International Journal of Research in Engineering, Science and Management
Volume-2, Issue-7, July-2019
www.ijresm.com | ISSN (Online): 2581-5792

Number Theory and its New Developments

Mohammod Noor[1], Venkata Srinivasa Rao Naralasetty[2]
[1,2]*Lecturer, Department of Mathematics, AG & SG Siddhratha Degree College, Vuyyuru, India*

***Abstract*: This paper presents an overview on number theory and its new developments.**

***Keywords*: number theory**

1. Introduction

Number theory (or arithmetic or higher arithmetic in older usage) is a branch of pure mathematics devoted primarily to the study of the integers. German mathematician Carl Friedrich Gauss (1777–1855) said, "Mathematics is the queen of the sciences-and number theory is the queen of mathematics." Number theorists study prime numbers as well as the properties of objects made out of integers (for example, rational numbers) or defined as generalizations of the integers (for example, algebraic integers).

Integers can be considered either in themselves or as solutions to equations (Diophantine geometry). Questions in number theory are often best understood through the study of analytical objects (for example, the Riemann zeta function) that encode properties of the integers, primes or other number-theoretic objects in some fashion (analytic number theory). One may also study real numbers in relation to rational numbers, for example, as approximated by the latter (Diophantine approximation).

The older term for number theory is arithmetic. By the early twentieth century, it had been superseded by "number theory". (The word "arithmetic" is used by the general public to mean "elementary calculations"; it has also acquired other meanings in mathematical logic, as in Peano arithmetic, and computer science, as in floating point arithmetic.) The use of the term arithmetic for number theory regained some ground in the second half of the 20th century, arguably in part due to French influence. In particular, arithmetical is preferred as an adjective to number-theoretic.

A. Dawn of arithmetic

The first historical find of an arithmetical nature is a fragment of a table: the broken clay tablet Plimpton 322 (Larsa, Mesopotamia, ca. 1800 BCE) contains a list of "Pythagorean triples", that is, integers such that . The triples are too many and too large to have been obtained by brute force. The heading over the first column reads: "The takiltum of the diagonal which has been subtracted such that the width..." The table's layout suggests that it was constructed by means of what amounts, in modern language, to the identity which is implicit in routine Old Babylonian exercises. If some other method was used, the triples were first constructed and then reordered by , presumably for actual use as a "table", for example, with a view to applications. It is not known what these applications may have been, or whether there could have been any; Babylonian astronomy, for example, truly came into its own only later. It has been suggested instead that the table was a source of numerical examples for school problems. While Babylonian number theory—or what survives of Babylonian mathematics that can be called thus—consists of this single, striking fragment, Babylonian algebra (in the secondary-school sense of "algebra") was exceptionally well developed. Late Neoplatonic sources state that Pythagoras learned mathematics from the Babylonians. Much earlier sources state that Thales and Pythagoras traveled and studied in Egypt.

Euclid IX 21–34 is very probably Pythagorean; it is very simple material ("odd times even is even", "if an odd number measures [= divides] an even number, then it also measures [= divides] half of it"), but it is all that is needed to prove that is irrational. Pythagorean mystics gave great importance to the odd and the even. The discovery that is irrational is credited to the early Pythagoreans (pre-Theodorus). By revealing (in modern terms) that numbers could be irrational, this discovery seems to have provoked the first foundational crisis in mathematical history; its proof or its divulgation are sometimes credited to Hippasus, who was expelled or split from the Pythagorean sect.

This forced a distinction between numbers (integers and the rationals-the subjects of arithmetic), on the one hand, and lengths and proportions (which we would identify with real numbers, whether rational or not), on the other hand.

The Pythagorean tradition spoke also of so called polygonal or figurate numbers. While square numbers, cubic numbers, etc., are seen now as more natural than triangular numbers, pentagonal numbers, etc., the study of the sums of triangular and pentagonal numbers would prove fruitful in the early modern period (17th to early 19th century).

We know of no clearly arithmetical material in ancient Egyptian or Vedic sources, though there is some algebra in both. The Chinese remainder theorem appears as an exercise in Sunzi Suanjing (3rd, 4th or 5th century CE.) (There is one important step glossed over in Sunzi's solution: it is the problem that was later solved by Āryabhaṭa's Kuṭṭaka

There is also some numerical mysticism in Chinese mathematics, but, unlike that of the Pythagoreans, it seems to have led nowhere. Like the Pythagoreans' perfect

numbers, magic squares have passed from superstition into recreation.

B. Classical Greece and the early Hellenistic period

Ancient Greek mathematics: Aside from a few fragments, the mathematics of Classical Greece is known to us either through the reports of contemporary non-mathematicians or through mathematical works from the early Hellenistic period. In the case of number theory, this means, by and large, Plato and Euclid, respectively. While Asian mathematics influenced Greek and Hellenistic learning, it seems to be the case that Greek mathematics is also an indigenous tradition.

Eusebius, PE X, chapter 4 mentions of Pythagoras: "In fact the said Pythagoras, while busily studying the wisdom of each nation, visited Babylon, and Egypt, and all Persia, being instructed by the Magi and the priests: and in addition to these he is related to have studied under the Brahmans (these are Indian philosophers); and from some he gathered astrology, from others geometry, and arithmetic and music from others, and different things from different nations, and only from the wise men of Greece did he get nothing, wedded as they were to a poverty and dearth of wisdom: so on the contrary he himself became the author of instruction to the Greeks in the learning which he had procured from abroad."

Aristotle claimed that the philosophy of Plato closely followed the teachings of the Pythagoreans, and Cicero repeats this claim: Platonem ferunt didicisse Pythagorea omnia("They say Plato learned all things Pythagorean").

