TSUKUBA J. MATH.
Vol. 4 (1980). 9—13

THE DISTRIBUTION OF RESIDUE CLASSES MODULO $\mathfrak{a}$ IN AN ALGEBRAIC NUMBER FIELD

By

Shigeki EGAMI

Let K be an algebraic number field of degree n and $\mathfrak{o}_K$ the ring of integers of K. It is easily seen that for every integral ideal $\mathfrak{a}$ of K and residue class A of $\mathfrak{o}_K/\mathfrak{a}$

$$\min_{\alpha\in A}|N_K\alpha|<c(K)N_K\mathfrak{a} \tag{1}$$

where $c(K)$, and in what follows $c'(K)$, $c''(K)$, $\cdots$, are constants depending only on K. An explicit estimate for $c(K)$ was obtained by H. Davenport [1]. In this paper we will show that for some "large number" of ideals $\mathfrak{a}$ and "almost all" its residue classes A, the estimate (1) can considerably be strengthend if K has infinitely many units. For any $\lambda>0$ and any integral ideal $\mathfrak{a}$ we define a subset $E(\lambda;\mathfrak{a})$ of $\mathfrak{o}_K/\mathfrak{a}$ by

$$E(\lambda;\mathfrak{a})=\{A\in\mathfrak{o}_K/\mathfrak{a}\,;\ \min_{\alpha\in A}|N_K\alpha|<\lambda N_K\mathfrak{a}\}\ .$$

The natural density of a set $\mathcal{P}$ of rational primes is defined as usual by

$$\lim_{x\to\infty}\frac{\sum_{\substack{p\in\mathcal{P}\\ p\leq x}}1}{\pi(x)} \tag{2}$$

where $\pi(x)$ denotes the number of primes not exceeding x. Then we can state our

THEOREM. *Let K be an algebraic number field having infinitely many units. Then there exists a set $\mathcal{P}$ of rational primes of natural density* 1 *such that*

$$\lim_{\substack{p\in\mathcal{P}\\ p\to\infty}}\frac{|E(\lambda;(p))|}{N_K(p)}=1 \tag{3}$$

for any $\lambda>0$, where $|S|$ is the cardinarity of a set S.

REMARK. *Theorem implies especially*

$$\limsup_{N_K\mathfrak{a}\to\infty}\frac{|E(\lambda;\mathfrak{a})|}{N_K\mathfrak{a}}=1\ ,$$

Received October 1, 1979

if K has infinitely many units. Otherwise, i.e. K is either the rational number field or an imaginary quadratic field, we can easily see

$$\lim_{N_K\mathfrak{a}\to\infty}\frac{|E(\lambda;\mathfrak{a})|}{N_K\mathfrak{a}}=\lambda c'(K).$$

For the proof of Theorem we show first an ergodic theorem for an automorphism of a vector space, which contains as a special case a theorem of A. G. Postnikov [2].

Let p be a rational prime, F_p the finite field with p elements, and $V=F_p^n$. Every element of V can be represented by a vector $(x_1, \cdots, x_n)$, $x_j\in \boldsymbol{Z}$, $0\leqq x_j<p$. ($\boldsymbol{Z}$ denotes the set of all rational integers.) An automorphism T of V is given by an $n\times n$ matrix $\{\overline{t_{ij}}\}$ with $\overline{t_{ij}}\in F_p$ such that det $\overline{t_{ij}}\neq 0$ in F_p. We define "the minimal period $\tau(T)$ of T" by

$$\tau(T)=\min_{\substack{x\in V\\ x\neq 0}}\min\{\nu>0;\ T^\nu x=x\},$$

and put for real numbers $\delta_1, \cdots, \delta_n$ with $0<\delta_j<1$

$$B(\delta_1, \cdots, \delta_n)=\{(x_1, \cdots, x_n)\in V;\ 0\leqq x_j<[\delta_j p]\},$$

where $[u]$ the largest integer not exceeding a real number u.

