International Journal of Engineering, Science and Mathematics
Vol. 6 Issue 5, September 2017,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

A STUDY ON ALGEBRAIC NUMBER THEORY AND ITS APPLICATIONS

Seema
Research Scholar, Calorx Teachers' University
Ahmedabad (Gujarat) - India

ABSTRACT

Current study explains the concept of Algebraic Number Theory and its applications. Study was based on the literature and descriptive in nature. Algebraic number theory is a rich and diverse subfield of abstract algebra and number theory, applying the concepts of number fields and algebraic numbers to number theory to improve upon applications such as prime factorization and primarily testing. In this study, researchers begin with an overview of algebraic number fields and algebraic numbers and then move into some important results of algebraic number theory, focusing on the quadratic, or Gauss reciprocity law.

KEYWORDS: Algebraic number, quadratic, number theory, factorization and Gauss reciprocity law.

INTRODUCTION TO ALGEBRAIC NUMBER THEORY

Algebraic number theory is a rich and diverse subfield of abstract algebra and number theory, applying the concepts of number fields and algebraic numbers to number theory to improve upon applications such as prime factorization and primality testing. In this study, we will begin with an overview of algebraic number fields and algebraic numbers. We will then move into some important results of algebraic number theory, focusing on the quadratic, or Gauss reciprocity law.

In this research, we will cover the basics of what is called algebraic number theory. Just as number theory is often described as the study of the integers, algebraic number theory may be loosely described as the study of certain subrings of fields K with $[K : \mathbb{Q}] < \infty$; these rings, known as "rings of integers", tend to act as natural generalizations of the integers. However, although algebraic number theory has evolved into a subject in its own right, we begin by emphasizing that the subject evolved naturally as a systematic method of treating certain classical questions about the integers themselves.

Much of our endeavour in the theoretical study of computation is aimed towards either finding an efficient algorithm for a problem or gauging the hairiness of a problem. And in meeting both these goals mathematical insights and ingenuities are constant companions. In particular, two branches of mathematics - combinatory, and algebra and number theory, have found extensive applications in theoretical computer science. In this thesis, our focus is on problems belonging to the latter branch.

For the past few decades there has been a growing interest among computer scientists and mathematicians, in the field of computational number theory and algebra. Computational number theory is the branch of computer science that involves finding efficient algorithms for algebraic and number theoretic problems. Since its inception in the early 1960s, this field has continued to grow with ever- rising interest among researchers from diverse disciplines that resulted in a fruitful union of different areas in mathematics and computer science, especially algebra, number theory and computational complexity theory.

Factoring large integers, checking if an integer is prime, factoring polynomials, multiplying large integers and matrices, and solving polynomial equations are a few among a plethora of problems that have made this area so rich and fascinating. Unlike numerical analysis, here we are interested in exact solutions to problems instead of approximate solutions. Owing to the fundamental nature of the problems involved, this is a subject of intense theoretical pursuit. And the tools and techniques developed to solve these problems have provided researchers with deep mathematical insights. But interest in them has escalated in recent time because of their important applications in key areas like cryptography, coding theory and complexity theory.

The subject of algebraic number theory, taught today with algebraic number fields $\mathbb{Q}(\alpha)$ as the central objects and with unique factorization recovered through the theory of ideals, has been built and rebuilt since the early nineteenth century in terms of different objects, and according to different methodologies. We review the nature of these alternative approaches here, and in the process will encounter the major questions that we will be concerned with in this thesis.
In early work, such as P.G.L. Dirichlet's (1805 - 1859) studies on what we today call units in the rings of integers of number fields, the notion was not that one was studying a collection called a "number field" but that one was simply studying the rational functions in a given algebraic number, i.e. expressions of the form

$$\frac{c_m\alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_0}{d_n\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_0}$$

Where the coefficients ci and dj were rational numbers, and where a was some fixed algebraic number, i.e. the root of a polynomial with rational coefficients.

$$a_k z^k + a_{k-1} z^{k-1} + \cdots + a_0$$

Even after R. Dedekind (1831 - 1916) introduced the term "Zahlkorper" ("number field" in English) in 1871, some, for example K. Hensel (1861 - 1941), persisted for at least a little while longer in thinking in the way that Dirichlet had, i.e. simply in terms of rational functions of an algebraic number. In this, Hensel was probably influenced by his teacher L. Kronecker (1823 - 1891), who did not believe that mathematics could legitimately deal with infinite completed
totalities like Zahlkdrper. For a time, Hensel teetered between the less popular framework of his doctoral advisor Kronecker, and the more popular Dedekindian viewpoint, for example opening a research of 1894 with, let x be a root of an arbitrary irreducible equation of nth degree with integral coefficients.

$$\xi = \varphi(x)$$

All rational functions of x with integral coefficients then form a closed domain $(\mathfrak{G})$ of algebraic numbers, a Gattungsbereich in Kroneckerian, a field in Dedekindian nomenclature. Hensel eventually came to use Dedekind's notion of Zahlkdrper himself (e.g. (Hensel 1904a, p. 66)), perhaps because it was expedient to use the same language that a majority of his intended audience wanted to use, or perhaps because he was not as philosophically strict as Kronecker.