Plato had a keen interest in mathematics, and distinguished clearly between arithmetic and calculation. (By arithmetic he meant, in part, theorizing on number, rather than what arithmetic or number theory have come to mean.) It is through one of Plato's dialogues—namely, Theaetetus—that we know that Theodorus had proven that are irrational. Theaetetus was, like Plato, a disciple of Theodorus's; he worked on distinguishing different kinds of incommensurables, and was thus arguably a pioneer in the study of number systems. (Book X of Euclid's Elements is described by Pappus as being largely based on Theaetetus's work.)

Euclid devoted part of his Elements to prime numbers and divisibility, topics that belong unambiguously to number theory and are basic to it (Books VII to IX of Euclid's Elements). In particular, he gave an algorithm for computing the greatest common divisor of two numbers (the Euclidean algorithm; Elements, Prop. VII.2) and the first known proof of the infinitude of primes (Elements, Prop. IX.20).

In 1773, Lessing published an epigram he had found in a manuscript during his work as a librarian; it claimed to be a letter sent by Archimedes to Eratosthenes. The epigram proposed what has become known as Archimedes's cattle problem; its solution (absent from the manuscript) requires solving an indeterminate quadratic equation (which reduces to what would later be misnamed Pell's equation). As far as we know, such equations were first successfully treated by the Indian school. It is not known whether Archimedes himself had a method of solution.

C. Diophantus

Very little is known about Diophantus of Alexandria; he probably lived in the third century CE, that is, about five hundred years after Euclid. Six out of the thirteen books of Diophantus's Arithmetica survive in the original Greek; four more books survive in an Arabic translation. The Arithmetica is a collection of worked-out problems where the task is invariably to find rational solutions to a system of polynomial equations, usually of the form or Thus, nowadays, we speak of Diophantine equations when we speak of polynomial equations to which rational or integer solutions must be found.

One may say that Diophantus was studying rational points, that is, points whose coordinates are rational—on curves and algebraic varieties; however, unlike the Greeks of the Classical period, who did what we would now call basic algebra in geometrical terms, Diophantus did what we would now call basic algebraic geometry in purely algebraic terms. In modern language, what Diophantus did was to find rational parametrizations of varieties; that is, given an equation of the form (say) , his aim was to find (in essence) three rational functions such that, for all values of and , setting for gives a solution to Diophantus also studied the equations of some non-rational curves, for which no rational parametrisation is possible. He managed to find some rational points on these curves (elliptic curves, as it happens, in what seems to be their first known occurrence) by means of what amounts to a tangent construction: translated into coordinate geometry (which did not exist in Diophantus's time), his method would be visualised as drawing a tangent to a curve at a known rational point, and then finding the other point of intersection of the tangent with the curve; that other point is a new rational point. (Diophantus also resorted to what could be called a special case of a secant construction.)

While Diophantus was concerned largely with rational solutions, he assumed some results on integer numbers, in particular that every integer is the sum of four squares (though he never stated as much explicitly).

D. Āryabhaṭa, Brahmagupta, Bhāskara

While Greek astronomy probably influenced Indian learning, to the point of introducing trigonometry, it seems to be the case that Indian mathematics is otherwise an indigenous tradition; in particular, there is no evidence that Euclid's Elements reached India before the 18th century. Āryabhaṭa (476–550 CE) showed that pairs of simultaneous congruences , could be solved by a method he called kuṭṭaka, or pulveriser; this is a procedure close to (a generalisation of) the Euclidean algorithm, which was probably discovered independently in India. Āryabhaṭa seems to have had in mind applications to astronomical calculations.

Brahmagupta (628 CE) started the systematic study of indefinite quadratic equations—in particular, the

misnamed Pell equation, in which Archimedes may have first been interested, and which did not start to be solved in the West until the time of Fermat and Euler. Later Sanskrit authors would follow, using Brahmagupta's technical terminology. A general procedure (the chakravala, or "cyclic method") for solving Pell's equation was finally found by Jayadeva (cited in the eleventh century; his work is otherwise lost); the earliest surviving exposition appears in Bhāskara II's Bīja-gaṇita (twelfth century). Indian mathematics remained largely unknown in Europe until the late eighteenth century; Brahmagupta and Bhāskara's work was translated into English in 1817 by Henry Colebrooke.

E. Arithmetic in the Islamic golden age

Mathematics in medieval Islam: Al-Haytham seen by the West: frontispice of Selenographia, showing Alhasen representing knowledge through reason, and Galileo representing knowledge through the senses.

In the early ninth century, the caliph Al-Ma'mun ordered translations of many Greek mathematical works and at least one Sanskrit work (the Sindhind, which may or may not be Brahmagupta's Brāhmasphuṭasiddhānta). Diophantus's main work, the Arithmetica, was translated into Arabic by Qusta ibn Luqa (820–912). Part of the treatise al-Fakhri (by al-Karajī, 953 – ca. 1029) builds on it to some extent. According to Rashed Roshdi, Al-Karajī's contemporary Ibn al-Haytham knew what would later be called Wilson's theorem.

F. Western Europe in the middle ages

Other than a treatise on squares in arithmetic progression by Fibonacci—who traveled and studied in North Africa and Constantinople—no number theory to speak of was done in western Europe during the Middle Ages. Matters started to change in Europe in the late Renaissance, thanks to a renewed study of the works of Greek antiquity.

A catalyst was the textual emendation and translation into Latin of Diophantus' Arithmetica.

G. Early modern number theory

Pierre de Fermat (1607–1665) never published his writings; in particular, his work on number theory is contained almost entirely in letters to mathematicians and in private marginal notes. He wrote down nearly no proofs in number theory; he had no models in the area. One of Fermat's first interests was perfect numbers (which appear in Euclid, Elements IX) and amicable numbers; these topics led him to work on integer divisors, which were from the beginning among the subjects of the correspondence (1636 onwards) that put him in touch with the mathematical community of the day.

