COLLOQUIUM MATHEMATICUM

VOL. XXXVIII 1978 FASC. 2

NORMAL ORDERS FOR CERTAIN FUNCTIONS ASSOCIATED WITH FACTORIZATIONS IN NUMBER FIELDS

BY

W. NARKIEWICZ AND J. ŚLIWA (WROCŁAW)

1. Let K be an algebraic number field and let $g(a)$ denote the number of distinct lengths of possible factorizations of an integer a of K into irreducibles. We shall mostly be concerned with the value of g at positive rational integers n and we shall prove the following result, answering a question of P. Turán:

THEOREM I. *If the class-number h of K is equal at least to 3, then g has a non-decreasing normal order equal to $C\log\log n$, where C is a positive constant depending on K.*

Note that it was shown recently that the function $f(n)$ giving the number of distinct factorizations of a rational positive integer n into irreducibles in K does not have a non-decreasing normal order except the trivial case $h = 1$ (see [5]).

In the course of proving Theorem I we shall obtain also the following result:

THEOREM II. *Let $g^+(a)$ and $g^-(a)$ denote the maximal and minimal lengths, respectively, of a factorization of a into irreducibles in K. The restrictions of g^+ and g^- to positive rational integers have non-decreasing normal orders equal to $C^+\log\log n$ and $C^-\log\log n$, respectively, where $0 < C^- \leqslant C^+$. If, moreover, $h \geqslant 3$, then $C^- < C^+$.*

Some special cases of Theorem I were obtained earlier in [3]. Another proof of Theorem I was also obtained by S. Allen and P. Pleasants and will appear in Acta Arithmetica. In their paper they note also that the constant λ_1 in our Theorem III may be taken equal to 1.

2. Let $E = X_0, X_1, \ldots, X_{h'}$ ($h' = h-1$) be the classes of the class-group $H(K)$ of K, E being the unit class. For any integer a of K denote by $\Omega_i(a)$ the number of prime ideals from X_i occurring in the factorization of the ideal generated by a into prime ideals.

LEMMA 1. *Each of the functions* $\Omega_i(n)$ $(i = 0, 1, \ldots, h')$ *has a non-decreasing normal order equal to* $a_i \log\log n$ *with positive* a_i.

Proof. Since Ω_i is additive, non-negative and bounded on primes, it has

$$\sum_{p \leqslant n} \Omega_i(p) p^{-1} \qquad (p \text{ being primes})$$

for normal order. But a recent result of Odoni [4] implies

$$\sum_{p \leqslant n} \Omega_i(p) p^{-1} = \big(a_i + o(1)\big) \log\log n.$$

For any integer $a \in K$ we define the type of a as the sequence

$$\langle \Omega_1(a), \Omega_2(a), \ldots, \Omega_{h'}(a) \rangle$$

and let

$$\tau_i = \langle \lambda_{1i}, \lambda_{2i}, \ldots, \lambda_{h'i} \rangle \qquad (i = 1, 2, \ldots, N)$$

be all the types corresponding to irreducible elements. We call two factorizations of a into irreducibles, say

$$a = \pi_1 \pi_2 \ldots \pi_m b_1 b_2 \ldots b_r = \pi_1 \pi_2 \ldots \pi_m c_1 c_2 \ldots c_s$$

(where $\pi_1, \pi_2, \ldots, \pi_m$ are all irreducibles dividing a which generate prime ideals), *similar* provided $r = s$ and after some rearrangement the types of b_j and c_j are the same for $j = 1, 2, \ldots, r$.

Observe now that for any a the classes of similar factorizations of a are in one-to-one correspondence with non-negative integral solutions of the system

$$\sum_{i=1}^{N} x_i \lambda_{ki} = \Omega_k(a) \qquad (k = 1, 2, \ldots, h'). \tag{1}$$

In particular, if $X^+(a)$ denotes the set of all such solutions, then $g^+(a)$, respectively $g^-(a)$, are equal to the sum of $\Omega_0(a)$ and the maximum, respectively the minimum, of the linear form

$$L(x_1, x_2, \ldots, x_N) = x_1 + x_2 + \ldots + x_N$$

on $X^+(a)$, and $g(a)$ equals the number of distinct values attained by that form on $X^+(a)$.

