International Journal of Research in Engineering, Science and Management
Volume-2, Issue-6, June-2019
www.ijresm.com | ISSN (Online): 2581-5792


# A Paper on Number Theory

Pulipaka Srinivasa Chakravarthy[1], Putta Babu Rao[2]
[1]*Senior Lecturer, Department of Mathematics, Parvathaneni Brahmayya Siddhartha College of Arts and Science, Vijayawada, India*
[2]*Lecturer & Vice-Principal, Department of Mathematics, Parvathaneni Brahmayya Siddhartha College of Arts and Science, Vijayawada, India*

***Abstract*: Number theory, branch of mathematics concerned with properties of the positive integers (1, 2, 3 …). Sometimes called "higher arithmetic," it is among the oldest and most natural of mathematical pursuits. Number theory has always fascinated amateurs as well as professional mathematicians. In contrast to other branches of mathematics, many of the problems and theorems of number theory can be understood by laypersons, although solutions to the problems and proofs of the theorems often require a sophisticated mathematical background. Until the mid-20th century, number theory was considered the purest branch of mathematics, with no direct applications to the real world. The advent of digital computers and digital communications revealed that number theory could provide unexpected answers to real-world problems. At the same time, improvements in computer technology enabled number theorists to make remarkable advances in factoring large numbers, determining primes, testing conjectures, and solving numerical problems once considered out of reach. Modern number theory is a broad subject that is classified into subheadings such as elementary number theory, algebraic number theory, analytic number theory, geometric number theory, and probabilistic number theory. These categories reflect the methods used to address problems concerning the integers.**

***Keywords*: Enter key words or phrases in alphabetical order, separated by commas.**

## 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*.

## 2. 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..."

### *A. The Plimpton 322 tablet*

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 methodwas 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 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*

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 they 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, theorising 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.

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*

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. 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.

- 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 *elementary* proof 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.

#### 1) *Analytic number theory*

Riemann zeta function $\zeta(s)$ in the complex plane. The color of a point $s$gives the value of $\zeta(s)$: 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. 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.

#### 2) *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.[81] 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.

*3) 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?

*4) Other subfields*

The areas below date from no earlier than the mid-twentieth century, even if they are based on older material. For example, as is explained below, the matter of algorithms in number theory is very old, in some sense older than the concept of proof; at the same time, the modern study of computability dates only from the 1930s and 1940s, and computational complexity theory from the 1970s.

*5) Probabilistic number theory*

Take a number at random between one and a million. How likely is it to be prime? This is just another way of asking how many primes there are between one and a million. Further: how many prime divisors will it have, on average? How many divisors will it have altogether, and with what likelihood? What is the probability that it will have many more or many fewer divisors or prime divisors than the average?

Much of probabilistic number theory can be seen as an important special case of the study of variables that are almost, but not quite, mutually independent. For example, the event that a random integer between one and a million be divisible by two and the event that it be divisible by three are almost independent, but not quite.

It is sometimes said that probabilistic combinatorics uses the fact that whatever happens with probability greater than must happen sometimes; one may say with equal justice that many applications of probabilistic number theory hinge on the fact that whatever is unusual must be rare. If certain algebraic objects (say, rational or integer solutions to certain equations) can be shown to be in the tail of certain sensibly defined distributions, it follows that there must be few of them; this is a very concrete non-probabilistic statement following from a probabilistic one.

At times, a non-rigorous, probabilistic approach leads to a number of heuristic algorithms and open problems, notably Cramér's conjecture.

*6) Arithmetic combinatoZ-rics*

Let $A$ be a set of $N$ integers. Consider the set $A + A = \{ m + n \mid m, n \in A \}$ consisting of all sums of two elements of $A$. Is $A + A$ much larger than $A$? Barely larger? If $A + A$ is barely larger than $A$, must $A$ have plenty of arithmetic structure, for example, does $A$ resemble an arithmetic progression?

*7) Computations in number theory*

While the word *algorithm* goes back only to certain readers of al-Khwārizmī, careful descriptions of methods of solution are older than proofs: such methods (that is, algorithms) are as old as any recognisable mathematics—ancient Egyptian, Babylonian, Vedic, Chinese—whereas proofs appeared only with the Greeks of the classical period. An interesting early case is that of what we now call the Euclidean algorithm. In its basic form (namely, as an algorithm for computing the greatest common divisor) it appears as Proposition 2 of Book VII in *Elements*, together with a proof of correctness. However, in the form that is often used in number theory (namely, as an algorithm for finding integer solutions to an equation , or, what is the same, for finding the quantities whose existence is assured by the Chinese remainder theorem) it first appears in the works of Āryabhaṭa (5th–6th century CE) as an algorithm called *kuṭṭaka* ("pulveriser"), without a proof of correctness.

There are two main questions: "can we compute this?" and "can we compute it rapidly?". Anyone can test whether a number is prime or, if it is not, split it into prime factors; doing so rapidly is another matter. We now know fast algorithms for testing primality, but, in spite of much work (both theoretical and practical), no truly fast algorithm for factoring.

## 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), van der Waerden 1961, p. 184.

[3] 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).

[4] Friberg 1981, p. 302.

[5] van der Waerden 1961, p. 43.

[6] 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.

[7] 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.
[8] Becker 1936, p. 533, cited in: van der Waerden 1961, p. 108.
[9] Becker 1936.
[10] van der Waerden 1961, p. 109.
[11] 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.
[12] von Fritz 2004.
[13] Heath 1921, p. 76.
[14] 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.
[15] 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.
[16] Boyer & Merzbach 1991, p. 82.
[17] "Eusebius of Caesarea: Praeparatio Evangelica (Preparation for the Gospel). Tr. E.H. Gifford (1903) – Book 10".
[18] Metaphysics, 1.6.1 (987a)
[19] Tusc. Disput. 1.17.39.
[20] Vardi 1998, pp. 305–19.
[21] Weil 1984, pp. 17–24.
[22] Jump up to: Plofker 2008, p. 119.
[23] Any early contact between Babylonian and Indian mathematics remains conjectural (Plofker 2008, p. 42).