Diophantine Approximation and Analytic Number Theory

M. Bennett (UBC),
A. Granville (Montreal),
J. Thunder (Northern Illinois),
G. Walsh (Ottawa)

5/30–6/4, 2010

1 Introduction

This conference dealt with two areas of Number Theory, "the queen of mathematics." Diophantine approximation can be broadly described as the solvability in rational integers to various inequalities. The name comes from the later Greek mathematician Diophantus, who studied the solutions to certain equations. Though clearly a very old branch of mathematics, it remains a vibrant area of study to this day. The last century saw many deep and powerful results: the theorems of Thue, Siegel and later Roth, Baker's linear forms in logarithms, and Schmidt's subspace theorem, to name but a few. Much recent work has melded the arithmetic nature of the subject with advances in algebraic geometry (e.g., the work of Faltings and Vojta), where one is interested in the properties of rational points on algebraic varieties defined over a number field. Recent successes in this area have lead to the solutions to many old and notoriously difficult problems.

Many mathematicians when asked about analytic number theory immediately think of the famous Riemann hypothesis and perhaps the Goldbach conjecture. In fact, the area is much more rich than that. Early last century Ramanujan together with Hardy, Littlewood and others developed analytic methods to answer questions about Diophantine equations. A famous example here would be Waring's problem, where one is concerned with writing an integer as a sum of equal powers of integers. This particular area has seen a recent resurgence of activity, spurred on by the work of Vaughn and Wooley. Another more recent line of work has brought probabilistic methods into the mix. The celebrated results of Green and Tao here bear testament to the efficacy of these ideas; they proved that the sequence of prime numbers contains arbitrarily long arithmetic progressions. Along more classical lines, Goldston and Yildirim have within the last five years made stunning progress on the study of gaps between prime numbers.

These two areas of number theory are far from being isolated "islands" in mathematics. Besides the obvious connections to algebra, geometry, complex variables, etc., these areas touch upon subjects as disparate as logic (via model theory), coding theory and cryptography. A glance at Math Reviews immediately confirms that Number Theory continues to be one of the most active subjects in all of mathematics, one that benefits from and employs tools from many areas, and where new applications continue to arise.

Finally, we note that this meeting was a tribute to the work of Cameron Stewart in celebration of his sixtieth birthday. Cam, as he is known to his friends and colleagues, has a lengthy record in these two areas of number theory and has made a great many outstanding contributions to the subject.

2 Overview of the Fields

It was observed early on that in order to find integer solutions to many Diophantine equations, one is naturally lead to approximating certain real numbers by rational numbers. For example, the old question of finding numbers that are both square and "triangular" results in a Pell equation, and as is well-known, the solutions to such equations come from good approximations to quadratic irrational numbers. These good approximations can be found, for example, using continued fractions. Unfortunately, finding such "good approximations" for algebraic numbers of higher degree still remains problematic to this day.

Let α be a real number. At its most basic, Diophantine approximation deals with finding rational numbers p/q (here p and q are relatively prime integers) with

$$\left|\alpha - \frac{p}{q}\right| < \frac{c(\alpha)}{q^{\delta}}, \qquad (*)$$

where $c(\alpha)$ is some positive number and $\delta \geq 2$. Liouville showed that for an algebraic number α of degree $d \geq 2$, there is a $c(\alpha)$ such that (*) has no solutions for $\delta \geq d$. On the other hand, Dirichlet showed that for any real number α, there are infinitely many solutions to (*) with $c(\alpha) = 1$ and $\delta = 2$.

Early last century Thue made a great breakthrough: he showed that for any algebraic α of degree $d \geq 3$, there are only finitely many solutions to (*) with $\delta > (d/2) + 1$. Unfortunately, while the methods of Thue allow one to get upper bounds on the *number* of such solutions, one has absolutely no information on the *size* (i.e., how large the denominator q may be) of such solutions. The method is called *ineffective*, as it doesn't allow one to find all such solutions (since the upper bounds one can derive for their number is most certainly larger than the "truth"). Nevertheless, a great deal of mathematics over the years has been devoted to extending and improving on Thue's original ideas. Two highlights are Roth's famous result [5] where he replaced Thue's bound above with the more simple $\delta > 2$, (Roth was awarded the Fields medal for his work) and Schmidt's famous subspace theorem (see [6], for example) which pushed things to higher dimensions (he won the Cole prize for his work).

