Normal order for a function associated with factorization into irreducibles

by

W. Narkiewicz (Wroclaw)

In memory of Paul Turán

1. Let \( K \) be an algebraic number field, let \( h \) be its class number, and for any integer \( a \) of \( K \) which is neither 0 nor a unit denote by \( f(a) \) the number of factorizations of \( a \) into irreducible elements. If \( h \) exceeds 1, the function \( f \) becomes nontrivial and one can ask how it behaves. P. Rémond [6] has shown that for \( x \) tending to infinity the sum

\[
\sum_{|V(a)| \leq x} f(a)
\]

taken over a set of nonassociated integers \( a \) is asymptotically equal to \( C_{\exp}(V(\log \log x, \log \log \log x)) \) where \( V(u, v) \) is a polynomial in two variables of degree equal to \( D \), the Davenport constant of the class group of \( K \) and the dominant term equals \( C_{\exp}(\log \log x)^2 \). The constants \( C \) and \( C_{\exp} \) appearing here are both positive and depend on the field \( K \).

Answering a question of P. Turán, J. Rosiński and J. Śliwa [7] proved recently that \( f(a) \), the restriction of \( f \) to positive rational integers, does not have a nondecreasing normal order; in [1], [4] it was shown that for the function \( g(a) \), defined as the number of factorizations of \( a \) in \( K \) with distinct lengths, a nondecreasing normal order exists and may be taken to be equal to \( C_{\log \log n} \), where \( C_{\log \log} \) is again a positive constant depending on \( K \).

In this note we utilize the ideas of [1] and [4] to obtain a nondecreasing normal order, equal to \( C_{\log \log x} \log \log \log x \), for the function \( \log f(a) \) \( (C_{\log \log} = C_{K}(\log \log x) > 0) \). In the case of a quadratic \( K \) with \( h = 2 \) this result (with \( C_2 = 1/k \) was obtained in [3].

2. Let \( E, X_1, \ldots, X_m \) (\( m = h - 1 \)) be the classes of the class group of the field \( K, E \) being the principal class. For any integer \( a \) of \( K \) let \( \omega_k(a) \) be the number of prime ideals from \( X_k \) which divide the ideal gen-
erated by \( \alpha \) and similarly let \( \Omega_{t}(\alpha) \) be the number of those ideals counted according to their multiplicities. We shall need a property of the restrictions of \( \alpha_{t}, \Omega_{t} \) to the set of positive rational integers, which we state as

**Lemma 1.** There exist positive constants \( \mu_{1}, \ldots, \mu_{m} \) such that for \( \alpha = 1, 2, \ldots, m \) and for every real \( t \) one has

\[
\mathcal{N} \left\{ n \leq x : \frac{\Omega_{t}(n) - \mu_{t} \log \log n}{\sqrt{\log n}} \leq t \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} \exp \left\{ -\frac{u^{2}}{2} \right\} du
\]

and

\[
\mathcal{N} \left\{ n \leq x : \frac{\omega_{t}(n) - \mu_{t} \log \log n}{\sqrt{\log n}} \leq t \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} \exp \left\{ -\frac{u^{2}}{2} \right\} du.
\]

**Proof.** Note that the functions \( \omega_{t}(n) \) are strongly additive, \( \Omega_{t}(n) \) are completely additive, and \( \Omega_{t}(p) = \omega_{t}(p) = 1 \), and apply Theorem 4.2 and Lemma 4.1 of I. P. Kubilius [2], utilizing a recent result of R. W. K. Odoni [5], which immediately implies

\[
\sum_{p \leq x} \frac{\Omega_{t}(p)}{p} = [\lambda_{t} + o(1)] \log \log x,
\]

\[
\sum_{p \leq x} \frac{\omega_{t}(p)}{p} = [\lambda_{t} + o(1)] \log \log x
\]

for \( t = 1, 2, \ldots, m \).

**Corollary.** There is a sequence of positive integers \( n_{1} < n_{2} < \ldots \) of density one such that for \( t = 1, 2, \ldots, m \) one has

\[
\lim_{x \to \infty} \frac{\Omega_{t}(n_{k})}{\log \log n_{k}} = \lim_{x \to \infty} \frac{\omega_{t}(n_{k})}{\log \log n_{k}} = \mu_{t} > 0.
\]

A sequence \( \langle Y_{1}, \ldots, Y_{k} \rangle \) of nonprincipal ideal classes is called a complex if the product \( Y_{1} \cdots Y_{k} \) equals \( E \), the principal class. Two complexes differ only in the ordering of their elements will be regarded as identical. A complex is called irreducible provided it does not contain a proper subcomplex. Note that a given complex \( \langle Y_{1}, \ldots, Y_{k} \rangle \) is irreducible if and only if the product \( P_{1}P_{1} \cdots P_{k} \) of prime ideals with \( P_{i} \in Y_{i} \), \( i = 1, 2, \ldots, k \) is generated by an irreducible integer of \( \mathbb{K} \). Observe also that the number of irreducible complexes is finite, because no such complex can contain more than \( h \) elements. (If a finite abelian group of \( n \) elements one takes a sequence of \( n \) elements, then it always has a subsequence with the product equal to the unit element.) Let \( \{ r_{1}, \ldots, r_{m} \} \) be the set of all irreducible complexes and define \( a_{m} \) for \( i = 1, \ldots, N; j = 1, \ldots, m \) as the number of occurrences of the class \( X_{j} \) in the complex \( r_{i} \).

