Number Theory – Số Học

Nguyễn Quản Bá Hồng[*]

Ngày 13 tháng 11 năm 2024

Tóm tắt nội dung

This text is a part of the series *Some Topics in Advanced STEM & Beyond*:
URL: https://nqbh.github.io/advanced_STEM/.
Latest version:

- *Number Theory – Số Học*.
PDF: URL: https://github.com/NQBH/advanced_STEM_beyond/blob/main/number_theory/NQBH_number_theory.pdf.
TEX: URL: https://github.com/NQBH/advanced_STEM_beyond/blob/main/number_theory/NQBH_number_theory.tex.

Mục lục

1 Wikipedia **1**
1.1 Wikipedia/analytic number theory 1
1.1.1 Branches of analytic number theory 1
1.1.2 History 2
1.1.3 Problems & results 2
1.1.4 Methods of analytic number theory 3
1.2 Wikipedia/number theory 3
1.2.1 History 3
1.2.2 Main subdivisions 3
1.2.3 Other subfields 3
1.2.4 Applications 4
1.2.5 Prizes 4

2 Basic **5**

3 Miscellaneous **5**

Tài liệu **5**

1 Wikipedia

1.1 Wikipedia/analytic number theory

"Riemann zeta function $\zeta(s)$ in the complex plane. The color of a point s encodes the value of $\zeta(s)$: colors close to black denote values close to 0, while hue encodes the value's argument. In mathematics, *analytic number theory* is a branch of number theory that uses method from mathematical analysis to solve problems about the integers. It is often said to have begun with Peter Gustav Lejeune Dirichlet's 1837 introduction of Dirichlet L-functions to give the 1st proof of Dirichlet's theorem on arithmetic progressions. It is well known for its results on prime numbers (involving the Prime Number Theorem & Riemann zeta function) & additive number theory (e.g., Goldbach conjectures & Waring's problem).

1.1.1 Branches of analytic number theory

Analytic number theory can be split up into 2 major parts, divided more by the type of problems they attempt to solve than fundamental differences in technique.

- Multiplicative number theory deals with the distribution of the prime numbers, e.g., estimating the number of primes in an interval, & includes the prime number theorem & Dirichlet's theorem on primes in arithmetic progressions.

- Additive number theory is concerned with the additive structure of the integers, e.g., Goldbach conjectures that every even number > 2 is the sum of 2 primes. 1 of the main results in additive number theory is the solution to Waring's problem).

[*] A Scientist & Creative Artist Wannabe. E-mail: nguyenquanbahong@gmail.com. Bến Tre City, Việt Nam.

1.1.2 History

1. **Precursors.**
2. **Dirichlet.**
3. **Chebyshev.**
4. **Riemann.**
5. **Hadamard & de la Vallée-Poussin.**
6. **Modern times.**

1.1.3 Problems & results

Theorems & results within analytic number theory tend not to be exact structural results about the integers, for which algebraic & geometrical tools are more appropriate. Instead, they give approximate bounds & estimates for various number theoretical functions, as the following examples illustrate.

1. **Multiplicative number theory.** Main article: Wikipedia/multiplicative number theory. Euclid showed that there are infinitely many prime numbers. An important question is to determine the asymptotic distribution of the prime numbers; i.e., a rough description of how many primes are smaller than a given number. Gauss, amongst others, after computing a large list of primes, conjectures that the number of primes $\le$ a large number N is close to the value of the integral $\int_2^N \frac{1}{\log t}\,\mathrm{d}t$. In 1859 Bernhard Riemann used complex analysis & a special meromorphic function now known as the Riemann zeta function to derive an analytic expression for the number of primes $\le x \in \mathbb{R}$. Remarkably, the main term in Riemann's formula was exactly the integral $\int_2^N \frac{1}{\log t}\,\mathrm{d}t$, lending substantial weight to Gauss's conjecture. Riemann found that the error terms in this expression, & hence the manner in which the primes are distributed, are closely related to the complex zeros of the zeta function. Using Riemann's ideas & by getting more information on the zeros of the zeta function, Jacques Hadamard & Charles Jean de la Vallée-Poussin managed to complete the proof of Gauss's conjecture. In particular, they proved that if $\pi(x) =$ (number of primes $\le x$) then $\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$. This remarkable result is what is now known as the *prime number theorem*. It is a central result in analytic number theory. Loosely speaking, it states that given a large number N, the number of primes $\le N$ is $\approx \frac{N}{\log N}$.

   More generally, the same question can be asked about the number of primes in any arithmetic progression $a + nq$ for any $n \in \mathbb{Z}$. In 1 of the 1st applications of analytic techniques to number theory, Dirichlet proved that any arithmetic progression with a, q coprime contains infinitely many primes. The prime number theorem can be generalized to this problem; letting $\pi(x, a, q) \coloneqq$ (number of primes $\le x$ s.t. p is in the arithmetic progression $a + nq, n \in \mathbb{Z}$), then given ϕ as the totient function & if a, q coprime, $\lim_{x\to\infty} \frac{\pi(x,a,q)\phi(q)}{\frac{x}{\log x}} = 1$. There are also many deep & wide-ranging conjectures in number theory whose proofs seem too difficult for current techniques, e.g., the twin prime conjecture which asks whether there are infinitely many primes p s.t. $p + 2$ is prime. On th assumption of the Elliott–Halberstam conjecture it has been proven recently that there are infinitely many primes p s.t. $p + k$ is prime for some positive even k at most 12. Also, it has been proven unconditionally (i.e., not depending on unproven conjectures) that there are infinitely many primes p s.t. $p + k$ is prime for some positive even k at most 246.