Fermat's work in arithmetic includes the following.

- Fermat's little theorem (1640), stating that, if a is not divisible by a prime p, then
- If a and b are co-prime, then is not divisible by any prime congruent to −1 modulo 4; and every prime congruent to 1 modulo 4 can be written in the form . These two statements also date from 1640; in 1659, Fermat stated to Huygens that he had proven the latter statement by the method of infinite descent.
- Fermat posed the problem of solving as a challenge to English mathematicians (1657). The problem was solved in a few months by Wallis and Brouncker. Fermat considered their solution valid, but pointed out they had provided an algorithm without a proof (as had Jayadeva and Bhaskara, though Fermat would never know this). He states that a proof can be found by descent.
- Fermat states and proves (by descent) in the appendix to Observations on Diophantus (Obs. XLV) that has no non-trivial solutions in the integers. Fermat also mentioned to his correspondents that has no non-trivial solutions, and that this could be proven by descent. The first known proof is due to Euler (1753; indeed by descent). Fermat's claim ("Fermat's last theorem") to have shown there are no solutions to for all appears only in his annotations on the margin of his copy of Diophantus.

H. Euler

The interest of Leonhard Euler (1707–1783) in number theory was first spurred in 1729, when a friend of his, the amateur Goldbach, pointed him towards some of Fermat's work on the subject. This has been called the "rebirth" of modern number theory, after Fermat's relative lack of success in getting his contemporaries' attention for the subject. Euler's work on number theory includes the following:

- Proofs for Fermat's statements. This includes Fermat's little theorem (generalized by Euler to non-prime moduli); the fact that if and only if ; initial work towards a proof that every integer is the sum of four squares (the first complete proof is by Joseph-Louis Lagrange (1770), soon improved by Euler himself); the lack of non-zero integer solutions to (implying the case n=4 of Fermat's last theorem, the case n=3 of which Euler also proved by a related method).
- Pell's equation, first misnamed by Euler. He wrote on the link between continued fractions and Pell's equation.
- First steps towards analytic number theory. In his work of sums of four squares, partitions, pentagonal numbers, and the distribution of prime numbers, Euler pioneered the use of what can be seen as analysis (in particular, infinite series) in number theory. Since he lived before the development of complex analysis, most of his work is restricted to the formal manipulation of power series. He did, however, do some very notable (though not fully rigorous) early work on what would later be called the Riemann zeta function.
- Quadratic forms. Following Fermat's lead, Euler did

further research on the question of which primes can be expressed in the form , some of it prefiguring quadratic reciprocity.

- Diophantine equations. Euler worked on some Diophantine equations of genus 0 and 1. In particular, he studied Diophantus's work; he tried to systematize it, but the time was not yet ripe for such an endeavour—algebraic geometry was still in its infancy. He did notice there was a connection between Diophantine problems and elliptic integrals, whose study he had himself initiated.

I. Lagrange, Legendre, and Gauss

Joseph-Louis Lagrange (1736–1813) was the first to give full proofs of some of Fermat's and Euler's work and observations—for instance, the four-square theorem and the basic theory of the misnamed "Pell's equation" (for which an algorithmic solution was found by Fermat and his contemporaries, and also by Jayadeva and Bhaskara II before them.) He also studied quadratic forms in full generality (as opposed to)—defining their equivalence relation, showing how to put them in reduced form, etc.

Adrien-Marie Legendre (1752–1833) was the first to state the law of quadratic reciprocity. He also conjectured what amounts to the prime number theorem and Dirichlet's theorem on arithmetic progressions. He gave a full treatment of the equation and worked on quadratic forms along the lines later developed fully by Gauss. In his old age, he was the first to prove "Fermat's last theorem" for (completing work by Peter Gustav Lejeune Dirichlet, and crediting both him and Sophie Germain).

J. Maturity and division into subfields

Starting early in the nineteenth century, the following developments gradually took place:

- The rise to self-consciousness of number theory (or higher arithmetic) as a field of study.
- The development of much of modern mathematics necessary for basic modern number theory: complex analysis, group theory, Galois Theory—accompanied by greater rigor in analysis and abstraction in algebra.
- The rough subdivision of number theory into its modern subfields—in particular, analytic and algebraic number theory.

Algebraic number theory may be said to start with the study of reciprocity and cyclotomy, but truly came into its own with the development of abstract algebra and early ideal theory and valuation theory; see below. A conventional starting point for analytic number theory is Dirichlet's theorem on arithmetic progressions (1837), whose proof introduced L-functions and involved some asymptotic analysis and a limiting process on a real variable. The first use of analytic ideas in number theory actually goes back to Euler (1730s), who used formal power series and non-rigorous (or implicit) limiting arguments. The use of complex analysis in number theory comes later: the work of Bernhard Riemann (1859) on the zeta function is the canonical starting point; Jacobi's four-square theorem (1839), which predates it, belongs to an initially different strand that has by now taken a leading role in analytic number theory (modular forms). The history of each subfield is briefly addressed in its own section below; see the main article of each subfield for fuller treatments. Many of the most interesting questions in each area remain open and are being actively worked on.

- Main subdivisions
- Elementary tools

The term elementary generally denotes a method that does not use complex analysis. For example, the prime number theorem was first proven using complex analysis in 1896, but an elementary proof was found only in 1949 by Erdős and Selberg. The term is somewhat ambiguous: for example, proofs based on complex Tauberian theorems (for example, Wiener–Ikehara) are often seen as quite enlightening but not elementary, in spite of using Fourier analysis, rather than complex analysis as such. Here as elsewhere, an elementaryproof may be longer and more difficult for most readers than a non-elementary one.