Moreover put

\[
D_{i} = \prod_{j=1}^{m} a_{ij} \!, \quad i = 1, 2, \ldots, N,
\]

and for given nonnegative rational integers \( e_{1}, \ldots, e_{m} \) denote by \( A(e_{1}, \ldots, e_{m}) \) the set of all nonnegative rational solutions \( (t_{1}, \ldots, t_{m}) \) of the system

\[
\sum_{j=1}^{m} a_{ij} t_{j} = e_{j}, \quad j = 1, 2, \ldots, m.
\]

For future reference observe that for \( i = 1, 2, \ldots, N \) the sum \( \sum_{j=1}^{m} a_{ij} \) equals at least 2 because the equality \( \sum_{j=1}^{m} a_{ij} = 1 \) would imply that the complex \( r_{i} \) consists of a single class \( X_{j} \), which is absurd, as then \( X_{j} = E \).

3. We may now obtain the upper and lower bounds for the function \( f(a) \): 

**Lemma 2.** Let \( a \) be an integer of the field \( \mathbb{K} \) satisfying the inequalities \( \omega_{t}(a) > h \) for \( t = 1, 2, \ldots, m \). Then there exist constants

\[
0 \leq \lambda_{1}(a), \ldots, \lambda_{m}(a) \leq h
\]

such that

\[
\mathcal{F} \left( \omega_{1}(a) - \lambda_{1}(a), \ldots, \omega_{m}(a) - \lambda_{m}(a) \right) = f(a) \leq \mathcal{F} \left( \Omega_{1}(a), \ldots, \Omega_{m}(a) \right),
\]

where for given \( s_{1}, \ldots, s_{m} \in \mathbb{Z} \)

\[
\mathcal{F}(s_{1}, \ldots, s_{m}) = \sum_{(t_{1}, \ldots, t_{m}) \in \langle t_{1}, \ldots, t_{m} \rangle} \frac{s_{1}! \cdots s_{m}!}{t_{1}! \cdots t_{m}!} D_{1}^{-t_{1}} \cdots D_{m}^{-t_{m}}.
\]

**Proof.** Consider a factorization

\[
\alpha = \pi_{1} \cdots \pi_{r}
\]

into irreducibles and note that every irreducible element determines an irreducible complex by means of

\[
\langle \pi_{1}, \ldots, \pi_{r} \rangle = p_{1}^{s_{1}} \cdots p_{g}^{s_{g}} \rightarrow \langle \text{class of } p_{1}, \ldots, \text{class of } p_{1}, \ldots, \text{class of } p_{g}, \ldots, \text{class of } p_{g} \rangle
\]

\[
\text{times } s_{1} \text{ times } \cdots \text{times } s_{g} \text{ times }
\]

If now \( t_{i} \) denotes for \( i = 1, 2, \ldots, N \) the number of irreducibles occurring in (2) which determine the irreducible complex \( \pi_{i} \), then obviously

\[
\langle t_{1}, \ldots, t_{N} \rangle \in A \left( \Omega_{1}(a), \ldots, \Omega_{m}(a) \right).
\]

Assume first that for \( i = 1, 2, \ldots, m \) one has \( \omega_{t}(a) = \Omega_{t}(a) = s_{t} \), i.e., the ideal \( \alpha \) is not divisible by the square of a nonprincipal prime ideal, and let \( \langle t_{1}, \ldots, t_{N} \rangle \in A \left( s_{1}, \ldots, s_{m} \right) \). If we write

\[
\alpha = \pi_{1}^{(1)} \cdots \pi_{g}^{(g)} \pi_{m}^{(m)} \pi_{m}^{(m)} \cdots \pi_{m}^{(m)} \quad (2_{i}^{(j)} \in X_{j}),
\]

