Liet. matem. rink., T. 43, spec. nr., 361–364

The geometry of numbers in Lithuanian school of the number theory

Antanas LAURINČIKAS (VU, ŠU) *
e-mail: antanas.laurincikas@maf.vu.lt

The investigations of some mathematical problems led to numbers α which are roots of polynomials with rational coefficients. Such numbers are called algebraic numbers. For example, 3 and $\sqrt{3}$ are algebraic numbers because they satisfy the equations $x - 3 = 0$ and $x^2 - 3 = 0$, respectively. A polynomial of minimal degree with a root α is called the minimal polynomial of the algebraic number α. An algebraic number is an algebraic integer if the coefficients of its minimal polynomial are rational integers.

All rational numbers form the field of rational numbers $\mathbb{Q}$. It is not difficult to see that if α and β are algebraic numbers, then $\alpha \pm \beta$, $\alpha \cdot \beta$, $\frac{\alpha}{\beta}$, $\beta \neq 0$, are again algebraic numbers. Therefore, algebraic numbers also form a field. The field $\mathbb{Q}$ can be extended by adding to it a given algebraic number θ. This leads to an algebraic numbers field $\mathbb{Q}(\theta)$ consisting of fractions $p(\theta)/q(\theta)$, where $p(\theta)$ and $q(\theta)$ are polynomials with rational coefficients. However, contrary to the field $\mathbb{Q}$, the numbers of algebraic numbers fields have not unique decomposition by factors. For example, consider the imaginary quadratic field $\mathbb{Q}(-\sqrt{5})$, its numbers α are of the form

$$\alpha = a + b\sqrt{-5}, \quad a, b \in \mathbb{Q}.$$

Clearly, $21 \in \mathbb{Q}(\sqrt{-5})$, and we have two decompositions

$$21 = 3 \cdot 7 \text{ and } 21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

by non-decomposable in $\mathbb{Q}(-\sqrt{5})$ factors. It turns out, that this is why because the factors 3 and $1 + 2\sqrt{-5}$ have a common divisor which is not in the field $\mathbb{Q}(\sqrt{-5})$. Therefore, in order to have the unique decomposition we must extend the field $\mathbb{Q}(\sqrt{-5})$ by adding common divisors of their elements not belonging to $\mathbb{Q}(\sqrt{-5})$. Such extended field is called an ideal numbers system.

Now let $\mathbb{Q}(\theta)$ be an arbitrary algebraic number field. The whole of linear combinations of

$$\alpha_1\xi_1 + \cdots + \alpha_r\xi_r$$

is called the ideal of $\mathbb{Q}(\theta)$. If $\alpha_1, \ldots, \alpha_r$ are integer algebraic numbers, then the latter ideal is integer. All integers of the field form the unit ideal (1). For ideals, the operations

*Partially supported by Lithuanian Science and Studies Foundation.

of multiplication, of power and of division are defined. Also, the relation of congruence is introduced. Similarly to the notion of rational prime number, a prime ideal $\mathfrak{P}$ is defined. $\mathfrak{P}$ is an integer non-zero ideal which is divided only by $\mathfrak{P}$ and (1). An analog of the principal theorem of arithmetic is true: every non-zero integer ideal $\mathfrak{A}$ of algebraic number field is decomposable uniquely in a product of prime ideals. This leads to the canonic decomposition $\mathfrak{A} = \mathfrak{P}_1^{\alpha_1} \dots \mathfrak{P}_r^{\alpha_r}$, where $\mathfrak{P}_i$ are distinct prime ideals, and $\alpha_i \geqslant 1$ are integers, $i = 1, \dots, r$. We note that E. Kummer (1810–1893) is a founder of the ideal theory. The origin of this theory was stimulated by attempts to prove the last Fermat problem on the non-solvability in integers of the equation $x^n + y^n = z^n, \quad n \geqslant 3$. In general, the founders of algebraic number theory are G. Cantor (1845–1918), C.F. Gauss (1777–1855), C. Jacobi (1804–1851), E. Galois (1811–1832), D. Hilbert (1862–1943), L. Dirichlet (1805–1859) and other famous mathematicians.

In the field of rational numbers one of the most important problems is the asymptotic behaviour of the number of prime numbers not exceeding x

$$\pi(x) = \sum_{p \leqslant x} 1,$$

as $x \to \infty$. The investigation of the last problem required much time and efforts of many mathematicians. At the end of the 19th century it was established that

$$\pi(x) \sim \int_2^\infty \frac{\mathrm{d}u}{\log u}, \quad x \to \infty.$$

Later, estimates for error terms in the latter asymptotic equality were given. Similar but more complicated problems also arise in algebraic number fields.