Number theory has the reputation of being a field many of whose results can be stated to the layperson. At the same time, the proofs of these results are not particularly accessible, in part because the range of tools they use is, if anything, unusually broad within mathematics.[76]

K. Analytic number theory

Riemann zeta function ζ(s) in the complex plane. The color of a points gives the value of ζ(s): dark colors denote values close to zero and hue gives the value's argument. The action of the modular group on the upper half plane. The region in grey is the standard fundamental domain.

Analytic number theory may be defined

- In terms of its tools, as the study of the integers by means of tools from real and complex analysis; or
- In terms of its concerns, as the study within number theory of estimates on size and density, as opposed to identities.

Some subjects generally considered to be part of analytic number theory, for example, sieve theory, are better covered by the second rather than the first definition: some of sieve theory, for instance, uses little analysis, yet it does belong to analytic number theory.

The following are examples of problems in analytic number theory: the prime number theorem, the Goldbach conjecture (or the twin prime conjecture, or the Hardy–Littlewood conjectures), the Waring problem and the Riemann hypothesis. Some of the most important tools of analytic number theory are the circle method, sieve methods and L-functions (or, rather, the study of their properties). The theory of modular forms (and, more generally, automorphic forms) also occupies an increasingly central place in the toolbox of analytic number theory.

One may ask analytic questions about algebraic numbers, and use analytic means to answer such questions; it is thus that algebraic and analytic number theory intersect. For example, one may define prime ideals (generalizations of prime numbers in the field of algebraic numbers) and ask how many prime ideals there are up to a certain size. This question can be answered by means of an examination of Dedekind zeta functions, which are generalizations of the Riemann zeta function, a key analytic object at the roots of the subject.[79] This is an example of a general procedure in analytic number theory: deriving information about the distribution of a sequence (here, prime ideals or prime numbers) from the analytic behavior of an appropriately constructed complex-valued function.

L. Algebraic number theory

An algebraic number is any complex number that is a solution to some polynomial equation with rational coefficients; for example, every solution of (say) is an algebraic number. Fields of algebraic numbers are also called algebraic number fields, or shortly number fields. Algebraic number theory studies algebraic number fields. Thus, analytic and algebraic number theory can and do overlap: the former is defined by its methods, the latter by its objects of study.

It could be argued that the simplest kind of number fields (viz., quadratic fields) were already studied by Gauss, as the discussion of quadratic forms in Disquisitiones arithmeticae can be restated in terms of ideals and norms in quadratic fields. (A quadratic field consists of all numbers of the form , where and are rational numbers and is a fixed rational number whose square root is not rational.) For that matter, the 11th-century chakravala method amounts—in modern terms—to an algorithm for finding the units of a real quadratic number field. However, neither Bhāskara nor Gauss knew of number fields as such.

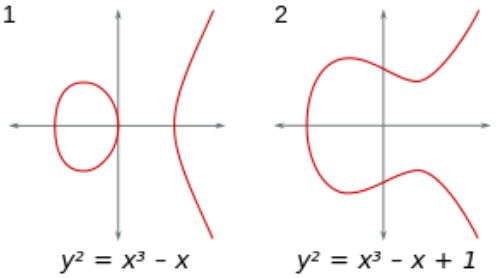
The grounds of the subject as we know it were set in the late nineteenth century, when ideal numbers, the theory of ideals and valuation theory were developed; these are three complementary ways of dealing with the lack of unique factorisation in algebraic number fields. (For example, in the field generated by the rationals and, the number can be factorised both as and all of and are irreducible, and thus, in a naïve sense, analogous to primes among the integers.) The initial impetus for the development of ideal numbers (by Kummer) seems to have come from the study of higher reciprocity laws, that is, generalizations of quadratic reciprocity.

M. Diophantine geometry

The central problem of Diophantine geometry is to determine when a Diophantine equation has solutions, and if it does, how many. The approach taken is to think of the solutions of an equation as a geometric object.

For example, an equation in two variables defines a curve in the plane. More generally, an equation, or system of equations, in two or more variables defines a curve, a surface or some other such object in n-dimensional space. In Diophantine geometry, one asks whether there are any rational points (points all of whose coordinates are rationals) or integral points (points all of whose coordinates are integers) on the curve or surface. If there are any such points, the next step is to ask how many there are and how they are distributed. A basic question in this direction is: are there finitely or infinitely many rational points on a given curve (or surface)? What about integer points?

An example here may be helpful. Consider the Pythagorean equation ; we would like to study its rational solutions, that is, its solutions such that x and y are both rational. This is the same as asking for all integer solutions to ; any solution to the latter equation gives us a solution , to the former. It is also the same as asking for all points with rational coordinates on the curve described by . (This curve happens to be a circle of radius 1 around the origin.)



Two examples of an elliptic curve, that is, a curve of genus 1 having at least one rational point. (Either graph can be seen as a slice of a torus in four-dimensional space.)The rephrasing of questions on equations in terms of points on curves turns out to be felicitous. The finiteness or not of the number of rational or integer points on an algebraic curve—that is, rational or integer solutions to an equation , where is a polynomial in two variables—turns out to depend crucially on the genus of the curve.

2. Some recent developments in number theory

M. Ram Murty In 1916, Srinivasa Aiyangar Ramanujan wrote two seminal papers that have shaped the development of modern number theory. The first paper modestly entitled, “On certain arithmetical functions,” dealt with his celebrated τ - function and conjectures relating to it as well as numerous unexplained congruences that emerged from his work. The second paper entitled “On the expression of a number in the form ax2 + by2 + cz2 + du2” determined all natural numbers a, b, c, d for which the quadratic form ax2+by2+cz2+du2 represents all natural numbers. He gave a complete list which included (a, b, c, d) = (1, 1, 1, 1) that corresponds to the celebrated theorem of Lagrange that every natural number can be written as a sum of four squares.