2. **Additive number theory.** Main article: Wikipedia/additive number theory. 1 of the most important problems in additive number theory is Waring's problem, which asks whether it is possible, for any $k \ge 2$, to write any positive integer as the sum of a bounded number of kth powers, $n = \sum_{i=1}^l x_i^k$. The case for squares, $k = 2$, was answered by Lagrange in 1770, who proved that every positive integer is the sum of at most 4 squares. The general case was proved by Hilbert in 1909, using algebraic techniques which gave no explicit bounds. An important breakthrough was the application of analytic tools to the problem by Hardy & Littlewood. These techniques are known as the circle method, & give explicit upper bounds for the function $G(k)$, the smallest number of kth powers needed, e.g., Vinogradov's bound $G(k) \le k(3\log k + 11)$.

3. **Diophantine problems.** Main article: Wikipedia/Diophantine problem. Diophantine problems are concerned with integer solutions to polynomial equations: one may study the distribution of solutions, i.e., counting solutions according to some measure of "size" or *height*. An important example is the Gauss circle problem, which asks for integers points (x, y) which satisfy $x^2 + y^2 \le r^2$. In geometrical terms, given a circle centered about the origin in the plane with radius r, the problem asks how many integer lattice points lie on or inside the circle. It is not hard to prove that the answer is $\pi r^2 + E(r)$, where $\frac{E(r)}{r^2} \to 0$ as $r \to \infty$. Again, the difficult part & a great achievement of analytic number theory is obtaining specific upper bounds on the error term $E(r)$.

   Gauss showed that $E(r) = O(r)$. In general, an $O(r)$ error term would be possible with the unit circle (or, more properly, the closed unit disk) replaced by the dilates of any bounded planar region with piecewise smooth boundary. Furthermore, replacing the unit circle by the unit square, the error term for the general problem can be as large as a linear function of r. Therefore, getting an error bound of the form $O(r^{\delta})$ for some $\delta < 1$ in the case of the circle is a significant improvement. The 1st to attain this was Sierpinski in 1906, who showed $E(r) = O(r^{\frac{2}{3}})$. In 1915, Hardy & Landau each showed that one does *not* have $E(r) = O(r^{\frac{1}{2}})$. Since then the goal has been to show that for each fixed $\epsilon > 0$ there exists a number number $C(\epsilon)$ s.t. $E(r) \leq C(\epsilon) r^{\frac{1}{2}+\epsilon}$. In 2000 Huxley showed that $E(r) = O(r^{\frac{131}{208}})$, which is the best published result.

1.1.4 Methods of analytic number theory

1. **Dirichlet series.**

2. **Riemann zeta function.**

” – Wikipedia/analytic number theory

1.2 Wikipedia/number theory

“The distribution of prime numbers is a central point of study in number theory. This Ulam spiral serves to illustrate it, hinting, in particular, at the conditional independence between being prime & being a value of certain quadratic polynomials. *Number theory* (or arithmetic or *higher arithmetic* in older usage) is a branch of pure mathematics devoted primarily to the study of the integers & arithmetic functions. German mathematician Carl Friedrich Gauss (1777–1855) said, “Mathematics is the queen of the sciences – & number theory is the queen of mathematics.” Number theorists study prime numbers as well as the properties of mathematical objects constructed from integers (e.g., rational numbers), or defined as generalizations of the integers (e.g., 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 (e.g., 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; e.g., as approximated by the latter (Diophantine approximation).

The older term for number theory is *arithmetic*. By the early 20th 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*, & computer science, as in *floating-point arithmetic*). The use of the term *arithmetic* for *number theory* regained some ground in the 2nd half of the 20th century, arguably in part due to French influence. In particular, *arithmetical* is commonly preferred as an adjective to *number-theoretic*.

1.2.1 History

1. **Origins.**

2. **Early modern number theory.**

3. **Maturity & division into subfields.**

1.2.2 Main subdivisions

1. **Elementary number theory.** Number theorists Paul Erdős & Terence Tao in 1985, when Paul Erdős was 72 & Tao was 10. The term *elementary* generally denotes a method that does not use complex analysis. E.g., the prime number theorem was 1st proven using complex analysis in 1896, but an elementary proof was found in 1949 by Erdős & Selberg. The term is somewhat ambiguous: e.g., proofs based on complex Tauberian theorems (e.g., 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 & 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.