LEMMA. *Let S be a subset of V satisfying $TS=S$. Then*

$$\left|\frac{|S|[\delta_1 p]\cdots[\delta_n p]}{p^n}-|S\cap B(\delta_1, \cdots, \delta_n)|\right|\leqq\sqrt{\frac{|S|p^n}{\tau(T)}}(\log p+2)^n.$$

PROOF. We write

$$\langle m, x\rangle=\sum_{j=1}^n m_j x_j$$

for $m=(m_1, \cdots, m_n)$, $x=(x_1, \cdots, x_n)$ in V, and define

$$\psi_m(x)=\exp\left(2\pi i\frac{\langle m, x\rangle}{p}\right),$$

so that $\{\psi_m(x)\}_{m\in V}$ is the character group of V. Thus the function

$$f(x)=\begin{cases}1 & x\in S\\ 0 & x\in V\backslash S\end{cases}$$

can be expressed as the finite Fourier series

$$f(x)=\sum_{m\in V}a_m\psi_m(x), \tag{4}$$

where

$$a_m=\frac{1}{p^n}\sum_{x\in V} f(x)\phi_m(-x).$$

We have

$$\begin{aligned} f(T^{-1}x) &= \sum_{m\in V} a_m\phi_m(T^{-1}x) \\ &= \sum_{m\in V} a_m\phi_{mT'^{-1}}(x) \\ &= \sum_{m\in V} a_{mT'}\phi_m(x), \end{aligned}$$

where T' is the transposed matrix of T. Since $TS=S$, it follows from the uniqueness of the expansion (4) that

$$a_m=a_{mT'}=a_{mT'^\nu}=\cdots.$$

Since $mT'^\nu \neq m$ for all $m\neq 0$ and $0<\nu<\tau(T)$, we obtain from Parseval's equality

$$\tau(T)\cdot|a_m|^2=\sum_{\nu=0}^{\tau(T)-1}|a_{mT'^\nu}|^2 \leqq \frac{1}{p^n}\sum_{x\in V}|f(x)|=\frac{|S|}{p^n}.$$

Hence

$$|a_m|\leqq\sqrt{\frac{|S|}{p^n\tau(T)}}, \quad m\neq 0. \tag{5}$$

Now by (4)

$$\sum_{x\in B(\delta_1,\cdots,\delta_n)} f(x)=\sum_{m\in V} a_m \sum_{x\in B(\delta_1,\cdots,\delta_n)}\phi_m(x).$$

Since

$$\begin{aligned} \left|\sum_{x\in B(\delta_1,\cdots,\delta_n)}\phi_m(x)\right| &= \left|\sum_{x_1=0}^{[\delta_1 p]-1}\cdots\sum_{x_n=0}^{[\delta_n p]-1}\exp\left(2\pi i\frac{\sum_{j=0}^{n} m_j x_j}{p}\right)\right| \\ &\leqq p^n\prod_{\substack{j=1\\ m_j\neq 0}}^{n}\frac{1}{\min(m_j,\ p-m_j)}, \end{aligned}$$

we have from (5)

$$\left|\sum_{m\neq 0} a_m\sum_{x\in B(\delta_1,\cdots,\delta_n)}\phi_m(x)\right|\leqq\sqrt{\frac{|S|\cdot p^n}{\tau(T)}}(\log p+2)^n.$$

Viewing that

$$\sum_{x\in B(\delta_1,\cdots,\delta_n)} f(x)=|S\cap B(\delta_1,\cdots,\delta_n)|$$

and

$$a_0\sum_{x\in B(\delta_1,\cdots,\delta_n)}\phi_0(x)=\frac{|S|}{p^n}[\delta_1 p]\cdots[\delta_n p],$$

we obtain

$$\left|\frac{|S|}{p^n}[\delta_1 p]\cdots[\delta_n p]-|S\frown B(\delta_1,\cdots,\delta_n)|\right|$$
$$=\sum_{m\neq 0} a_m \sum_{x\in B(\delta_1,\cdots,\delta_n)} \phi_m(x)$$
$$\leqq\sqrt{\frac{|S|\cdot p^n}{\tau(T)}}(\text{lop}\ p+2)^n\,,$$

which proves Lemma.

COROLLARY. (A. G. Postnikov [2] Ch. 1 §4 Theorem 1.) *If the characteristic equation of T is irreducible over F_p and $x_0\neq 0$, then*

$$\left|N(x_0\,;\,\delta_1,\cdots,\delta_n)-\frac{[\delta_1 p]\cdots[\delta_n p]}{p^n}\right|\leqq 2\sqrt{p^n}\log^n p$$

where $N(x_0\,;\,\delta_1,\cdots,\delta_n)$ is the number of ν, $0<\nu<\tau(T)$ such that $T^\nu x_0\in B(\delta_1,\cdots,\delta_n)$.