In our brief survey of some recent developments in number theory, we will describe how these two papers gave birth to two lines of development, one in the theory of quadratic forms, and the other in the theory of Galois representations, both of which

are now central themes in modern number theory. We begin with the second paper first. Quadratic forms Ramanujan's paper addresses a special case of a more general question: which positive definite quadratic forms with integral coefficients represent all natural numbers? Given a quadratic form Q(x), we can write it as a matrix equation x tAx with A a symmetric matrix. In 1993, Conway and Schneeberger proved a surprising theorem: suppose that A is positive definite with integer entries. If the associated quadratic form represents all natural numbers up to 15, then it represents all natural numbers. The original proof was complicated and never published.

In 2000, Manjul Bhargava published a much simpler proof. Conway conjectured that if we consider integer valued quadratic forms (instead of A being integral), then a similar result should hold with 15 replaced by 290. In 2005, Manjul Bhargava and Jonathan Hanke announced a proof of this conjecture. Their work will soon be published in Inventiones Math. If we turn our attention to indefinite quadratic forms, then a theorem of A. Meyer proved in 1884 asserts that any indefinite form Q with rational coefficients in n variables (n ≥ 5) represents zero non-trivially. In other words, there is a non-zero integral vector x such that Q(x) = 0. It is the best possible theorem in terms of the number of variables since the example Q(x1, x2, x3, x4) = x 2 1 + x 2 2 − p(x 2 3 + x 2 4) with p a prime congruent to 3 (mod 4) shows that Q(x) = 0 implies x = 0. Indeed, if there were a solution, then reducing (mod p) shows that x 2 1 ≡ −x 2 2 (mod p). If x2 is not divisible by p, then we deduce that −1 is a square (mod p), a contradiction.

Thus x2 is divisible by p and a fortiori, 1 some recent developments in number theory. Math. Newsl. 19 (2010), Sp. Number 1, 175–182. Published on the occasion of the International Congress of Mathematicians held at Hyderabad, India. x1 is divisible by p. Similarly, one deduces that x3 and x4 are divisible by p. Thus, by a descent argument, we see that x = 0. If we put m(Q) = inf{Q(x) : x ∈ Z n , x 6= 0}, then Meyer's theorem is equivalent to m(Q) = 0 for any (non-degenerate) indefinite quadratic form which is a multiple of a form with rational coefficients for n ≥ 5. If we consider a real (non-degenerate) indefinite quadratic form Q which is not a multiple of a rational form, then Alexander Oppenheim conjectured in 1929 that m(Q) = 0 for n ≥ 5. It was later noted by Davenport and Heilbronn that the conjecture should hold for n ≥ 3. Building on the 1934 work of Sarvadaman Chowla Davenport wrote a series of papers with Birch, Heilbronn, Lewis and Ridout attacking the Oppenheim conjecture with the main tool being the circle method of Ramanujan. In this way, it was shown that Oppenheim's conjecture is true for n ≥ 21. In the 1970's, M.S. Raghunathan gave a reformulation of the Oppenheim conjecture in terms of homogeneous group actions. Armed with this new perspective on an old conjecture, Margulis resolved the matter in 1986 using a combination of methods from Lie theory, ergodic theory and number theory. We refer the reader to his highly readable exposition. In the subsequent years, Marina Ratner, motivated by conjectures of Raghunathan, proved in 1990 a major theorem concerning unipotent flows on homogeneous spaces. Once this theorem is available, Oppenheim's conjecture can be deduced without too much difficulty.

We will give a short description of how this is done. If V is a vector space over a field k and f is a bilinear form on V , we denote by O(f) the elements of GL(V) which preserve the form. In our context, the matrix A associated with the quadratic form Q gives rise to a bilinear form and we can consider the group of transformations H such that Q(hx) = Q(x) for all h ∈ H. Thus, to prove the Oppenheim conjecture, it suffices to show that for any > 0, Q takes values in [−,] at a point of the form hx with x 6= 0, h ∈ H and x ∈ Z n . For instance, if we can show that {hx : h ∈ H, x ∈ Z n , x 6= 0} contains zero in its closure, then the Oppenheim conjecture follows. The advantage of this perspective is that we have moved from the standard lattice, namely Z n to the H-orbits of the standard lattice. This viewpoint slowly allows us to translate the problem into a problem of homogeneous spaces. A lattice in R n is the set of Z-linear combinations of n linearly independent vectors. It is not hard to see that every lattice is of the form gZ n for some g ∈ GLn(R). Let Ln be the set of lattices in R n and let Ln() be the set of lattices that contain v ∈ R n with ||v|| < . The lattice Z n can be thought of as a point of Ln. The Oppenheim conjecture would follow if we can show the H-orbit of Z n intersects non-trivially with Ln(), which is a dynamical reformulation of the conjecture. To any lattice, we can associate an element X of GLn(R) simply by taking the 2 basis of the lattice for its columns. It is not hard to see that X and X0 give rise to the same lattice if and only if X0 = AX for A ∈ GLn(Z). Thus, the space of lattices can be identified with the coset space GLn(R)/GLn(Z). Since all the elements of O(f) have determinant 1, it is more convenient to move to the coset space Kn = SLn(R)/SLn(Z).