It is known that one and only one ideal corresponds every ideal number. On the contrary, all ideal numbers corresponding the same ideal of the field are associated, i.e., they differ only by an unit factor. Therefore, in the investigation of algebraic number field its ideal numbers can be identified with ideals. For the statement of the problem we also need the ideal norm which is defined in the following manner. All algebraic integer numbers of an ideal form a ring $\mathfrak{R}$. Let $\mathfrak{A}$ be an integer ideal of the field. Then all elements of the ring $\mathfrak{R}$ can be divided into residue classes with respect to the ideal $\mathfrak{A}$. The set of these classes also is a ring, and the number of elements of this ring is called the norm $N\,\mathfrak{A}$ of the ideal $\mathfrak{A}$. Clearly, $N\,\mathfrak{A}$ is a positive integer, while the norm $N\alpha$ of an algebraic number α is equal to the product of all roots of its minimal polynomial. If an ideal number α corresponds an ideal $\mathfrak{A}$, then we have that $N\alpha = N\,\mathfrak{A}$. Also, for an ideal we can introduce a notion of its argument, and we have $\arg\alpha = \arg\mathfrak{A}$.

Thus in an algebraic number field a problem of the distribution of prime ideal numbers or of prime ideals $\mathfrak{P}$ arises. Clearly, the simplest problem is to find the asymptotics of $\sum_{N\,\mathfrak{P} \leqslant x} 1$ as $x \to \infty$. Long time the latter problem was investigated and made more precise. However, the norm $N\,\mathfrak{A}$ do not reflect completely the distribution of prime ideal numbers, since, in general, $\mathfrak{P}$ is multidimensional numbers, for example, in the case of the imaginary number field $\mathbb{Q}(\sqrt{-d})$ these numbers are twodimensional, therefore it is

natural to consider their location on the complex plane. Only in the second decade of last century a German mathematician E. Hecke (1887–1947) began to study the distribution laws of prime ideal numbers taking into account the geometric location of these numbers. Investigating an algebraic number field of degree n, he obtained the asymptotics of the function

$$\widehat{\pi}(x) = \sum_{\substack{N\mathfrak{P}\leqslant x \\ \mathfrak{P}\in(n-1)\text{-dimensional sector}}} 1$$

as $x \to \infty$. Unfortunately, his method based on Weil's criterion of uniform distribution did not allow him to estimate the error term in the asymptotic law. In 1935 an other German mathematician H. Rademacher (1892–1969) in the case of real quadratic field obtained the asymptotics for the function $\widehat{\pi}(x)$ with error term $Bx\exp\{-c_1\sqrt{\log x}\}$ (B is a quantity bounded by a constant)for hyperbolic sectors as well as for rectangles with vertices at the origin. These results were a foundation for a new direction in the geometry of numbers. Later results in this field belong to Professor J. Kubilius. During his doctoral studies in Leningrad University (1948–1951), he began to consider the distribution of prime numbers in the Gaussian field $\mathbb{Q}(i), i = \sqrt{-1}$, and proved (1950) that, for sufficiently large x,

$$\sum_{\substack{N\mathfrak{P}\leqslant x \\ \varphi_1\leqslant arg\,\mathfrak{P}\leqslant\varphi_2}} 1 = \frac{2}{\pi}(\varphi_2-\varphi_1)\int_2^x \frac{\mathrm{d}u}{\log u} + Bx\exp\{-c_2\sqrt{\log x}\}. \tag{1}$$

Here $0 \leqslant \varphi_1 < \varphi_2 \leqslant 2\pi$, and $\mathfrak{P}$ denotes an ideal prime number of $\mathbb{Q}(i)$.

After publishing this result J. Kubilius continued the investigations in the case of an arbitrary algebraic number field $\mathbb{K}$ of degree n. The results obtained are contained in the paper of great volume [1], where several statement of type (1) are obtained. To state the simplest of them we need some additional notation. Let $\mu \neq (0)$ be an integer ideal of $\mathbb{K}$, and let $h(\mu)$ stand for the residue class number $mod\mu$. Denote by $\mathrm{e}(\mu)$ the index of the field $\mathbb{K}$. Moreover, let $g(\alpha)$ be the Hecke character of the first kind with exponents m_j, i.e., $g(\alpha) = g_1^{m_1}(\alpha)\dots g_{n-1}^{m_{n-1}}(\alpha)$. The characters $g_j(\alpha),\ j = 1,\dots,n-1$, are called the generators, and the real numbers $w_j(\alpha)$ satisfying $g_j(\alpha) = \mathrm{e}^{2\pi w_j(\alpha)}, j = 1,\dots,n-1$, are called the amplitudes of generators. The asterisk in $\sum^*$ means that the sum is taken over the set of nonassociated nonzero numbers. Let w_j' and w_j'', $0 \leqslant w_j' < w_j'' \leqslant 1$, $j = 1,\dots,n-1$, be real numbers and let $\mathcal{P}$ denote the $(n-1)$-dimensional parallelepiped $w_j' \leqslant w_j \leqslant w_j'', j = 1,\dots,n-1$. Then in [1] the following distribution low of ideal prime numbers of the field $\mathbb{K}$ is obtained: for all $x > 2$