PROOF. Put $S=\bigcup_{\nu=0}^{\tau(T)-1} T^\nu x_0$ in Lemma.

Proof of Theorem. Let $\omega_1,\cdots,\omega_n$ be an integral bases of K and ε be a torsion-free unit of K. Then through the expressions

$$\varepsilon\omega_i=\sum_{j=1}^{n} t_{ij}\omega_j \quad (i=1,\cdots,n)$$

ε defines the matrix $\{t_{ij}\}$. Denoting by $\overline{t_{ij}}$ the residue class mod p of t_{ij}, we get an automorphism $T=\{\overline{t_{ij}}\}$ of the vector space $\mathfrak{o}_K/(p)$. We identify $\mathfrak{o}_K/(p)$ and V by the correspondence

$$(x_1,\cdots,x_n)\longleftrightarrow x_1\omega_1+\cdots+x_n\omega_n\,,\quad 0\leqq x_j<p\,.$$

Put $S=\mathfrak{o}_K/(p)\backslash E(\lambda\,;\,(p))$. It is easily seen that $TS=S$. Furthermore there exists a $\delta>0$ such that $S\frown B(\delta,\cdots,\delta)=\phi$ since, by the inequality (1), $B(\delta,\cdots,\delta)\subset E(\lambda\,;\,(p))$ for every p. Then it follows from Lemma that

$$|\mathfrak{o}_K/(p)\backslash E(\lambda\,;\,(p))|=|S|=O\left(\frac{p^n(\log p+2)^{2n}}{\tau(T)}\right)$$

where the O-symbol depends only on λ and the field K. Now we define the set $\mathcal{P}$ of rational primes by

$$\mathcal{P}=\{p\,;\,\tau(T)\geqq\log^{2n+1}p\}$$

so that for $p\in\mathcal{P}$

$$N_K(p)-|E(\lambda\,;\,(p))|=|S|=O\left(\frac{p^n}{\log p}\right)=o(N_K(p))\,.$$

It remains only to prove that the natural density of $\mathcal{P}$ is 1 or equivalently

$$\sum_{\substack{p \notin \mathcal{P} \\ p \leq x}} \log p = o(x)\,, \tag{6}$$

where p runs through rational primes. Note first that

$$\tau(T) = \min_{\mathfrak{p} | p} \tau_{\mathfrak{p}}(\varepsilon)\,,$$

where

$$\tau_{\mathfrak{p}}(\varepsilon) = \min \{\nu > 0\,;\ \varepsilon^{\nu} \equiv 1 \pmod{\mathfrak{p}}\}\ .$$

and the minimum is taken over all prime ideals $\mathfrak{p}$ which devides p. Then

$$\sum_{\substack{\tau(T) < \log^{2n+1} p \\ p \leq x}} \log p \leqq \sum_{\substack{\tau(T) < \log^{2n+1} x \\ p}} \log p$$

$$\leqq \sum_{\tau_{\mathfrak{p}}(\varepsilon) < \log^{2n+1} x} \log N_K \mathfrak{p} \leqq \sum_{\mu < \log^{2n+1} x} \log \Big(\prod_{\tau_{\varepsilon}(\mathfrak{p}) = \mu} N_K \mathfrak{p} \Big)$$

$$\leqq \sum_{\mu < \log^{2n+1} x} \log |N_K(\varepsilon^{\mu} - 1)|$$

(since $\varepsilon^{\mu} - 1 \neq 0$) and

$$|N_K(\varepsilon^{\mu} - 1)| \leqq c''(K)^{\mu}\,.$$

Hence we obtain

$$\sum_{\substack{p \notin \mathcal{P} \\ p \leq x}} \log p = O(\log^{4n+2} x)$$

References

[1] Davenport, H., Linear forms associated with an algebraic number field. Quart. J. Math 3 (1952), 32-41.

[2] Postnikov, A.G., Ergodic problems in the theory of congruences of Diophantine approximations. Proc. Steklov Inst. Math. 82 (English translation) (1966).

Department of Mathematics
Faculty of Engineering
Keio University
3-14-1, Hiyoshi, Kohoku, Yokohama
223 Japan