

# Number Theory – Số Học

Nguyễn Quân Bá Hồng\*

Ngày 12 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/](https://nqbh.github.io/advanced_STEM/).

Latest version:

- *Number Theory – Số Học*.

PDF: URL: [.pdf](#).

T<sub>E</sub>X: URL: [.tex](#).

## Mục lục

<b>1</b>	<b>Wikipedia</b>	<b>1</b>
1.1	Wikipedia/analytic number theory	1
1.1.1	Branches of analytic number theory	1
1.1.2	History	1
1.1.3	Problems & results	2
1.1.4	Methods of analytic number theory	2
1.2	Wikipedia/number theory	3
<b>2</b>	<b>Miscellaneous</b>	<b>3</b>

## 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**).

#### 1.1.2 History

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

---

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

### 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  $\leq$  a large number  $N$  is close to the value of the integral  $\int_2^N \frac{1}{\log t} dt$ . 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  $\leq x \in \mathbb{R}$ . Remarkably, the main term in Riemann's formula was exactly the integral  $\int_2^N \frac{1}{\log t} dt$ , 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  $\pi(x) = (\text{number of primes } \leq x)$  then  $\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$ . 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  $\leq N$  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  $\pi(x, a, q) := (\text{number of primes } \leq x \text{ s.t. } p \text{ is in the arithmetic progression } a + nq, n \in \mathbb{Z})$ , then given  $\phi$  as the **totient function** & if  $a, q$  coprime,  $\lim_{x \rightarrow \infty} \frac{\pi(x, a, q)\phi(q)}{\frac{x}{\log x}} = 1$ . 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 the 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  $k \geq 2$ , to write any positive integer as the sum of a bounded number of  $k$ th 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  $k$ th powers needed, e.g., VINOGRADOV's bound  $G(k) \leq k(3 \log k + 11)$ .
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  $x^2 + y^2 \leq r^2$ . 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  $\frac{E(r)}{r^2} \rightarrow 0$  as  $r \rightarrow \infty$ . 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

2 Miscellaneous