RESEARCH REVIEW JOURNALS
Volume-04
Issue-01
January-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Statistical Analysis of Algebraic Number Theory in Particular Area

[1]Rupen Chatterjee and [2]Dr. V. Meena

[1]*Research scholar Sri Satya Sai University, Sehore, Bhopal*
[2]*Research Supervisor Sri Satya Sai University, Sehore, Bhopal*

ARTICLE DETAILS

Article History
Published Online: 20 January 2019

Keywords
Statistical analysis, algebraic number theory, algorithms, problems, mathematics

ABSTRACT

The study problems of algorithmic algebraic number theory are discussed in this paper in particular. The focus is on aspects of purely mathematical interest, and practical issues are largely ignored. We define the activities and, above all, what still needs to be carried out in this area. We aim to show that the study of algorithms not only improves our comprehension of algebraic areas but also increases our interest. The main interest of the algorithms is that they offer numerical theoreticians a way to satisfy their professional curiosity. Numerical testing in numerical theoretical research is praised as widely as numerical research is praised and good algorithms are necessary for both activities. What sadly makes an algorithm good defies its definition – too many extra-mathematical factors affect its practicability, such as the capacity of the operator and the characteristics of the machine to be used. Problems with algorithms in pure mathematics have all the virtues of good problems. They are so fundamentally essential that one is often surprised to discover that they were not previously considered, even in well-trodden fields of mathematics; and often even in fields which are thought of as well as well as well-understood, there are no ready solutions to the existing theory, even if they are fundamental. Often found solutions need tools that seem to be foreign to the declaration of the problem at first sight.

1. Introduction

The algebraic theory of number is a branch theory which uses abstract algebraic techniques to study integral, rational and generalized figures. Number-theoretical questions relate to properties of algebraic objects such as algebraic numbers, integers and finite fields and function fields. The following questions are discussed: These properties can solve questions of primary importance for theoretical numbers, like the existence of solutions to diophantine equations, such as whether a ring recognizes a unique factorisation, ideal behavior and the Galois field groups.

In recent times, algebraic number theory has been used to solve algorithmic problems that do not at all refer to algebraic number theory in their formulations. This is not a surprise, because they are at the root of algebraic count theory, in solving diophantine equations. The apparently basic problem of breaking down integrals into primary factors gives a better example. The construction of Hilbert grade fields of imaginary quadratic fields and class number estimates of fourth grade CM-fields are some of the ingredients which make up the modern test for primalities. The most stringently demonstrated time-based factorization is achieved by a quadratic algorithm and the most promising approach to the problem at this time: the number field sieve, which uses so large 'random' fields of numbers which allow discrimination to become totally inapplicable by many traditional computational methods. The analysis of many algorithms related to the algebraic numbers challenges our theoretical understanding seriously, and one is often forced to dispute heuristic assumptions. It is considered an aid in a standard speculation such as the generalized Riemann hypothesis or the speculation of Leopoldt that p-adic regulators do not fade away. In this document, we consider algorithms in algebraic number theory for themselves rather than for any of the applications mentioned above.

The discussion will focus on three basic algorithmic questions one can ask regarding the fields of algebraic number: how the Galois group is to determine the normal closure of the field or, generally speaking, any polynomial over all algebraic fields; how the field integral ring is to be determined; These are exactly the topics discussed by M within the algorithmic theory of algebraic number. Pohst and H. Pohst and H. But our view is entirely distinct from the Zassenhaus (Cambridge, 1989). The algorithms provided by Pohst and Zassenhaus are 'strong to great results in small and not too large areas,' but the approach we take is clearly and exclusively asymptotic. In the current paper, a single algorithm is better than another if it is at least N times fast for every positive number N, except for the limited number of input data values. for every positive real number N. We can obviously make no statements with this mindset as to the functional applicability of any of the findings. Actually, after Archimedes, it should be possible to find an upper limit for all numeric input sets, on the basis of current physical knowledge, and in all these finitely many conditions an algorithm that is faster can still become worse in our context.

The above can seem ridiculous to some people. It's liberation and relaxation to the intended reader, who would never use any algorithm anyway. If he clearly abandons all realistic statements, he understands that he can deal with algorithms without fear of the bad dreams generated by the messy specifics and dirty tricks between the elegant and the functional implementation of the algorithm. It is located in the platonic paradise of pure mathematics, where an algorithm 's conceptual and concise version is more valued than an ad hoc device that speeds it up to a factor of ten, and where words have precise meaning which does not change when the world changes. He never needs to enter the obscure factories that are full of applied mathematicians in his imagination, where boxes full of numbers called the matrices are transported and

RRIJM 2015, All Rights Reserved

real electronic computers feed on proliferating triple indices. And he knows in his heart that his own work will eventually have the widest range of applications, just as no specific application was taken into account.