These coset spaces inherit topologies from SLn(R) and GLn(R) and can be given the structure of manifolds. Our interest now is to consider how the H orbit of Z n sits in this homogeneous space. A famous criterion of Mahler says that a subset K of Kn is bounded if it does not intersect K() = L() ∩ Kn. In other words, our goal is to show that the orbit H[Z n] is unbounded in Kn. An essential feature here is that we are dealing with n ≥ 3 and that our form is indefinite, not commensurate with a rational form. This means that H contains unipotent elements (that is, elements of SLn(R) for which all eigenvalues are 1). Now we can explain Ratner's theorem and how the Oppenheim conjecture can be deduced from it. Let H ⊂ SLn(R) be generated by one-parameter unipotent subgroups. Very briefly, Ratner's theorem is that the closure of the orbit of H[Z n] inside Kn is of the form H0 [Z n] for a closed subgroup H0 ⊇ H. Moreover, there exists an H0 -invariant probability measure on H0 [Z n].

Now the group H = SO(f) is maximal inside SLn(R). So Ratner's theorem implies that H[Z n] is closed or dense in Kn. The former possibility can occur only if Q is a multiple of a

rational form, which it isn't. Thus, the orbit is dense, and this completes the proof of the Oppenheim conjecture. (Note that we have proved something stronger than the conjecture.) A readable and more detailed exposition can be found in Venkatesh's paper [30]. Refinements of Ratner's theorems have found applications in other questions of number theory such as in the work of Vatsal [29] settling a conjecture of Mazur in the theory of elliptic curves. Higher degree forms The results on the Oppenheim conjecture expand our understanding of quadratic forms and the values they assume at integer lattice points. The situation is not the same when we move to cubic forms or higher degree forms. Binary quadratic forms are the easiest to study.

They have a long and venerable history. Already in the work of Brahmagupta in sixth century (C.E.) India, we find the equation (x 2 1 − dy2 1)(x 2 2 − dy2 2) = (x1x2 + dy1y2) 2 − d(x1y2 + x2y1) 2 which is an example of a "composition law." In the 1801 work Disquisitiones Arithmeticae of Gauss, we find the complete generalization of this in the form (a1x 2 1 + b1x1y1 + c1y 2 1)(a2x 2 2 + b2x2y2 + c2y 2 2) = AX2 + BXY + CY 2 , where X, Y are linear functions of x1x2, x1y2, y1x2, y1y2 and A, B, C are determined as functions 3 of a1, b1, c1, a2, b2, c2. This is the celebrated law of composition of binary quadratic forms. For binary quadratic forms ax2+bxy+cy2 with discriminant b 2−4ac fixed, Gauss's composition law serves to establish a one-to-one correspondence between ideal classes of the quadratic number field with discriminant D and binary quadratic forms of discriminant D.

This correspondence allows us to define a group law on the set of binary quadratic forms of a fixed discriminant. This is the essence of Gauss's theorem. If we identify the binary quadratic form ax2 + bxy + cy2 with the integer triple [a, b, c] as a lattice point in R 3 , then Gauss's theorem is that certain lattice points may be put in one-to-one correspondence with quadratic number fields and their ideal class groups. Viewed in this way, it is natural to ask if there are other lattice points in higher dimensional Euclidean spaces that could be made to correspond in a "natural way" to higher degree number fields and their ideal class groups. In 1964, Delone and Fadeev, building on earlier work of Hermite discovered a non-trivial lattice correspondence betweeen integral binary cubic forms and cubic rings. It is precisely this question that is addressed in the Princeton doctoral thesis of Manjul Bhargava.

In particular, Bhargava finds new composition laws that allow one to study ideal class groups of quartic and quintic extensions. This work has applications to a folklore conjecture regarding the enumeration of algebraic number fields with absolute discriminant below a given bound. This conjecture predicts that the number of algebraic number fields K/Q with [K : Q] = n and Galois closure Ke satisfying Gal(K/ e Q) ' Sn and discriminant dK satisfying |dK| ≤ X is asymptotically cnX as x tends to infinity. For n = 2, this is an easy exercise. For n = 3, it follows from the work of Davenport and Heilbronn. The cases n = 4 and 5 were recently completed by Bhargava [4] [5]. A good exposition of this work can be found in the Seminaire Bourbaki article.

The re-interpretation of questions concerning indefinite quadratic forms allowed us to use the recent advances in the ergodic theory. There is another celebrated conjecture formulated in 1930 by Littlewood that also can be reformulated in dynamical terms. Littlewood conjectured that for any α, β, we have lim inf n→∞ n||nα||||nβ|| = 0. Another way to say this is that for any > 0, the inequality |x(xα − y)(xβ − z)| < can be solved with x 6= 0 and x, y, z integers.

The function L(x, y, z) = x(xα − y)(xβ − z) is a product of three linear forms which admits a two-dimensional torus as a group of automorphisms. This conjecture has received considerable attention recently simply because it fits into this dynamical framework and one feels that the new methods of ergodic theory and Lie theory 4 should resolve the conjecture. Indeed, in a recent paper, Einsiedler, Katok and Lindenstrauss showed that the set of exceptions to Littlewood's conjecture has Hausdorff dimension zero. Galois representations and Serre's conjecture Let us now turn to the other paper of Ramanujan written in 1916 concerning the τ -function.

Ramanujan found many interesting congruences for it. For example, τ (n) ≡ σ11(n)(mod 691), where σ11(n) denotes the sum of the 11-th powers of the positive divisors of n. Similar congruences were found by Ramanujan for the modulus 2, 3, 5, 7, and 23. To explain the mystery of these congruences, Serre suggested the existence of an `-adic representation ρ` : Gal(Q/Q) → GL2(F`) such that if Frobp denotes the Frobenius automorphism, then ρ`(Frobp) has trace τ (p) and determinant p 11 (mod `).