Among Hensel's published papers, only seven mentions the terms Gattung or Gattungsbereich in the title; the first of these was published in 1889, and the last in 1897, while overall, Hense Fs publications run from 1884 to 1937. At least Kronecker's terminology, if not his conception of things, was still recalled by E. Hecke (1887-1947) ' as late as 1923, but gradually awareness of Kronecker's framework seems to have faded from popular discourse.

As for the means by which to recover unique factorization, there is a great deal more variation. For a basic pedigree of nineteenth century methods, we can begin by naming those of Dedekind, Kronecker, Hensel, and E.E. Kummer (1810- 1893), and we will say later how these methods relate to one another. There was also the approach of E.I. Zolotarev (1847 - 1878), who achieved a complete generalization of Rummer's theory to general number fields; using ideas almost identical with those Hensel would later publish. His treatise (Zolotarev 1880) was published posthumously and through an unfortunate reception never became widely known. There is a method by E. Selling, and there may be more still.

The basic problem, in today's language, is that in a number field such as $E = \mathbb{Q}(\sqrt{-5})$, the ring of integers may fail to have unique factorization. Following Dedekind, we define the ring of integers $\mathcal{O}_E$ in E to be the ring of all numbers $\alpha \in E$ whose minimal polynomial (defined to be monic) over $\mathbb{Q}$ has all integral coefficients. For this particular field $\mathbb{Q}(\sqrt{-5})$ it is equal to the set of all $\mathbb{Z}$ –linear combinations over the basis $\{1, \sqrt{-5}\}$.
Irreducibility of a non-unit $\alpha \in E$ means that in any factorization $\alpha = \beta\gamma$ of α, at least one of the factors β, γ must be a unit. Each of the numbers $2,\ 3,\ 1+\sqrt{-5}$ and $1-\sqrt{-5}$ is integral in E (since their minimal polynomials $x-2,\ x-3$ are x^2-2x+6, and), and it can be shown easily (by considering norms) that each is irreducible in $\mathcal{O}_E$, so that in

$$6 = 2 \cdot 3$$

$$6 = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$$

We have a failure of unique factorization: the number 6 can be factored into irreducibles in $\mathcal{O}_E$ in two distinct ways. Starting not with a quadratic field such as we have considered in this example, but with cyclotomic fields $\mathbb{Q}(\alpha)$, α a primitive λ^{th} root of unity, λ a positive rational prime, Kummer invented a way to "save" unique factorization, which he presented in detail in a research of 1847. The language of "saving" unique factorization is taken from a letter of 28 April 1847 from

Kummer to Liouville, 12 and it is figurative; we must take a moment to understand properly what was actually done by each of Kummer, Dedekind, Kronecker, and Hensel.

What each of these mathematicians did, in his own way, was to provide a correlate, of some kind, for each integer in a number field, (i.e. to define a mapping from the integers of a number field to some other domain of objects) in such a way that for the entire system of these correlated objects there was indeed a kind of unique factorization, and such that an algebraic integer a would divide another, β , if and only if the correlate of α "divided" the correlate of β. In this way all questions of divisibility in the ring of integers of a number field could be decided on the grounds of divisibility in a separate domain of correlated objects, where unique factorization did hold. Kummer initially called these correlated objects "ideal complex numbers", and later "ideal divisors". In subsequent work of Dedekind, Kronecker, and Hensel, this name curiously would be split in half, Dedekind referring to his objects as "ideals", while Kronecker and Hensel would call their objects "divisors".

In general, the correlated domain contained many more objects than just those that corresponded to algebraic integers. For one thing, in general the correspondence would be extended so that not just algebraic integers but all algebraic numbers (quotients of integers) would have a correlate; namely, an algebraic number would be written as a quotient of two algebraic integers, and then the correlate assigned to α would be the quotient of those assigned to β and to γ . Beyond this, however, there could be still more elements in the correlated domain, which corresponded to no algebraic number whatsoever, and this "surplus" represented the failure of unique factorization in a very precise sense: there would be a surplus in the domain correlated to a number field E if and only if unique factorization failed in E. I stress that this language of correlation is mine, and that individual writers held varying conceptions of what they were doing.