2. Modern Number Theory

For me, part of the appeal of modern number theory is that it seems to have much more of a unified sense of purpose than any other branch of math. Nevertheless, it seems to me that since that Diophantus and Euclid number theory has concerned itself with two basic questions:

• The properties of the primes, and

• The solutions of polynomial equations.

Let me continue with what I see as the large picture and break it down to where I have learned every single pixel. Some words that I use here will seem obscure, but I will refer to them again in the related subsection below. It is my full understanding of Langlands. Two L-functions are available. There are numerical theories or sometimes geometry-dirichlet and ddekind Zeta functions which immediately lead to L-functions counting on elliptical curves or L-functions, which are somewhat important. The other form comes from the theory of representation. For example, modular shapes are some kind of SL(2,Z) representation. L-functions are connected with these linear forms. There are several different functions to take into account and you obviously have to look at classes greater than SL(2,Z). I run up here to the edge of what I know but in fact you are at least as far as algebraic groups and groups of Lie are concerned. The assumption is, then, that both L-functions are the same. Each L-function number theory is consistent with one theory of representation. However, the connection is more complex. This is the meaning of the word functionality. In one hand you should combine L-features and this will somehow fit that on the other hand you combine them. For example, if you have L functions that match the extensions (Dedekind), you can use a composite field extension and now you have a new zeta function which is a combination of the two above in some way. Then on the other side should be three L functions and somehow a combination of the first two with the third function. In any case, there would appear to be a fair amount of needed background to even understand all of these functions, at the least sufficient to keep me busy in the near future.

3. Classical Algebraic Number Theory

If your theory of numbers hoped to make some of the students mathematician, it took some time to achieve quadratic reciprocity. This is just the easiest example of a far larger theory, which deals again with our two fundamental questions. We see a larger field, say K when we solve an irreducible polynomial over Q. The algebraic integers within K now correspond to Z within Q. Please note that an element α / to K is algebraic for a field extension of K, if a polynomial f(x) = Q[x] has been met. We now talk to you about the minimal polynomial of α if we request a small polynomial of a size so that the leading coefficient is 1. It is also important if f(x) has the minimum polynoms and coefficients in Z .. We make a further distinction. Now since Q has characteristic 0, every algebraic extension is separable, so by the primitive element theorem every extension K is of the form Q[α]. It is not true in general, however, that OK, the ring of algebraic integers, is equal to Z[α]. For instance, if K = Q[√ 5], then Z[√ 5] is contained in, but is not equal to, the ring of integers. In fact,

$$O_K = \mathbb{Z}[\frac{1+\sqrt{5}}{2}].$$

Generally speaking, it is difficult to find the ring of integer(although quadratic extensions are easy to do so). What is true is that the whole ring is the free Z module n = [K: Q]. Indeed, the ring of fundamental objects as a ring can be stated much more.

A commonly asked test or generals question is to name a ring that is not a UFD. The standard answer is Z[√ −5]. This is a standard mathematical theme: by looking at a large object, we can gain something but also lose something. We are algebraically shut, for example, by moving from R to C, but we are losing our order. Likewise, we get solutions to a polynomial in the ring of the integers over Z, but we lose the special factorisation. Note that it is a problem factorizing the structure of the primes with our other theme. Although we can no longer convert elements into primary elements exclusively from factor ideals to prime ideals. If we start with a primary ideal in Z, it can remain prime or not, that is to say, there can be greater prime ideals and more than one prime ideal. Exactly three things can happen at prime p of Z, for example, in the ring of integer Z[i]. I mean pZ[i], that is, the ideal generated by p in this larger ring.

$$\begin{array}{ll} p=2 & (p)=(1+i)^2 \\ p\equiv 1 \pmod 4 & p=(a+bi)(a-bi) \text{ where } a^2+b^2=p \\ p\equiv 3 \pmod 4 & (p)=(p) \end{array}$$

p is said to ramify in the first case, in the second to split, and in the third to be inert. Note that p in Z[i] is about whether −1 is a square (mod p). We use quadratic reciprocity in order to see whether −1 is a square (mod p). Generally speaking, (p) action in Z[alternatively] has to do with whether or not x 2 − q divides (mod p).