Another great stride forward was made by A. Baker (see [1]). Briefly, he was able to prove effective upper bounds on the size of solutions to (*). This method, called linear forms in logarithms, is a major tool in solving Diophantine equations (Baker was awarded the Fields medal for his work). It does not make the Thue methods obsolete, however, since it yields rather large upper bounds on the size of the possible solutions. For example, Tijdeman used linear forms in logarithms to essentially "solve" Catalan's conjecture in 1976. But improvements to the method and quantum leaps in computing power were still unable to exhaust all possible solutions before the problem was completely resolved via algebraic number theoretic methods by Mihailescu in 2002.

The use of analytical tools and methods to solve questions about integers has a long history. One can start with Euler's product formula which relates the Riemann zeta function with the primes. The proof of the prime number theorem late in the nineteenth century was a great achievment and a testament to the power of complex analysis. More recently, Bombieri's development of the large sieve in the 1960s (see [3]) has led to many deep and interesting results. (Bombieri was awarded the Fields medal for his work.) As a testimony to the continued vibrancy of research in this area, one might note the number of first-rate mathematicians currently working in areas related to the field, including Sarnak, Granville, Friedlander, Green, Iwaniec, Soundararajan, Tao, Bourgain and Connes.

3 Recent Developments

Though Thue's original method of proof was "ineffective" as described above, it was clear that one could derive upper bounds for the *number* of exceptional solutions. This has carried through to Roth's theorem and the subspace theorem; versions of these results where one has such upper bounds are called quantitative. There has been much effort to make stronger quantitative versions of both Roth's theorem and the subspace theorem. Also, there have been quantitative versions involving other absolute values and even a "absolute" version [4] over the field of all algebraic numbers. In a similar manner, there are more recent versions of linear forms in logarithms which give better bounds [2], as well as linear forms in p-adic, elliptic and even hyperelliptic logarithms.

While the above efforts to improve on machinery is clearly fundamental, the majority of work in the area has been applying these tools to solving actual Diophantine equations and inequalities. One major topic here deals with S-unit equations, the simplest of which is just

$$a + b = 1$$

where a and b are S-units in a given number field (or perhaps a function field). Every number field (finite algebraic extension of the rational numbers) has a countable colletion of places which correspond to topologically inequivalent absolute values on the field. These places are in one-to-one correspondence with the embeddings of the field into the complex numbers (these are the "infinite" places") and the non-zero prime ideals in the ring of integers of the field. Given a finite set S of such places containing all of the infinite places, an S-integer is an element a of the field which has absolute value $|a|_v = 1$ for all places v not in S. It turns out that many Diophantine questions are equivalent to solving a particular S-unit equation or family of such.

In analytic number theory, work continues on using the machinery already on hand to answer deep questions about the primes and other sets of interest, as well as on applications of new techniques coming from additive combinatorics and the theory of automorphic forms. Progress is also being made on the methods themselves, where one often looks to optimize the techniques to suit the particular question at hand. An example here would be Vaughan and Wooley's improvements on the circle method to answer then-open questions regarding Waring's problem. In addition, work continues on the Riemann zeta function. The Riemann hypothesis is obviously the "holy grail" here, but more modest goals are still very important. Recent work of Soundararajan has increased our knowledge of the moments of the zeta function, for example.

4 Presentation Highlights

Yann Bugeaud of Strasbourg spoke on the irrationality exponent of a certain type of number. Given a real number α, the irrationality exponent of α is the infimum of the set of δ for which the inequality (*) above has infinitely many solutions in rational numbers p/q. Thus, by Roth's theorem the irrationality exponent of any algebraic number is simply 2. Computing the irrationality exponent of non-algebraic numbers is typically an extremely difficult task. Often we must be content trying simply to prove upper bounds for the irrationality exponent. This is the case, for example, with the number π (presently the best upper bound for its irrationality exponent is approximately 8, while it is generally thought that the actual irrationality exponent here is 2).

Bugeaud discussed α of the following form. Start with the Thue-Morse sequence $\{t_n\}_{n \geq 0}$ defined recursively by $t_0 = 0$, $t_{2n} = t_n$ and $t_{2n+1} = 1 - t_n$. Choose an integer $b \geq 2$. Bugeaud proved that the irrationality exponent of the number $\alpha = \sum_{n \geq 0} t_n b^{-n}$ is 2.

