are the number of vertices, edges and faces in G .
- No more than 12 spheres can simultaneously touch a sphere of the same size.
- There are $n - 2$ different labeled trees on n vertices. A partial Latin square of order n with at most $n - 1$ filled cells can be completed to a Latin square of the same order.
- Every planar map can be five coloured.
- For any museum with n walls $n/3$ guards suffice.
- A triangle-free graph on n vertices has at most $n^2/4$ edges (generalizations exist for p -clique-free graphs for all p).

The main rationale in giving the listing above is to show the simplicity of the statements. Different exciting elements are that none of the proofs run for a range of pages; and are available to anybody with an excellent excessive faculty degree of mathematical education. That is the character of succinctness or beauty of mathematical thought. It might be extremely fascinating to think up the ebook of algorithms. Computer science is possibly, nearly ready to provide applicants. I ought to make the subsequent random selection, without plenty trepidation. The Euclidean algorithm for greatest common divisor.

- The quick-sort algorithm.
- Algorithm to test the planarity of a graph. Finding the maximum matching in a graph.
- The randomized algorithm for the roots of a polynomial over a finite field.
- The Fast Fourier transform algorithm.
- The deterministic polynomial time primality testing algorithm.
- Determination of the convex hull of a set of points in 3 dimensions.
- Run length compression of binary strings. Set union, search algorithm.

VIII. CONCLUSION

In the above sections we discussed the important capabilities of theorems of mathematics and algorithms of laptop technology to carry out the close parallels, connections and also some variations. The motive turned into to display the character of wondering: mathematical and algorithmic. Fundamentally we see how those two disciplines have enriched every other.

Many applications draw closely upon existing body of mathematical outcomes and now and again call for new mathematics. Current computing technological know-how offers a new shape of engendering new mathematical outcomes. It affords new ways of searching at classical effects. I just point out a few thrilling modern traits in both mathematics and pc technology which have many connections based on deep mathematical and algorithmic wondering – ramanujan's modular functions and expander graphs, computation of trillions of digits of constants like π ; ramanujan's asymptotic techniques in combinatory analysis²² and their implications in analysis of algorithms; the principle of elliptic curves (one of the three components in the proof of fermat's final theorem with the aid of a. Wiles) and its function in current public key cryptography^{15,23}; new algebraic and variety theoretic questions springing up out of cryptography and coding theory²⁴ inclusive of the usage of quantity fields in integer factoring, divisors of

algebraic curves in cryptosystems and codes¹⁵; lower bounds on computational complexity in algebraic models of computation; pseudo-randomness in algorithms and mathematics; many combinatorial optimization questions stemming out of pc algorithms for applications inside the computer global of networks, circuit layout; many new algorithmic questions in linear algebra with new applications. For this reason we live in an technology while the 2 disciplines of arithmetic and pc science have installation many robust interactions. Those interactions and their interplay are main to the enrichment of each disciplines. Collectively they'll offer the proper force multiplier impact to take a look at and solution a number of the inner most questions bothering mankind – of cognition, self, and thought.

REFERENCES

- [1]. Knuth, D. E., The Art of Computer Programming Vol. 1 Fundamental Algorithms, Addison Wesley, New York, 1973.
- [2]. Dijkstra, E. W., A Short Introduction to the Art of Programming, Computer Society of India Press, Mumbai, 1977.
- [3]. Appel, K. and Haken, W., Every planar map is four colourable. Illinois J. Math., 1977, 21, 429–567.
- [4]. Manna, Z., Logics of Programs, Addison Wesley, 1987.
- [5]. Knuth, D. E., Algorithmic thinking and mathematical thinking. Am. Math. Monthly, 1986, 81, 322–343.
- [6]. Edmonds, J., Paths, trees and flowers. Can. J. Math., 1965,17, 449–467.
- [7]. Garey, M. R. and Johnson, D. S., Computers and Intractability– A Guide to the Theory of NP-com pleteness, W. H. Freeman, San Francisco, 1979.
- [8]. Lemmermeyer, F., Reciprocity Laws: From Euler to Eisenstein, Springer, New York, 2000.
- [9]. Edwards, H. M., Fermat's Last Theorem , Springer, New York, 1977.
- [10]. Knuth, D. E., The Art of Computer Programming Vol. 2 Seminumerical algorithms, Addison Wesley, New York, 1981.
- [11]. Yan, S. Y., Number Theory for Computing, Springer, New York, 2000.
- [12]. Knuth, D. E., The Art of Computer Programming Vol. 3 Sorting and Searching, Addison Wesley, New York, 1981.
- [13]. Aho, V., Hopcroft, R. E. and Ullman, J. D., Design and Analysis of Algorithms, Addison Wesley, New York, 1982.
- [14]. Aigner, M. and Ziegler, G. M., Proofs from The Book, Springer, New York, 1998.
- [15]. Abhijit Das and Veni Madhavan, C. E., Public Key Cryptography: Theory and Practice, Manuscript of a forthcoming book, 2005.
- [16]. van Lint, J. H. and Wilson, R. M., A Course in Combinatorics, Cambridge University Press, London, 1992.
- [17]. Gessel, I. and Gian-Carlo Rota (eds), Classic Papers in Combinatorics, Birkhauser, 1987.
- [18]. Jukna, S., Extremal Combinatorics with Applications to Computer Science, Springer, New York, 2001.
- [19]. Konig, D., Math. Ann., 1916, 77, 453–465.
- [20]. Hall, P., On representatives of subsets. J. London Math. Soc., 1935, 10, 26–30.
- [21]. Dilworth, R. P., A decomposition theorem for partially ordered sets. Ann. Math., 1950, 51, 161–166.
- [22]. Hardy, G. H. and Ramanujan, S., Asymptotic formulae in combinatory analysis. Proc. London Math. Soc., 1918, 17, 75– 115.
- [23]. Koblitz, N., A Course in Number Theory and Cryptography, Springer, New York, 1996.
- [24]. MacWilliam, F. J. and Sloane, N. J. A., The Theory of Error Correcting Codes, North Holland, New York, 1977.