2. **Analytic number theory.**

3. **Algebraic number theory.**

4. **Diophantine geometry.**

1.2.3 Other subfields

The areas below date from no earlier than the mid-20th century, even if they are based on older material. E.g., as explained below, algorithms in number theory have a long history, arguably predating the formal concept of proof. However, the modern study of computability began only in the 1930s & 1940s, while computational complexity theory emerged in the 1970s.

1. **Probabilistic number theory.** Main article: Wikipedia/probabilistic number theory. Probabilistic number theory starts with questions e.g.: Take $n \in \mathbb{Z} \cap [1, 10^6]$ randomly. How likely is it to be prime? (this is just another way of asking how many primes there are between 1 & 10^6). How many prime divisors will n have on average? 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. E.g., the event that a random integer between 1 & 10^6 be divisible by 2 & the even that it be divisible by 3 are almost independent, but not quite.

   It is sometimes said that probabilistic combinatorics uses the fact that whatever happens with probability > 0 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 & open problems, notably Cramér's conjecture.

2. **Arithmetic combinatorics.** Main articles: Wikipedia/arithmetic combinatorics, Wikipedia/additive number theory. Arithmetic combinatorics starts with questions like: Does a fairly "thick" infinite set A contain many elements in arithmetic progression: $a, a+b, a+2b, \ldots, a+10b$, say?? Should it be possible to write large integers as sums of elements of A?

   These questions are characteristic of *arithmetic combinatorics*. This is a presently coalescing field; it subsumes *additive number theory* (which concerns itself with certain very specific sets A of arithmetic significance, e.g. the primes or the squares) &, arguably, some of the *geometry of numbers*, together with some rapidly developing new material. Its focus on issues of growth & distribution accounts in part for its developing links with ergodic theory, finite group theory, model theory, & other fields. The term *additive combinatorics* is also used; however, the sets A being studied need not be sets of integers, but rather subsets of non-commutative groups, for which the multiplication symbol, not the addition symbol, is traditionally used; they can also be subsets of rings, in which case the growth of $A + A$ & $A \cdot A$ may be compared.

3. **Computational number theory.** Main article: Wikipedia/computational number theory. A Lehmer sieve, a primitive digital computer used to find primes & solve simple Diophantine equations. While the word *algorithm* goes back only to certain readers of al-Khwarizmi, careful descriptions of methods of solution are older than proofs: such methods (i.e., algorithms) are as old as any recognizable mathematics – ancient Egyptian, Babylonian, Vedic, Chinese – whereas proofs appeared only with the Greeks of the classical period.

   [...]

1.2.4 Applications

The number-theorist Leonard Dickson (1874–1954) said "Thank god that number theory is unsullied by any application"[1]. Such a view is no longer applicable to number theory. In 1974, Donald Knuth said "virtually every theorem in elementary number theory arises in a natural, motivated way in connection with the problem of making computers do high-speed numerical calculations". Elementary number theory is taught in discrete mathematics courses for discrete mathematics courses for computer scientists. It also has applications to the continuous in numerical analysis.

Number theory has now several modern applications spanning diverse areas e.g.:

- Cryptography: Public-key encryption schemes e.g. RSA are based on the difficulty of factoring large composite numbers into their prime factors.
- Computer science: The fast Fourier transform (FFT) algorithm, which is used to efficiently compute the discrete Fourier transform, has important applications in signal processing & data analysis.
- Physics: The Riemann hypothesis has connections to the distribution of prime numbers & has been studied for its potential implications in physics.
- Error correction codes: The theory of finite fields & algebraic geometry have been used to construct efficient error-correcting codes.
- Communications: The design of cellular telephone networks requires knowledge of the theory of modular forms, which is a part of analytic number theory.
- Study of musical scales: the concept of "equal temperament", which is the basis for most modern Western music, involves dividing the octave into 12 equal parts. This has been studied using number theory & in particular the properties of the $\sqrt[12]{2}$.

1.2.5 Prizes

The American Mathematical Society awards the *Cole Prize in Number Theory*. Moreover, number theory is 1 of the 3 mathematical subdisciplines rewarded by the *Fermat Prize*." – Wikipedia/number theory

[1] Lý thuyết số không bị ảnh hưởng bởi bất kỳ ứng dụng nào.

2 Basic

Community – Cộng đồng.

1. Dương Quốc Việt.

   Website. https://vietduongquoc.wordpress.com.

Resources – Tài nguyên.

1. [VN25]. Dương Quốc Việt, Đàm Văn Nhỉ. *Cơ Sở Lý Thuyết Số & Đa Thức.*

- Chap. 1: Lý thuyết chia hết trong vành các số nguyên.
- Chap. 2: Các hàm số học.
- Chap. 3: Lý thuyết đồng dư.
- Chap. 4: Phương trình đồng dư.
- Chap. 5: Sơ đồ xây dựng số.
- Chap. 6: Liên phân số.
- Chap. 7: Đa thức.

3 Miscellaneous

Tài liệu

[VN25] Dương Quốc Việt and Đàm Văn Nhỉ. *Cơ Sở Lý Thuyết Số & Đa Thức*. Nhà Xuất Bản Đại Học Sư Phạm, 2025, p. 231.