As for the pedigree of the methods of these four mathematicians, we receive different advice from different corners. H. Hasse (1898 - 1979), for one, would always speak of "the Kronecker-Hensel method of divisors". H. Weyl (1885 - 1955), on the other hand, in his book (Weyl 1940) depicts Hensel's method as the natural extension of Rummer's method, not Kronecker's. To the present author, Weyl's picture seems to be the more accurate, although time has not permitted a proper study of Kronecker's basic work on number fields (Kronecker 1882), commonly referred to as "the Grundzuge." To be fair, Hensel's work does involve Kronecker's forms, to some extent, but its defining characteristic, the use of p-adic numbers, seems to have its roots in Kummer. For the present discussion we will not try to settle this question, but will be satisfied to simply give a brief idea of the nature of each of the four methods. Dedekind's method seems to be the one that has remained the most well-known to this day, probably because it is the one taught in most graduate courses in algebraic number theory. This at least seems the proximate cause, whereas the distal cause must be "Hilbert's reigning influence" (as Hasse would put it) and his use of Dedekind's theory of ideals in his Zahlbericht (Hilbert 1897), which, according to Lemmermeyer and Schappacher, "was the principal textbook on algebraic number theory for a period of at least thirty years after its appearance," and "has served as a model for many standard textbooks on algebraic number theory through the present day". Or consider Corry, who writes that, Since Hilbert basically adopted Dedekind's approach as the leading one, and since the Zahlbericht became the standard reference text for mathematicians working in algebraic number theory, the publication of this survey turned

out to be a decisive factor for the consequent dominance of Dedekind's perspective over that of Kronecker within the discipline.
Weyl too expressed similar sentiments in 1944 (ibid., p. 148), as have many others. 18 Considering this eventual outcome, it is surprising to learn that Dedekind complained in an 1876 letter to R. Lipschitz (1832-1903) that he had given up hope that his theoretical framework would in his time interest anyone but himself (Edwards, Neumann, and Purkert 1982, p. 52).

The ideal at any rate, correlated to an algebraic number α is denoted (α) and is simply the set of all multiples of α with algebraic integers in the field in question. In general, ideals may be generated as the set of all linear combinations over any finite set of algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$, with the coefficients again being algebraic integers, and with such an ideal denoted $(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Only those ideals that can be generated by a single number are called principal. These principal ideals are the ones correlated to actual algebraic numbers; the others are the "surplus" which represents the failure of unique factorization.

Dedekind defines the product of two ideals I and J to be the set of all finite sums $\sum \alpha_i \beta_i$ with the α_i in I and the β_i in J. With respect to this notion of multiplication, Dedekind defines prime ideals to be those that are divisible only by themselves and by the ideal (1), i.e. the entire ring of integers. He shows that ideals have unique factorization into prime ideals.

Meanwhile, from the sketchy image of Kronecker's theory that can be gleaned from a cursory inspection of his Grundziige, together with hints from Weyl 1940, and especially Edwards's study (Edwards 1990), we may say a few things about Kronecker's theory of divisors.
Kronecker's approach is perhaps best understood by putting the failure of unique factorization in rings of algebraic integers into a different light. It can be expressed instead as the existence of pairs of integers $\alpha, \beta \in \mathcal{O}_E$ for which there is no greatest common divisor (CCD) in $\mathcal{O}_E$. This is equivalent to the failure of unique factorization, and it is in fact on the subject of greatest common divisors that Kronecker opens the second part of the Gmndzuge (Kronecker 1882, p. 45), in the section immediately before the one in which he introduces divisors (ibid., p. 48).

Given algebraic numbers $\alpha_1, \alpha_2, \ldots, \alpha_n,$ whereas Dedekind would form the ideal $I = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ generated by these numbers, Kronecker instead forms a polynomial, or form, having the α_i as its coefficients, namely, the linear form

$$f(u_1, u_2, \ldots, u_n) = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n$$

Where $u_1, u_2, \ldots, u_n$ are indeterminate. Immediately, the form f does appear to be in a certain sense equivalent to Dedekind's ideal I; if you allowed the indeterminate u_i to run over the ring of integers $\mathcal{O}_E$ then the set of values that the form f would take on would be precisely I. This already sounds like just the sort of alternative approach which we would expect Kronecker to prefer: instead of speaking of a completed infinite totality like I, we simply speak of a finite, symbolically representable form which in some way contains the same data.

