WeSchool Knowledge Builder - The National Journal 2015
Volume -3 | 2015 | ISBN 978-1-63102463-4
weschool.editor@rtmonline.in |http://weschool.rtmonline.in | http://www.rtmonline.in

THEORETICAL CONCEPT OF ALGEBRAIC NUMBER THEORY

by

Nurul Amin | Research Scholar | Maharishi University of Information Technology, Lucknow, Uttar Pradesh

&

Dr V K Rathaur Ph.d | Research Supervisor | Maharishi University of Information Technology, Lucknow, Uttar Pradesh

ABSTRACT

Algebraic number theory is the branch of number theory that deals with algebraic numbers. Historically, algebraic number theory developed as a set of tools for solving problems in elementary number theory, namely Diophantine equations (i.e., equations whose solutions are integers or rational numbers). Using algebraic number theory, some of these equations can be solved by "lifting" from the field $\mathbb{Q}$ of rational numbers to an algebraic extension K of $\mathbb{Q}$. An algebraic number field is a finite extension field of the field of rational numbers. Within an algebraic number field is a ring of algebraic integers, which plays a role similar to the usual integers in the rational numbers. The study of algebraic number theory goes back to the nineteenth century, and was initiated by mathematicians such as Kronecker, Kummer, Dedekind, and Dirichlet. Gauss called Algebraic Number Theory the ``Queen of Mathematics."

KEYWORDS: Algebraic, study, Number Theory, Mathematics, field, problems, solving problems, branch, etc.

INTRODUCTION

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 [1]. What makes an algorithm good unfortunately defies definition—too many extra-mathematical factors affect its practical performance, such as the skill of the person responsible for its execution and the characteristics of the machine that may be used [2].

The present study addresses itself not to the researcher who is looking for a collection of well-tested computational methods for use on his recently acquired personal computer. Rather, the intended reader is the perhaps imaginary pure mathematician who feels that he makes the most of his talents by staying away from computing equipment. It will be argued that even from this perspective the study of algorithms, when considered as objects of research rather than as tools, offers rich rewards of a theoretical nature. The problems in pure mathematics that arise in connection with algorithms have all the virtues of good problems [3]. They are of such a distinctly fundamental nature that one is often surprised to discover that they have not been considered earlier, which happens even in well-trodden areas of mathematics; and even in areas that are believed to be well-understood it occurs frequently that the existing theory offers no ready solutions, fundamental though the problems may be. Solutions that have been found often need tools that at first sight seem foreign to the statement of the problem [4].

REVIEW OF LITERATURE

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. That this occurs in the context of solving Diophantine equations does not come as a surprise, since these lie at the very roots of algebraic number theory [5]. A better example is furnished by the seemingly elementary problem of decomposing integers into prime factors. Among the ingredients that make modern primarily tests work one may mention reciprocity laws in cyclostomes fields, arithmetic in cyclic fields, the construction of Hilbert class fields of imaginary quadratic fields, and class number estimates of fourth degree CM-fields. The best rigorously proved time bound for integer factorization is achieved by an algorithm that depends on quadratic fields, and the currently most promising practical approach to the same problem, the number field sieve, employs "random" number fields of which the discriminates are so huge that many traditional computational methods become totally inapplicable. The analysis of many algorithms related to algebraic number fields seriously challenges our theoretical understanding, and one is often forced to argue on the basis of heuristic assumptions that are formulated for the occasion [6]. It is considered a relief when one runs into a standard conjecture such as the generalized Riemann hypothesis or Leopold's conjecture on the no vanishing of the p-adic regulator.

In this study we will consider algorithms in algebraic number theory for their own sake rather than with a view to any of the above applications [7]. The discussion will be concentrated on three basic algorithmic questions that one may ask about algebraic number fields, namely, how to determine the Galois group of the normal closure of the field, or, more generally, of any polynomial over any algebraic number field; how to find the ring of integers of the field; and how to determine the unit group and the ideal class group of that ring of integers. These are precisely the subjects that are discussed in Algorithmic algebraic number theory [8] but our point of view is completely different. Present algorithms that "yield good to excellent results for number fields of small degree and not too large discriminate", but our attitude will be decidedly and exclusively asymptotic. For the purposes of the present study one algorithm is considered better than another if, for each positive real number N, it is at least N times as fast for all but finitely many values of the input data. It is clear that with this attitude we can make no claims concerning the practical applicability of any of the results that are achieved [9]. In fact, following Archimedes one should be able, on the basis of current physical knowledge, to find an upper estimate for all sets of numerical input data to which any algorithm will ever be applied, and an algorithm that is faster in all those finitely many instances may still be worse in our sense.