Let $X_R(a)$ be the set of all real solutions of (1), $X_R^+(a)$ the set of all non-negative real solutions, and $X(a) = X_R(a) \cap Z^N$. The set $B = X_R(1)$ is a linear subspace of R^N, $X(1)$ is a lattice in B, $X(a)$ is a coset of $X(1)$, and $X_R(a)$ is the linear variety spanned by it. These observations imply immediately the equalities

$$\max_{X^+(a)} L = \max_{X_R^+(a)} L + O(1) \tag{2}$$

and

$$\min_{X^+(a)} L = \min_{X_R^+(a)} L + O(1), \tag{3}$$

where the constants are independent of a.

LEMMA 2. *To every non-empty subset A of $\{1, 2, \ldots, N\}$ and to each $i = 1, 2, \ldots, h'$ there corresponds a real number $c_i(A)$ such that, with the notation*

$$M_A(a) = \Omega_0(a) + \sum_{i=1}^{h'} c_i(A)\,\Omega_i(a),$$

we have

$$g^+(a) = \max_{\substack{A \subset \{1,2,\ldots,N\} \\ A \neq \emptyset}} M_A(a) + O(1)$$

and

$$g^-(a) = \min_{\substack{A \subset \{1,2,\ldots,N\} \\ A \neq \emptyset}} M_A(a) + O(1).$$

Proof. We consider only $g^+(a)$, the case of $g^-(a)$ being analogous. By (2) and (3) it suffices to evaluate $\max_{X_R^+(a)} L$. Since $X_R^+(a)$ is a polyhedron and L is linear, the maximal value is attained at a vertex, say $P = \langle u_1, u_2, \ldots, u_N \rangle$. At least one of its coordinates vanishes and we may assume that P has the maximal possible number of vanishing coordinates. Let $u_i = 0$ for $i \in A$ and $u_i \neq 0$ for the remaining i's, where A is a subset of $\{1, 2, \ldots, N\}$ of $k > 0$ elements.

If the matrix

$$B_A = (\lambda_{ij})_{\substack{i=1,2,\ldots,h' \\ j \notin A}}$$

had its rank equal at most to $N-k-1$ and if

$$\{1, 2, \ldots, N\} \setminus A = \{j_1, j_2, \ldots, j_{N-k}\},$$

then the system

$$\sum_{s=1}^{N-k} \lambda_{ij_s} z_s = \Omega_i(a) \ (i = 1, 2, \ldots, h'), \qquad z_s \geqslant 0 \ (s = 1, 2, \ldots, N-k)$$

would define an at least one-dimensional polyhedron containing P. The maximal values of L must be attained at a vertex which has at least one vanishing coordinate, and so we get a point at which the maximal value of L is attained and which has more vanishing coordinates than P, in contradiction to the choice of P.

Hence the rank of B_A equals $N-k$, and so we obtain, with suitable $t_{ij} = t_{ij}(A)$, the equalities

$$u_j = \sum_{i=1}^{h'} t_{ij}\,\Omega_i(a).$$

Since

$$L(u_1, \ldots, u_N) = \sum_{i=1}^{h'} \Big(\sum_{j=1}^{N} t_{ij} \Big)\, \Omega_i(a),$$

the lemma follows.