An algebraic number field is a finite extension of $\mathbb{Q}$; an algebraic number is an element of an algebraic number field. Algebraic number theory studies the arithmetic of algebraic number fields — the ring of integers in the number field, the ideals in the ring of integers, the units, the extent to which the ring of integers fails to behave unique factorization, and so on. One important tool for this is "localization", in which we complete the number field relative to a metric attached to a prime ideal of the number field. The completed field is called a local field — its arithmetic is much simpler than that of the number field, and sometimes we can answer questions by first solving them locally, that is, in the local fields.

An abelian extension of a field is a Galois extension of the field with abelian Galois group. Global class field theory classifies the abelian extensions of a number field K in terms of the arithmetic of K; local class field theory does the same for local fields. This course is concerned with algebraic number theory. Its sequel is on class field theory. I now give a quick sketch of what the course will cover. The fundamental theorem of arithmetic says that integers can be uniquely factored into products of prime powers: an $m \neq 0$ in $\mathbb{Z}$ can be written in the form, $m = up_1^{r_1} \cdots p_n^{r_n}, \quad u = \pm 1,$ p_i prime number, $r_i > 0,$ and this factorization is essentially unique. Consider more generally an integral domain A. An element $a \in A$ is said to be a unit if it has an inverse in A: I write $A^{\times}$ for the multiplicative group of units in A. An element p of A is said to prime if it is neither zero nor a unit,

$$p|ab \Rightarrow p|a \text{ or } p|b.$$

If A is a principal ideal domain, then every nonzero nonunit element a of A can be written in the form, $a = p_1^{r_1} \cdots p_n^{r_n},$ prime element, $r_i > 0,$ and the factorization is unique up to order and replacing each p_i with an associate, i.e., with its product with a unit. Our first task will be to discover to what extent unique factorization holds, or fails to hold, in number fields. Three problems present themselves. First, factorization in a field only makes sense with respect to a subring, and so we must define the "ring of integers" $\mathcal{O}_K$ in our number field K. Secondly, since unique factorization will in general fail, we shall need to find a way of measuring by how much it fails.

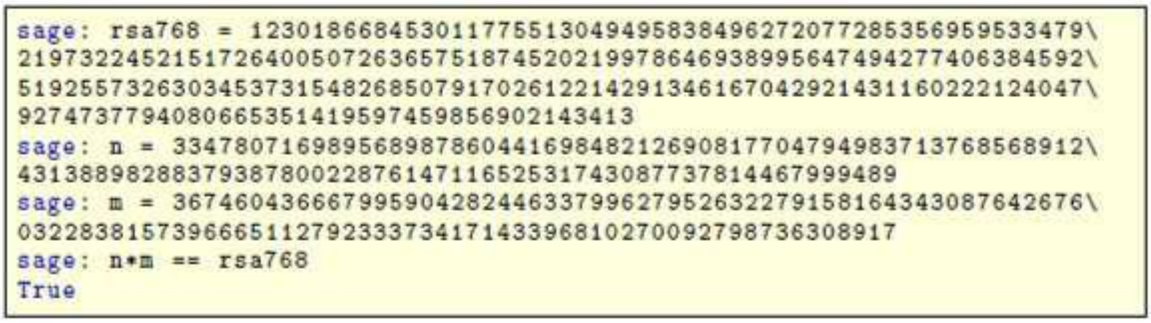
Finally, since factorization is only considered up to units, in order to fully understand the arithmetic of K, we need to understand the structure of the group of units UK in $\mathcal{O}_K$ resolving these three problems will occupy the first five sections of the course.

OBJECTIVES: Current study explains the concept of Algebraic Number Theory and its applications.

APPLICATIONS OF ALGEBRAIC NUMBER THEORY

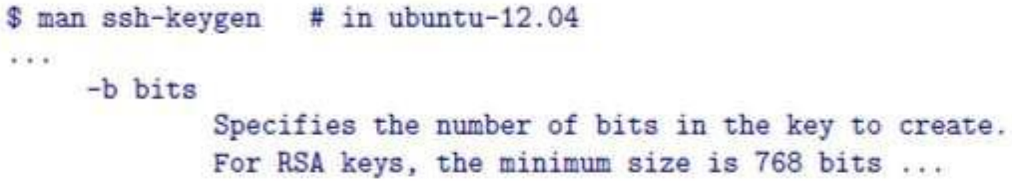
The following examples illustrate some of the power, depth and importance of algebraic number theory.