4. Analytic Number Theory

Analytical objects encoding knowledge about numbers fields are the first business order. These include the functions Dirichlet L, Dedekind zeta, Hecke L (which generalize the first two) and Arttin L (which generalizes the ones Hecke has). These link to algebraic theory of numbers via the formulation of class numbers which refers the class number to the value of a Dirichlet L feature, and the theorem of density of Tchebatorev, which tells you how primes split into extensions. We have their own property and software, however. The functions of Dirichlet L include the Riemann zeta function, which are equally used to address questions about primary numbers distribution (including primary numbers). We also share the essential functional equations and eulerfactorisation characteristics of meromorphic (or analytical) continuation. More specifically, let χ be a homomorphism from G = (Z/nZ) ∗ to C. Because χ is a homomorphism and every element in G has finite order, the image is actually contained in μφ(n) , the φ(n)th roots of unity. Extend this function to all of Z/nZ by letting χ(m) = 0 if (m, n) > 1. Now we can turn this into a function of Z by composing Z → Z/nZ → C. Now define the function

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

RRIJM 2015, All Rights Reserved

This function will be good, if we have chosen the μ right one (we want it to be primitive). In particular, if n = p, a certain prime p, all β are primitive. When we are clever in adding the difference · that matches a fixed p together, we get a sum that only selects terms n that match one (mod p). This is how one shows that

$$\sum_{\chi} L(\chi, s) \sim \sum_{q \equiv a \pmod{p}} \frac{1}{q^s},$$

where the sum on the right is over prime q. Then since the sum on the left diverges to ∞ as s → 1 + (it includes a term that is essentially the Riemann zeta function), there must be infinitely many q ≡ a (mod p). This is how one proves

5. Representation Theory

This happens in a variety of ways. Second, they are the theory of finite groups representation. Since the functions of Artin L are defined like this, it is helpful to know a bit about this. In his algebraic study of Lie algebras, Humphreys is very pure. It's all evidence but it can be hard to understand what is happening. Fulton & Harris is the opposite extreme, putting all proofs in (or doesn't) appendix, but is full of examples, giving you the general algorithm for the analysis of a semicircular Lie algebra representation. I think the Lie group phrase is not present at all in Humphreys, and Fulton & Harris are quite a runner, that it should be enough to take care of Lie algebras. Adams' lectures on Lie groups are great to study Lie groups. Some of her terminology is a little archaic, and parts of the evidence are being pointed out to other sources (as in the Peter-Weyl theorem). It is the groups you really care about, however, so it's necessary to read.

6. Commutative Algebra

This study for numerical theories and algebraic geometry as needed essentially. Since algebraic geometry often tells geometric facts based on algebraic data, algebraic facts need to be understood. But without pairing with geometry, it's difficult to remember algebraic facts, so you get an intuition.

7. Algebraic Geometry

Modern theory of algebraic number has been closely linked to algebraic geometry. I have heard that Deligne 's proof of the Weil conjectures and Falting's proof of Mordell's conjecture are two great results in number theory which show that algebraic geometry is effective. You must use some light algebraic geometry in what I've learned about algebraic geometry.

8. Elliptic Curves

Elliptic curves would generally be viewed as a substructure for algebraic geometry on a strictly logical basis. There seems, however, to be so much special that it does not apply in more general cases that it deserves its own study. In any case, I found it useful to learn about elliptical curves both because the theory itself is interesting and because it provides concrete examples of algebriac geometry definitions and theorems. An elliptic curve is an elliptic equation with coefficients across a base field in two variables. This naive interpretation needs to be refined. The first is that we need a curve that is not single-handed-this means that there are no double points, no cusps, no crossing points. This means that the curve is not secretly simpler than the equation of a third degree. It is analogous to a degenerated conical x 2, and 0 is the union of two sides, and thus one does not assume that the circle should be viewed as two sections. The quadratic x 2 − y 2 = 0. Similar questions about quadratics motivate many initial questions on elliptical curves. For example , you can ask for rational solutions given a quadratic equation like x 2 + y 2 = z 2. As I said earlier, to find solutions to the equations is one of the fundamental problems of count theory. To find logical solutions, we can simply split the two sides into z 2 and change variables to x 2 + y 2 = 1. Now this is a graphical equation over the actual figures — we get a circle. It is also an equation in which a solution can be easily found, e.g. (−1, 0). The smart part. Suppose (x , y) that the equation is another rational solution. Then there is a rational slope in the connection lines (−1, 0) and (x, y). Often, if we obey a logical incline, the circle at a point of rationality is crossed. This because it gives us a quadratic in one variable that we can solve with the quadratic equation if we consider the crossing of a line and a loop. Since one solution, x = −1, is known to be sound, the other solution also must be so. We have therefore a bijection from the set of rational paths Q to the rational points of the curve. Please note that the option of the initial component depends on this bijection. It follows the path t, it is the t 2−1 1+t 2 , 2 t 1+t 2. We return to the famous parametrization of the Pythagorean integer trio, x = m2 − n 2, y = 2mn, z = m2 + n 2. In this analysis, the fact that our equation was quadratic was something special, let 's say we had one rational point, we could consider the remainder of them. This problem would be even harder to increase the degree by 1. We think we have one rational point as we have done before. In fact the other condition of an elliptic curve, that is usually given as a base point. We change the variables and move the point to (0 , 0) if our curve exceeds Q (we already apply this map to algal geometry, which is a rational map and thus does not affect one of the essential curve properties). Indeed, we can use Y 2 = x 3 − g2x − g3 to write the equation on Q. Also, in this curve we would like to see the rational points. However, simply drawing a line with the rational pitch does not work on this time-most lines, but there is no guarantee that the other two are rational (or even true). It should cross the curve at three points.