Such a representation was discovered by Deligne (in the context of his work on the Weil conjectures and Ramanujan's conjecture). Serre and Swinnerton-Dyer studied this representation and noted that the special congruences arise from the "ramification" of this representation. These results inspired Serre to ask if the converse holds. That is, does every such representation "arise" from some modular form? To be precise, suppose that ρ: Gal(Q/Q) → GL2(F`) is a continuous homomorphism such that ρ is simple (that is, there is no basis in which the image of ρ is upper triangular). If ρ is odd (that is ρ(complex conjugation)= −1) and unramified at all primes unequal to `, is there a modular form f (of level 1 and weight k) such that the trace of ρ(Frobp) is equal to af (p) (the p-th Fourier coefficient of f) and its determinant is p k−1 (mod `)? Serre conjectured that the answer is "yes" and this is usually referred to as the level one case of Serre's conjecture. In 2006, Chandrasekhar Khare proved this level one case. Serre also formulated a higher "level" analogue of his conjecture and this was recently settled by Khare and Wintenberge.

An interesting application of this work that has a "popular appeal" is to Fermat's Last Theorem. The long and complicated proof of Ribet, Taylor and Wiles is now replaced with a relatively "shorter proof." In fact, all of the conjectural applications given in Serre's paper are now theorems. Even

more astounding about Khare's work is its application to Artin L-series attached to odd two-dimensional complex linear representations of the absolute Galois group over Q. 5 These non-abelian L-series generalize the classical Riemann ζ-function and the Dirichlet Lfunctions to the non-abelian Galois setting.

Artin conjectured that each of his non-abelian Lseries attached to an irreducible representation ρ extends to an entire function. One of the principal goals of the program of Langlands is to prove Artin's conjecture. Indeed, if the image of ρ is a finite solvable group of GL2(C), then Langlands [18] and Tunnell proved Artin's conjecture using the full theory of the Langlands program for GL2. This was the starting point of Wiles's celebrated proof of Fermat's Last Theorem. As a consequence of his work on Serre's conjecture, Khare was able to show the full Artin conjecture for all odd 2-dimensional representations. One can view this as a 2-dimensional version of the classical Artin reciprocity law (which includeds the well-known law of quadratic reciprocity). The study of Galois representations and their properties has led to other advances in number theory and this short survey cannot do justice to these new results. The most notable among these is the resolution of the Sato-Tate conjecture in the theory of elliptic curves due to Clozel, Harris, Shepherd-Baron and Taylor. A short survey of this work along with a generalization related to the Chebotarev density theorem can be found in.

The theory of modular forms is a special case of the larger universe of automorphic representations and the Langlands program. Central to this program is the fundamental lemma or the "fundamental matching conjecture" recently proved by Ngo. Surely this work will have significant consequences for the theory of L-function in the coming years. Other developments and future directions We have not been able to discuss the recent advances in additive combinatorics, especially the work of Green and Tao.

Their theorem is quite elementary to state. It is that the sequence of prime numbers contains arbitrarily long arithmetic progressions. That is, for every natural number k, there is a k-term arithmetic progression of primes. Here again, the new ideas consist of a combination of methods from analytic number theory and ergodic theory. What is interesting in this work is the use of some classical techniques from analytic number theory involving truncted von Mangoldt functions: ΛR(n) := X d|n,d≤R μ(d) log(R/d), where μ denotes the Mobius function. These functions also appear in work of Goldston, Pintz ¨ and Yildirim who showed that lim inf n→∞ pn+1 − pn log pn = 0, which was a famous conjecture for a long time. 6 Another important theme inspired by quantum mechanics and number theory is the quantum unique ergodicity conjecture. In a special case, this conjecture states that if f(z) is a holomorphic cuspidal Hecke eigenform of weight k (like Δ(z), with k = 12 for example) then for any smooth bounded function in the fundamental domain D for the standard action of SL2(Z) on the upper half-plane, we have lim k→∞ Z D y k |f(z)| 2 g(z) dxdy y 2 → Z D g(z) dxdy y 2 .

This conjecture was recently proved by Holowinsky and Soundararajan . A nice corollary of this result is that the zeros of holomorphic Hecke eigenforms become equidistributed in the fundamental domain as the weight tends to infinity. An essential ingredient in their proof is the recurrent theme of "breaking convexity" in the theory of L-functions. The analog of this conjecture for Maass forms (which form the non-holomorphic counterpart of the theory of classical modular forms) is that if f(z) is a Maass form which is an eigenfunction for all the Hecke operators as well as the non-Euclidean Laplacian, (with corresponding eigenvalue λ) then for any smooth g(z), Z D |f(z)| 2 g(z) dxdy y 2 → Z D g(z) dxdy y 2 as λ → ∞. Lindenstrauss proved using ergodic methods that the limit is as expected, upto a scalar factor of some constant c with 0 ≤ c ≤ 1. Recently, Soundararajan showed that c = 1.

These are some of the highlights in number theory in the recent decades. Surely, it is impossible to faithfully record all of the accomplishments. However, we hope that in this short survey, we have been able to give some flavour of the developments that have emerged in the recent past and some that are yet to come. Acknowledgements. I would like to thank Sanoli Gun, Kumar Murty and Purusottam Rath for their comments on an earlier version of this article. References K. Belabas, Parametrisation de structure alg ´ ebriques et densit ´ e de discriminants, ´ Sem. Bourbabki, 56eme ann ` ee, 2003-2004, no. 935. M. Bhargava, On the Conway-Schneeberger theorem, in Quadratic Forms and Their Applications, (Dublin, 1999), 27-37, Contemporary Math., 272, American Math. Society, Providence, RI. 2000. 7 M. Bhargava, Higher Composition Laws I: A new view on Gauss composition and quadratic generalizations, Annals of Math., 159 (1) (2004), 217-250; Higher Composition Laws II: On cubic analogues of Gauss composition, Annals of Math., 159 (2) (2004), 865-886; Higher Composition Laws III: The parametrization of quartic rings, Annals of Math., 159 (3) (2004), 1329-1360; Higher Composition Laws IV: The parametrization of quintic rings, Annals of Math., 167 (2) (2008), 53-94.

