© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 04 , Issue : 10 | October – December 2017

APPLICATIONS OF ALGORITHMS IN PURE MATHEMATICS

Balwan Singh , M.Sc, Mathematics
Rohtak, Haryana (India).

Abstract
The main interest of algorithms in algebraic number theory is that they provide number theorists with a means of satisfying their professional curiosity. The praise of numerical experimentation in number theoretic research is as widely sung as purely numerological investigations are indulged in, and for both activities good algorithms are indispensable. Algebraic number theory has in recent times been applied to the solution of algorithmic problems that, in their formulations, do not refer to algebraic number theory at all. so a description of algorithm along with its applications is necessary.

ISSN : 2348-5612 © URR
9 770234 856124

Complexity :-By analyzing the complexity of an algorithm we mean in this study finding a reasonably sharp upper bound for the running time of the algorithm expressed as a function of the length of the input data. This should, more precisely, be called time complexity, to distinguish it from space complexity. An algorithm is said to be polynomial-time or good if its running time is $(l+2)^{0(1)}$, where is the length of the input. Studying the complexity of a problem means finding an algorithm for that problem of the smallest possible complexity.

Encoding data - As we know the input and the output of an algorithm consist of finite sequences of nonnegative integers. However, in the mathematical practice of thinking and writing about algorithms one prefers to work with mathematical concepts rather than with sequences of nonnegative integers that encode them in some manner. Thus, one likes to say that the input of an algorithm is given by an algebraic number field rather than by the sequence of coefficients of a polynomial that defines the field; and it is both shorter and clearer to say that one computes the kernel of a certain endomorphism of a vector space than that one determines a matrix of which the columns express a basis for that kernel in terms of a given basis of the vector space.

Algorithms :- An algorithm is that recipe which works on finite sequence of nonnegative integers, called the input data, produces another, called the output. Formally, an algorithm may be defined as a Turing machine, but for several of our results it is better to choose as our "machine model" an idealized computer that is more realistic with respect to its running time,where the length of a finite sequence of nonnegative integers $n_1,n_2.....,n_i$ is defined to be$\sum_{i=1}^{t} \log(n_i + 2)$.

Here we are discussing applications of algothmic approach in different fields of mathematics

Elementary arithmetic - The traditional algorithms for addition and subtraction take time $0^{(l)}$, where is the length of the input. The ordinary algorithms for multiplication and division with remainder, as well as the Euclidean algorithm for the computation of greatest common divisors, have running time $0(l^2)$. With the help of more sophisticated methods this can be improved to $l^{1+0(1)}$ for $1\rightarrow\infty$ .An operation that is not known to be doable by means of a good algorithm is decomposing a positive integer into prime numbers, but there is a good probabilistic algorithm for the related problem of deciding whether a given integer is prime. No good algorithms are known for the problem of recognizing square free numbers and the

problem of finding the largest square dividing a given positive integer, even when the word "good" is given a less formal meaning.

Linear algebra :- Let F be a field, and suppose that one has agreed upon an encoding of its elements, as is the case when F is the field Q of rational numbers or the field Fp for some prime number p. Giving a finite-dimensional vector space over F simply means giving a nonnegative integer n, which is the dimension of the vector space. This number n is to be given in unary, i.e., as a sequence 1, 1, ... , 1 of n ones, so that the length of the encoding is at least n. This is because almost any algorithm related to a vector space of dimension n takes time at least n. The elements of such a vector space are encoded as sequences of n elements of F. Homomor- phisms between vector spaces are encoded as matrices. A subspace of a vector space can be encoded as a sequence of elements that spans the subspace, or as a sequence of elements that forms a basis of the subspace, or as the kernel of a homomorphism from the vector space to another one.

Rings: -Almost any ring that we need to encode an additive group that is either finitely generated or a finite dimensional vector space over Q.Ideals are encoded as subgroups or, equivalently, as kernels of ring homomorphisms. There are good algorithms for computing the sum, product, and intersection of ideals, as well as the ideal $I: J = \{x \epsilon A: xJ \subset I\}$ for given I and J, and the quotient ring of A modulo a given ideal.

A polynomial over a ring is always supposed to be given by means of a complete list of its coefficients, including the zero coefficients; thus we do not work with sparse polynomials of a very high degree.

Local fields: - A local field is a locally compact, nondiscrete topological field. Such a field is topologically isomorphic to the field R of real numbers, or to the field C of complex numbers, or, for some prime number p, to a finite extension of the field Qp of p-adic numbers, or, for some finite field E, to the field E((t)) of formal Laurent series over E. A local field is uncountable, which implies that we have to be satisfied with specifying its elements only to a certain precision. The discussion below is limited to the case that the field is non-archimedean, i.e., not isomorphic to R or C.

Conclusion:-use of the algorithms in mathematics is not new but for the pure mathematics like linear algebra, group theory and ring theory and finite dimensional vector space is very interesting and very useful for development of computer based number theory .apart from that fast convergence algorithm there is a strong need of further research on that .encoding of subgroups,rings,time scale,basis and coordinates is anew pattern for the future research

REFERENCES

- Avigad, Jeremy (2006). \Methodology and metaphysics in the development of Dedekind's theory of ideals". In: The Architecture of Modern Mathematics. Ed. by Jose Ferreiros and Jeremy Gray. Oxford University Press, pp. 159{186 (cit. on pp. 8, 30).
- G. Greaves, Sieves in Number Theory. Results in Mathematics and Related Areas (3), 43. Springer-Verlag, Berlin, 2001.
- Gabor Ivanyos, Marek Karpinski, Lajos Ronyai, and Nitin Saxena. Trading GRH for algebra: algorithms for factoring polynomials and related structures. CoRR, abs/0811.3165, 2008. 30
- H.Cohen, A course in computational algebraic number theory, Springer-Verlag, Berlin, 1993. MR 94i:11105