1. Integer factorization using the number field sieve. The number field sieve is the asymptotically fastest known algorithm for factoring general large integers (that don't have too special of a form). On December 12, 2009, the number field sieve was used to factor the RSA-768 challenge, which is a 232-digit number that is a product of two primes:



```
sage: rsa768 = 123018668453011775513049495838496272077285356959533479\
219732245215172640050726365751874520219978646938995647494277406384592\
519255732630345373154826850791702612214291346167042921431160222124047\
927473779408066535141959745985690214341 3
sage: n = 334780716989568987860441698482126908177047949837137685689l2\
431388982883793878002287614711652531743087737814467999489
sage: m = 367460436667995904282446337996279526322791581643430876426 76\
032283815739666511279233373417143396810270092798736308917
sage: n*m == rsa768
True
```

This record integer factorization cracked a certain 768-bit public key cryptosystem, thus establishing a lower bound on one's choice of key size:



```
$ man ssh-keygen   # in ubuntu-12.04
...
     -b bits
             Specifies the number of bits in the key to create.
             For RSA keys, the minimum size is 768 bits ...
```

2. Primality testing: Agrawal and his students Saxena and Kayal from India found in 2002 the first ever deterministic polynomial-time (in the number of digits) primality test. There methods involve arithmetic in quotients of $(\mathbb{Z}/n\mathbb{Z})[x]$, which are best understood in the context of algebraic number theory.

3. Deeper point of view on questions in number theory:

4. Pell's Equation $x^2 - dy^2 = 1$ can be reinterpreted in terms of units in real quadratic fields, which leads to a study of unit groups of number fields.

5. Integer factorization leads to factorization of nonzero ideals in rings of integers of number fields.

6. The Riemann hypothesis about the zeros of $\zeta(s)$ generalizes to zeta functions of number fields.

7. Reinterpreting Gauss's quadratic reciprocity law in terms of the arithmetic of cyclotomic fields $\mathbb{Q}(e^{2\pi i/n})$ leads to class field theory, which in turn leads to the Langlands program.

8. Wiles's proof of Format's Last Theorem, i.e., that the equation $x^n + y^n = z^n$ has no solutions with x. y.z.n all positive integers and $n \geq 3$, uses methods from algebraic number theory extensively, in addition to many other deep techniques. Attempts to prove Fermat's Last Theorem long ago were hugely influential in the development of algebraic number theory by Dedekind, Hilbert, Kummer, Kronecker, and others.

9. Arithmetic geometry: This is a huge field that studies solutions to polynomial equations that he in arithmetically interesting rings, such as the integers or number fields. A famous major triumph of arithmetic geometry is Faltings's proof of MordelPs Conjecture.

Theorem (Faltings). Let X be a non-singular plane algebraic curve over a number field K. Assume that the manifold X $(\mathbb{C})$ of complex solutions to X has genus at least 2 (i.e., X $(\mathbb{C})$ is topologically a donut with two holes). Then the set X (K) of points on X with coordinates in K is finite.

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 150
- H.P.F. Swinnerton-Dyer. A Brief Guide to Algebraic Number Theory. University Press of Cambridge, 2001.
- Harper, M., and Murty, R., Euclidean rings of algebraic integers, Canadian Journal of Mathematics, **56**(1), (2004), 71-76.
- 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)
- J.W.S. Cassels, Global fields, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 42{84.
- Kimball Martin. Nonunique factorization and principalization in number fields. Proc. Amer. Math. Soc. 139, No. 9: 3025-3038, 2011.
- Lawrence C. Washington, Introduction to cyclotomic fields, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997. MR 1421575 (97h:11130)
- M.Artin, Algebra, Prentice Hall Inc., Englewood Clients, NJ, 1991. MR 92g:00001
- Michael Atiyah and Ian G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley, 1969.
- Mollin, Richard: Algebraic Number Theory. Chapman and Hall/CRC Press. 1999
- Murty, R., Problems in Analytic Number Theory, GTM/RIM 206, Springer-Verlag, 2001
- Ono, Takashi: An Introduction to Algebraic Number Theory. Plenum Publishing Corporation. 1990
- S. Lang, Algebraic numbers, Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London, 1964. MR 28 #3974
- Schwermer, Joachim (2007). Minkowski, Hensel, and Hasse: On the Beginnings of the Local-Global Principle".In: Episodes in the History of Modern Algebra (1800-1950).
- Serge Lang. Algebra revised 3rd ed. Springer-Verlag, 2002.
- Serge Lang. Algebra. Springer-Verlag, New York Inc., third edition, 2002. 11

- Steve Chien and Alistair Sinclair. Algebras with Polynomial Identities and Computing the Determinant. In FOCS, pages 352{361, 2004. 82
- Victor Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, New York, 2009. Available from http://shoup.net/ntb/.
- W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), no. 3{4, 235{265, Computational algebra and number theory (London, 1993). MR 1 484478