3. Conclusion

This paper presented an overview on number theory and its new developments.

References

[1] Neugebauer & Sachs 1945, p. 40. The term takiltum is problematic. Robson prefers the rendering "The holding-square of the diagonal from which 1 is torn out, so that the short side comes up...". Robson 2001, p. 192.
[2] Robson 2001, p. 189. Other sources give the modern formula. Van der Waerden gives both the modern formula and what amounts to the form preferred by Robson.(van der Waerden 1961, p. 79)
[3] van der Waerden 1961, p. 184.
[4] Neugebauer (Neugebauer 1969, pp. 36–40) discusses the table in detail and mentions in passing Euclid's method in modern notation (Neugebauer 1969, p. 39).
[5] Friberg 1981, p. 302.
[6] van der Waerden 1961, p. 43.

[7] Iamblichus, Life of Pythagoras, (trans., for example, Guthrie 1987) cited in van der Waerden 1961, p. 108. See also Porphyry, Life of Pythagoras, paragraph 6, in Guthrie 1987Van der Waerden (van der Waerden 1961, pp. 87–90) sustains the view that Thales knew Babylonian mathematics.
[8] Herodotus (II. 81) and Isocrates (Busiris 28), cited in: Huffman 2011. On Thales, see Eudemus ap. Proclus, 65.7, (for example, Morrow 1992, p. 52) cited in: O'Grady 2004, p. 1. Proclus was using a work by Eudemus of Rhodes (now lost), the Catalogue of Geometers. See also introduction, Morrow 1992, p. xxx on Proclus's reliability.
[9] Becker 1936, p. 533, cited in: van der Waerden 1961, p. 108.
[10] Becker 1936.
[11] van der Waerden 1961, p. 109.
[12] Plato, Theaetetus, p. 147 B, (for example, Jowett 1871), cited in von Fritz 2004, p. 212: "Theodorus was writing out for us something about roots, such as the roots of three or five, showing that they are incommensurable by the unit;..." See also Spiral of Theodorus.
[13] von Fritz 2004.
[14] Heath 1921, p. 76.
[15] Sunzi Suanjing, Chapter 3, Problem 26. This can be found in Lam & Ang 2004, pp. 219–20, which contains a full translation of the Suan Ching (based on Qian 1963). See also the discussion in Lam & Ang 2004, pp. 138–140.
[16] The date of the text has been narrowed down to 220–420 CE (Yan Dunjie) or 280–473 CE (Wang Ling) through internal evidence (= taxation systems assumed in the text). See Lam & Ang 2004, pp. 27–28.
[17] Boyer & Merzbach 1991, p. 82.
[18] "Eusebius of Caesarea: Praeparatio Evangelica (Preparation for the Gospel). Tr. E.H. Gifford (1903) – Book 10".
[19] Metaphysics, 1.6.1 (987a)
[20] Tusc. Disput. 1.17.39.
[21] Vardi 1998, pp. 305–19.
[22] Weil 1984, pp. 17–24.
[23] Jump up to:a b Plofker 2008, p. 119.
[24] Any early contact between Babylonian and Indian mathematics remains conjectural (Plofker 2008, p. 42).
[25] Mumford 2010, p. 387.
[26] Āryabhaṭa, Āryabhatīya, Chapter 2, verses 32–33, cited in: Plofker 2008, pp. 134–40. See also Clark 1930, pp. 42–50. A slightly more explicit description of the kuṭṭaka was later given in Brahmagupta, Brāhmasphuṭasiddhānta, XVIII, 3–5 (in Colebrooke 1817, p. 325, cited in Clark 1930, p. 42).
[27] Mumford 2010, p. 388.
[28] Plofker 2008, p. 194.
[29] Plofker 2008, p. 283.
[30] Colebrooke 1817.
[31] Colebrooke 1817, p. lxv, cited in Hopkins 1990, p. 302. See also the preface in Sachau 1888 cited in Smith 1958, pp. 168
[32] Pingree 1968, pp. 97–125, and Pingree 1970, pp. 103–23, cited in Plofker 2008, p. 256.
[33] Rashed 1980, pp. 305–21.
[34] Bachet, 1621, following a first attempt by Xylander, 1575
[35] Weil 1984, pp. 45–46.
[36] Weil 1984, p. 118. This was more so in number theory than in other areas (remark in Mahoney 1994, p. 284). Bachet's own proofs were "ludicrously clumsy" (Weil 1984, p. 33).
[37] Mahoney 1994, pp. 48, 53–54. The initial subjects of Fermat's correspondence included divisors ("aliquot parts") and many subjects outside number theory; see the list in the letter from Fermat to Roberval, 22.IX.1636, Tannery & Henry 1891, Vol. II, pp. 72, 74, cited in Mahoney 1994, p. 54.
[38] Tannery & Henry 1891, Vol. II, p. 209, Letter XLVI from Fermat to Frenicle, 1640, cited in Weil 1984, p. 56
[39] Tannery & Henry 1891, Vol. II, p. 204, cited in Weil 1984, p. 63. All of the following citations from Fermat's Varia Opera are taken from Weil 1984, Chap. II. The standard Tannery & Henry work includes a revision of Fermat's posthumous Varia Opera Mathematica originally prepared by his son (Fermat 1679).