Proof of Theorem II. By Lemma 1, for every positive ε and almost all n we have the inequalities

$$(a_i - \varepsilon)\log\log n \leqslant \Omega_i(n) \leqslant (a_i + \varepsilon)\log\log n \qquad (i = 0, 1, \ldots, h'),$$

whence, for those n and every non-empty $A \subset \{1, 2, \ldots, N\}$,

$$\Big(\sum_{i=1}^{h'} c_i(A)\, a_i - D_1 \varepsilon \Big) \log\log n \leqslant \sum_{i=1}^{h'} c_i(A)\, \Omega_i(n) \leqslant \Big(\sum_{i=1}^{h'} c_i(A)\, a_i + D_2 \varepsilon \Big) \log\log n$$

with certain positive D_1 and D_2 independent of ε and n. Putting now

$$C^+ = a_0 + \max_{A \neq \emptyset} \sum_{i=1}^{h'} c_i(A)\, a_i, \qquad C^- = a_0 + \min_{A \neq \emptyset} \sum_{i=1}^{h'} c_i(A)\, a_i$$

and adjusting the value of ε we infer from Lemma 2 that for almost all n

$$(C^+ - \varepsilon)\log\log n \leqslant g^+(n) + O(1) \leqslant (C^+ + \varepsilon)\log\log n,$$
$$(C^- - \varepsilon)\log\log n \leqslant g^-(n) + O(1) \leqslant (C^- + \varepsilon)\log\log n$$

and it remains to show that C^- is positive. For this purpose observe that, for irreducible π, $\sum_{i=0}^{h'} \Omega_i(\pi)$ is bounded by a constant D independent of π, and thus

$$g^-(n) \geqslant \frac{1}{D} \sum_{i=0}^{h'} \Omega_i(n) \gg \log\log n$$

for almost all n.

Finally, we show that, in the case $h \geqslant 3$, $C^- \neq C^+$. The equality $C^- = C^+$ would imply that, for all positive ε and almost all n,

$$g(n) \leqslant g^+(n) - g^-(n) + 1 \leqslant \varepsilon \log\log n,$$

but it was established in [2] that $g(n) \leqslant k$ implies $\Omega_i(n) \leqslant hk$ for a certain $i > 0$. Thus

$$g(n) \geqslant \frac{1}{h} \min_i \Omega_i(n)$$

and, therefore, $g(n) \geqslant \mu \log\log n$ ($\mu > 0$) holds for almost all n by Lemma 1.

3. Theorem I will be deduced from Theorem II using the following result:

THEOREM III. *If $h \geqslant 3$, then there exist two constants λ_1 and λ_2 such that for almost all n the set of all lengths of factorizations of n in K differs from an arithmetic progression of difference λ_1 by at most λ_2 elements.*

Proof. Define $m > 0$ in Z by $L(X(1)) = mZ$ and put

$$C_0 = \mathrm{Ker} L \cap X(1).$$

(The integer m is positive, for otherwise all factorizations of any integer in K would be of the same length and we would have $h \leqslant 2$.)

For every real r choose $a_r \in B$ with $L(a_r) = rm$. Thus

$$X(1) = \bigcup_{k=-\infty}^{\infty} (a_k + C_0).$$

Now let $\bar{u}_a = \langle u_1, u_2, \ldots, u_N \rangle$ be a fixed element of $X(a)$. Then

$$X(a) = \bar{u}_a + X(1) = \bigcup_{k=-\infty}^{\infty} (\bar{u}_a + a_k + C_0)$$

and

$$L(X(a)) = \{L(\bar{u}_a) + km\colon\ k \in Z,\ (\bar{u}_a + a_k + C_0) \cap Z_+^N \neq \emptyset\}$$

($Z_+^N = \{\langle u_1, u_2, \ldots, u_N \rangle\colon\ u_i \geqslant 0,\ u_i \in Z\}$).

Finally, for $\delta > 0$ put

$$R_\delta^N = \{\langle u_1, u_2, \ldots, u_N \rangle\colon\ u_i \geqslant \delta\ (i = 1, 2, \ldots, N)\}, \quad Z_\delta^N = R_\delta^N \cap Z^N,$$
$$X_{R,\delta}^+(a) = X_R^+(a) \cap R_\delta^N, \quad X_\delta^+(a) = X^+(a) \cap Z_\delta^N.$$

LEMMA 3. *There exists a positive number $\delta = \delta(C_0, X(1))$ such that if for some $k \in Z$ and $x_1, x_2 \in X_\delta^+(a)$ the inequalities*

$$L(x_1) < L(\bar{u}_a) + km < L(x_2)$$

hold, then for a suitable $x_3 \in X^+(a)$ we have $L(x_3) = L(\bar{u}_a) + km$.