$$\sum_{\substack{N\mathfrak{P}\leqslant x \\ (\{\omega_1(\mathfrak{P})\},\dots,\{\omega_{n-1}(\mathfrak{P})\})\in\mathcal{P}}}^{*} 1 = \frac{e(\mu)}{h(\mu)}\prod_{j=1}^{n-1}(\omega_j''-\omega_j')\int_2^\infty \frac{\mathrm{d}u}{\log u} + R(x), \tag{2}$$

where the error term $R(x)$ is the same as in (1).

We note that the paper [1] is very rich in new results and methods used, later it was a starting point for many mathematicians. The second part of this paper is devoted to the quadratic imaginary field $\mathbb{Q}(\sqrt{d}), d < 0$ is a square-free number. Using successfully the method of trigonometric sums and the zero-density method, the author obtained the distribution law of prime ideal numbers in sectors with an error term better than in (1).

It is of interest that J. Kubilius, investigating the quadratic imaginary field, observed the relation between his results and the famous Landau hypothesis on infinitely many rational prime numbers p of the form $p = a^2 + 1$. The results obtained on prime ideal numbers allowed him to prove that there are infinitely many prime ideal numbers p of the form $p = a^2 + b^2$ with $|b| \leqslant p^{\theta+\epsilon}$ for $\theta = \frac{7}{16} = 0.4375$ and every $\epsilon > 0$ (1951). This result was improved in [1] until $\theta = \frac{25}{64} = 0.390625$. However, J. Kubilius did not stop in this place. Already after defending his famous thesis of candidate degree (1951), in the case of quadratic imaginary field he obtained the distribution low of prime ideal numbers in narrow sectors, and decreased θ until $\frac{57}{146} = 0.3904\ldots$.

The works of J. Kubilius on the geometry of numbers were continued and developed by a group of his students. J. Vaitkevičius, see [2], p. 239, 1962, connected the error term in [1] with that in the asymptotic formula for $\pi(x)$. J. Urbelis, see [2] p. 236, 1964, improved formula (2) obtaining $R(x) = Bx\exp\{-c_3(\log x)^{\frac{7}{12}}(\log\log x)^{-\frac{4}{3}}\}$, and derived a more precise result, see [2], p. 236, 1965, in the case of a purely real field. K. Bulota and M. Maknys once more improved Kubilius's results on the distribution of prime ideal numbers in narrow sectors, and decreased the constant θ until $\frac{1}{3}$ (K. Bulota, see [2], p. 44, 1964), and until $\frac{11}{48}$ and $\frac{13}{74}$ (M. Maknys, see [2], p. 137, 1975–1977).

E. Gaigalas developed the ideas of A.I. Vinogradov and obtained the distribution law of prime ideal numbers of two quadratic imaginary fields having the same norm in both fields, see [2], p. 62, 1979. This led him to the statement that there are infinitely many prime rational numbers p of the form $p = a_1^2 + d_1b_1^2 = a_2^2 + d_2b_2^2$ with $|b_j| \leqslant p^{\frac{7}{22}+\epsilon}$, $j = 1, 2$.

The results on a decomposition of products $p_1p_2p_3$ and p_1p_2 into a sum of two squares where obtained by J. Kubilius jointly with his teacher J. Linnik in 1951–1956.

The ideas of J. Kubilius on the distribution of prime ideal numbers also were developed by foreign mathematicians, among then N. Kalnins (1966), A. Danilov (1967), T. Mitsui (1965, 1968), R. Schultz–Arestorff (1957) and others.

References

[1] J. Kubilius, On some problems on geometry of primes, *Matem. Sb.*, **31**, 507–542 (1952) (in Russian).
[2] V. Verikaitė, H. Jasiūnas (Eds.), *Lietuvos Matematikos Rinkinys, 1–40 tomų autorių rodyklė*, TEV, Vilnius (2001).

Skaičių geometrija Lietuvos skaičių teorijos mokykloje

A. Laurinčikas

Pateikta Lietuvos autorių darbų apžvalga apie pirminių idealiųjų skaičių geometriją bei jos taikymus.