Jan-Hendrik Evertse of Leiden discussed orders of number fields which are generated (as modules over the integers) by a single element. Such orders are called "monogenic." When the order in question is the maximal order, i.e., the ring of integers of the field, one says there is a power basis if it is monogenic. This is usually not the case, but it is extremely useful when it is. If one has a monogenic order O of the form $Z[\alpha]$, then clearly $O = Z[\beta]$ for any β of the form $\beta = \pm\alpha + a$ for some $a \in Z$. We say such β are equivalent to α. Given a monogenic order O, one is interested in the number of inequivalent α which generate O. Evertse proved that for orders in number fields of degree at least 3, only finitely many can be monogenic with at least three inequivalent generators. Also, for non-CM fields, there are infinitely many monogenic orders with exactly two non-equivalent generators. The method of proof here relies on previous results dealing with S-unit equations in two variables.

Noriko Hirata-Kohno of Tokyo discussed Iwasawa p-adic logarithms and showed how one could use these in the p-adic linear forms in logarithms machinery. The goal here is to improve/extend the machinery to give better estimates and/or be more widely applicable.

Helmut Maier of Ulm spoke on exponential sums over prime numbers. He presented a conjecture for such sums over "short" intervals which is reasonably natural, and showed how this conjecture implies the twin prime conjecture. Further, he showed that an analogous conjecture is true when the set of prime numbers is replaced by a set of integers without small prime factors.

Two speakers, Andras Sárközy and Rob Tijdeman, spoke directly about the work of Cam Stewart. Both are frequent coauthors with Cam; Sárközy has written more than 15 papers with him.

Andras gave a history of his work with Cam on sums $a+b$ and shifted products $ab+1$. Given sufficiently large sets A and B, one is interested in the arithmetic properties of sums of the form $a+b$ where $a \in A$ and $b \in B$ and also of the form $ab+1$. Such questions go back all the way to Diophantus. By "arithmetic properties" here we mean questions about the prime factors, square factors, etc. Together with Cam, and occasionally other authors, Andras has proven many results in this area.

Rob's talk concentrated on Cam's work involving linear forms in logarithms. Cam's first paper appeared in the journal Acta Arithmetica in 1975. It dealt with the largest prime factor of sums of the form $a^n - b^n$. If we denote the largest such prime factor by P, then Cam proved that

$$\frac{P(a^n - b^n)}{n} \to \infty$$

as n tends to ∞ through some well-defined set of density 1. Stewart and Tijdeman together worked on the abc-conjecture. Suppose $a,\ b$ and c are positive integers with $a+b=c$. Denote their conductor by N; N is the product of all primes dividing abc. The abc-conjecture states that, for all $\epsilon > 0$, one has $N^{1+\epsilon} \gg_\epsilon c$, where the implicit constant in the Vinogradov notation here depends only on ϵ. In an important paper from 1985, Stewart and Tijdeman proved that $\log c \ll N^{15}$ and also that

$$c > N \exp\left((4-\delta)\frac{\sqrt{\log N}}{\log\log N}\right)$$

for infinitely many cases, where $\delta > 0$ is arbitrary. In particular, the ϵ in the abc-conjecture is necessary. Rob further spoke on Cam's work involving S-unit equations and Thue-Mahler equations.

References

[1] A. Baker, Linear forms in the logarithms of algebraic numbers I, II, III, *Mathematatika* **13** (1966), 204–216; ibid. **14** (1967) 102–107; ibid. 220–228.

[2] A. Baker and G. Wustholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993) 19–62.

[3] E. Bombieri, Le grand crible dans la théorie analytique des nombres, *Astérisque* **18** (1974) i+87 pp.

[4] J.-H. Evertse and H.-P. Schlickewei, A quantitative version of the absolute subspace theorem, *J. Reine Angew. Math.* **548** (2002) 21–127.

[5] K. F. Roth, Rational approximations to algebraic numbers, *Mathematika* **2** (1955) 1–20.

[6] W. M. Schmidt, Linear forms with algebraic coefficients I, *J. Number Theory* **3** 253-277.