Proof. Since $X_{R,\delta}^+(a)$ is convex, we can find y in it with

$$L(y) = km + L(\bar{u}_a),$$

whence $y \in (\bar{u}_a + a_k + C) \cap R_\delta^N$. But the set $\bar{u}_a + a_k + C$ is the linear span of $\bar{u}_a + a_k + C_0$, and so we can find an element x_3 in $\bar{u}_a + a_k + C_0$ (thus in $X^+(a)$) at a bounded distance from y provided δ was chosen sufficiently large.

LEMMA 4. *For every positive δ we can find two positive constants C_1 and C_2 such that if $\Omega_i(a) > C_1$ for $i = 1, 2, \ldots, h'$, then for each element $u \in X^+(a)$ we can find a $u' \in X_\delta^+(a)$ with the distance from u less than C_2.*

Proof. For a large C the condition $\Omega_i(a) \geqslant C$ $(i = 1, 2, \ldots, h')$ ensures that the set $X_\delta^+(a)$ is non-empty. As $X(a)$ is a coset of the lattice $X(1)$, for every point of $X^+(1)$ there is a point of $X_\delta^+(1)$ at a bounded distance provided $X(1)$ does not lie on one of the coordinate-hyperplanes. If this happens, say $\langle x_1, x_2, \ldots, x_N\rangle \in X(1)$ implies $x_1 = 0$, then the type τ_1 occurs the same number of times in every factorization of a given integer, which is clearly a nonsense.

Proof of Theorem III. Let δ be as in Lemma 3 and C_1 as in Lemma 4. Let $\Omega_i(a) > C_1$ $(i = 1, 2, \ldots, h')$ and put

$$t_1 = \min\{t \in Z\colon (\overline{u}_a + a_i + C) \cap Z_\delta^N \neq \emptyset\},$$
$$t_2 = \max\{t \in Z\colon (\overline{u}_a + a_i + C) \cap Z_\delta^N \neq \emptyset\}.$$

Then, by Lemma 3,

$$L\big(X^+(a)\big) = L\big(X_\delta^+(a)\big) \cup L\big(X^+(a) \setminus X_\delta^+(a)\big)$$
$$= \{L(\overline{u}_a) + km\colon t_1 \leqslant k \leqslant t_2\} \cup L\big(X^+(a) \setminus X_\delta^+(a)\big)$$

and by Lemma 4 every value of $L\big(X^+(a) \setminus X_\delta^+(a)\big)$ is of the form $L(\overline{u}_a) + km$ with $k \in Z$, $t_1 - C_3 \leqslant k \leqslant t_2 + C_3$ for some fixed C_3.

Theorem I follows now directly from Theorems II and III.

REFERENCES

[1] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4-th edition, Oxford 1962.

[2] W. Narkiewicz, *On algebraic number fields with non-unique factorization*, Colloquium Mathematicum 12 (1964), p. 59-68.

[3] — *Factorization of natural numbers in some quadratic number fields*, ibidem 16 (1967), p. 257-268.

[4] R. W. K. Odoni, *On a problem of Narkiewicz*, Journal für die reine und angewandte Mathematik 288 (1976), p. 160-167.

[5] J. Rosiński and J. Śliwa, *Number of factorizations in an algebraic number field*, Bulletin de l'Académie Polonaise des Sciences, Série des sciences mathématiques, astronomiques et physiques, 24 (1976), p. 821-826.

INSTITUTE OF MATHEMATICS
WROCŁAW UNIVERSITY

Reçu par la Rédaction le 22. 9. 1976