1. Algorithms in Algebraic Number Theory:

Algorithms and complexity - It is assumed that the reader has an intuitive understanding of the notion of an algorithm as being a recipe that given one 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, which is another intuitively clear notion that we do not define. We refer to and the literature given there for a further discussion of these points.

The length of a finite sequence of nonnegative integers $n_1, n_2, \ldots, n_t$ is defined to be $\sum_{i=1}^{t} \log(n_i + 2)$. It must informally be thought of as proportional to the number of bits needed to spell out in binary. 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 it’s running time is $(l+2)^{O(1)}$, where l is the length of the input Studying the complexity of a problem means finding an algorithm for that problem of the smallest possible complexity. In the present study we consider the complexity analysis complete when a good algorithm for a problem has been found, and we will not be interested in the value of the 0-constant. Informally, a problem has a good algorithm if an instance of the problem is almost as easily solved as it is formulated.

Encoding data - As stated above, 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. To justify such a concise mode of expression we have to agree on a way of encoding entities such as number fields, vector spaces, and maps between them by means of finite sequences of nonnegative integers. That is one of the purposes of the remainder of this section. Sometimes there is one obvious way to do the encoding, but often there are several, in which case the question arises whether there is a good algorithm that passes from one encoding to another. When there is, we will usually not distinguish between the encodings, although for practical purposes they need not be equivalent.

Elementary arithmetic - By Z we denote the ring of integers. Adding a sign bit we can clearly use nonnegative integers to represent all integers. The traditional algorithms for addition and subtraction take time $O(l)$, where l 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 $O(l^2)$. With the help of more sophisticated methods this can be improved to $l^{1+o(1)}$ for $l \to \infty$.

2. Number Theory (Analytic and Combinatorial Number Theory, Algebraic Number Theory):

One of the features of the analytic and combinatorial number theory is the interplay of a great variety of mathematical techniques, including combinatory, harmonic analysis, probability theory, algebraic geometry or ergodic theory. The modern analytic number theory has benefitted from the harmonic analysis in some groups related to auto orphic forms, while Additive Combinatory is a relatively recent term coined to comprehend the developments of the more classical combinatorial number theory, mainly focused on problems related to the addition of integers [10].

Algebraic Number Theory: Many problems in arithmetic can be translated into the problem of deciding if an algebraic variety contains rational points. Modular varieties and modular curves appear in the proof of three cornerstones in this area: Fatlings proof of Modell's conjecture; Wiles proof of Fermat's last theorem using the Shimura-Taniyama-Weil conjecture, and the Birch and Swine ton-Dyer conjecture whose case of analytic rank one has been proved by Gross-Zagier and Kolyvagin. The concept of height also plays a central role; it appears in two of these proofs and has been used to design algorithms to solve Diophantine equations. The Arakelov theory provides a framework to give precise definitions of heights and to study its properties.

CONCLUSION

In this study we discuss the basic problems of algorithmic algebraic number theory. The emphasis is on aspects that are of interest from a purely mathematical point of view, and practical issues are largely disregarded. We describe what has been done and, more importantly, what remains to be done in the area. We hope to show that the study of algorithms not only increases our understanding of algebraic number fields but also stimulates our curiosity about them. The discussion is concentrated of three topics: the determination of Galois groups, the determination of the ring of integers of an algebraic number field, and the computation of the group of units and the class group of that ring of integers. The researchers in Algebraic Number Theory at LSU also are studying Quadratic Forms both from the algebraic point of view (function fields of quadrics, generic splitting, The methods used in these studies include techniques from diverse areas of algebra.

REFERENCES

1. 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).
2. G.Greaves, Sieves in Number Theory. Results in Mathematics and Related Areas (3), 43. Springer-Verlag, Berlin, 2001.
3. 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
4. H.Cohen, A course in computational algebraic number theory, Springer-Verlag, Berlin, 1993. MR 94i:11105
5. H.P.F. Swinnerton-Dyer. *A Brief Guide to Algebraic Number Theory*. University Press of Cambridge, 2001.

6. Harper, M., and Murty, R., Euclidean rings of algebraic integers, *Canadian Journal of Mathematics*, **56**(1), (2004), 71-76.
7. J. A. Buchmann and H. W. Lenstra, Jr., Approximating rings of integers in number fields, J. Th_eor. Nombres Bordeaux 6 (1994), no. 2, 221{260. MR 1360644 (96m:11092) **8.** J.W.S. Cassels, Global fields, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42{84.
8. Kimball Martin. Nonunique factorization and principalization in number fields. Proc. Amer. Math. Soc. 139, No. 9: 3025-3038, 2011.
9. Lawrence C. Washington, Introduction to cyclotomic fields, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130).