However, we can manipulate the rational points of an elliptic curve with an algebraic property. In fact, on the issues that make them an abelite group, we can create a group law. Again, algebraic geometry is the most natural way to define this law, but it can be defined, though mysteriously, by simple planar geometry. Draw the secant line connecting the two dots P, Q on the curves (if P = Q, use a tangent line by P). This line crosses the curve at a third point. The curve is symmetrical to the x-axis because of the equation. Take the x-axis representation of the intersection point. This point is set to P + Q.

In terms of the P and Q co-ordinates, we can evaluate directly from the equation of the elliptical curve. We consider that P + Q has coordinates which are rational functions of P and Q co-ordinates. If P is a rational point, then P + Q is a rational point. Our operation is therefore on a number of rational points.

To make it a group, the identity, the additive inverse and the associative legislation have to be identified. Again, when

RRIJM 2015, All Rights Reserved

given from the algebraic geometry perspective, these seem more obvious but can still be addressed directly without it. Identity is the endlessness of the curve; intuitively, the endlessness point is at x = 0, and y = è, as. The drawing of the secant line from point P to point O is a vertical line that passes through P; then the described group operation gives you the point O. What should be the other way around −P is also clear, to reflect P on the x-axis. Finally, it is easy to verify the operation with the explicit form, albeit computationally heavy. Of reality, it's flipping.

9. Conclusion

Algebraic number theory-The way to define bias is through the group cohomology of the Galois Group in case of local class field theory. I 'm told that their cohomological characteristics are important when considering the specimens of a ring and systems. The main interest of the algorithms is that they offer numerical theoreticians a way to satisfy their professional curiosity. Numerical testing in numerical theoretical research is praised as widely as numerical research is praised and good algorithms are necessary for both activities. In reality, Fourier 's analysis is what often happens. Again, you could probably accept the theory as it is, and only allow Poisson to sum up. In complex analysis, the integration of contours must be understood-this is more difficult to do and takes as it is. In addition , it is important to learn more about complex analyzes as complex geometry, eventually for algebraic geometry.

References

1. L. M. Adleman and M. A. Huang, Recognizing primes in random polynomialtime, Research report, Dept. of Computer Science, Univ. of Southern California, 1988; Lecture Notes in Math., Springer, Heidelberg (to appear). Extended abstract: Proc. 19th Ann. ACM Sympos. on Theory of Computing (STOC), ACM, New York 1987, pp. 462–469.
2. L. M. Adleman and H. W. Lenstra, Jr., Finding irreducible polynomials over finite fields, Proc. 18th Ann. ACM Sympos. on Theory of Computing (STOC), ACM, New York (1986, pp. 350–355.
3. L. M. Adleman, C. Pomerance, and R. S. Rumely, On distinguishing prime numbers from composite numbers, Ann. of Math. (2) 117 (1983), 173–206.
4. Archimedes, The sand-reckoner, in: Opera quaequidem extant, J. Hervagius, Basel, 1544. (Greek and Latin)
5. A. O. L. Atkin and F. Morain, Elliptic curves and primality proving (to appear).
6. E. Bach, Explicit bounds for primality testing and related problems, Math. Comp. 55 (1990), 355–380.
7. E. Bach and J. O. Shallit, Factor refinement, J. Algorithms (to appear).
8. W. E. H. Berwick, Integral bases, Cambridge Univ. Press, Cambridge, 1927.
9. Z. I. Borevi˘c and I. R. Safarevi˘c, ˘ Teorija ˘cisel, Izdat. “Nauka”, Moscow, 1964; English transl.: Number theory, Academic Press, New York, 1966.
10. W. Bosma and M. P. M. van der Hulst, Primality proving with cyclotomy, Academischproefschrift, Universiteit van Amsterdam, 1990.
11. E. Brieskorn and H. Kn¨orrer, Ebene algebraischeKurven, Birkh¨auser, Basel, 1981.
12. J. Buchmann, Complexity of algorithms in algebraic number theory, Proceedings of the first conference of the Canadian Number Theory Association (R. A. Mollin, ed.), De Gruyter, Berlin, 1990, pp. 37–53.

RRIJM 2015, All Rights Reserved