Moreover put

\[
D_{i} = \prod_{j=1}^{m} a_{ij} \!, \quad i = 1, 2, \ldots, N,
\]
then we find that \( a \) has

\[
\frac{s_1! \ldots s_m!}{\tilde{t}_1! \ldots \tilde{t}_n!} D_{i_1}^{s_1} \ldots D_{i_n}^{s_n}
\]
distinct factorizations corresponding to the same sequence \( \langle t_1, \ldots, t_N \rangle \in T(s_1, \ldots, s_m) \). Indeed, every such factorization is of the form

\[
(a) = \prod_{i=1}^{N} \prod_{j=1}^{m} a_i^{t_j} \prod_{j=1}^{m} \prod_{i=1}^{N} p_{(i,j)}^{(i,j,a_i)}
\]
and so induces permutations of each of the sets \( \{1, \ldots, s_1\}, \{1, \ldots, s_2\}, \ldots, \{1, \ldots, s_m\} \), giving hence \( s_1 s_2 \ldots s_m \) possibilities. However, certain of these permutations correspond to the same factorization. Indeed, inside of each bracket one may permute the prime ideals lying in the same class, and this gives the factor \( D_{i_1}^{t_1} \ldots D_{i_n}^{t_n} \). One may also, for each \( i = 1, \ldots, N \), permute the \( t_i \) brackets corresponding to the same irreducible complex \( \tau_i \), without affecting the factorization, and so finally we arrive at \((4)\).

This proves the lemma in the case where \( a \) is not divisible by the square of a nonprincipal prime ideal, and we see in this case that we may take \( \lambda_i(a) = 0 \) for \( i = 1, 2, \ldots, m \) and we do not have to assume that \( \omega_i(a) > \tilde{h} \).

In the general case let \( I = p_1 \ldots p_n \) be the product of all distinct nonprincipal prime ideals dividing \( a \). Since by our assumption \( \tilde{h} > h \), there is a principal divisor of \( I \), say \( I = p_{1}^{c_1} \ldots p_{n}^{c_n} \), which we may choose such that \( r \) is maximal. Obviously, \( g - r < \tilde{h} \) so \( \tilde{h} > \sum \omega_i(a) - h \).

and if \( \omega_i(a) \) is a generator of \( I_i \), then by the already proved part of the lemma we get

\[
\mathcal{P}(\omega_1(a), \ldots, \omega_m(a)) \leq f(a) \leq f(a);
\]
but

\[
0 \leq \omega_i(a) - \omega_i(a) \leq \tilde{h}
\]
so we may put

\[
\lambda_i(a) = \omega_i(a) - \omega_i(a) \quad (i = 1, 2, \ldots, m).
\]

Finally, let \( a_i \) be any integer of \( K \) satisfying

\[
\Omega_i(a_i) = \omega_i(a) = \lambda_i(a) \quad (i = 1, 2, \ldots, m).
\]

Then by the already proved part of our lemma we get

\[
f(a) \leq f(a) \leq \mathcal{P}(\Omega_1(a_1), \ldots, \Omega_m(a_m)) = \mathcal{P}(\Omega_1(a), \ldots, \Omega_m(a)).
\]

Note that in the case \( \omega_i(a) = \Omega_i(a) \) we have thus obtained an explicit formula for \( f(a) \).

4. The last lemma evaluates the function \( \log \mathcal{P}(s_1, \ldots, s_m) \) under certain conditions:

**Lemma 3.** Let \( T_1 < T_2 < \ldots \) be a sequence of positive numbers tending to infinity, let \( s_i(T) \) be integer-valued functions defined for \( i = 1, 2, \ldots, m \) in such a way that the limit

\[
\lim_{k \to \infty} 
\]
exists and is positive for \( i = 1, 2, \ldots, m \), and put

\[
\mathcal{P}(T) = \mathcal{P}(s_1(T), \ldots, s_m(T))
\]

Then for \( k \) tending to infinity one has

\[
\log \mathcal{P}(T_k) = (A_1 + o(1)) T_k \log T_k
\]

with a certain positive \( A_1 \), depending only on \( A_1, \ldots, A_m \) and the coefficients \( a_{ij} \) of \((1)\).

**Proof.** Write \( \mathcal{A}(T) \) for \( \mathcal{A}(s_1(T), \ldots, s_m(T)) \) and denote by \( \mathcal{M}(T) \) the maximal term in the sum defining \( \mathcal{P}(T) \), thus

\[
\mathcal{M}(T) = \max_{a_{ij} \geq 0, \sum \omega_i(a) - h} s_1(T)^{t_1} \ldots s_m(T)^{t_m} D_{i_1}^{t_1} \ldots D_{i_n}^{t_n}.
\]

As the number of elements of \( \mathcal{A}(T_k) \) is \( O(T_k^k) \), we obtain

\[
\log \mathcal{P}(T_k) = \log \mathcal{M}(T_k) + O(\log T_k)
\]
and so it suffices to prove that \( \log \mathcal{M}(T_k) = (A_1 + o(1)) T_k \log T_k \). Now Stirling's formula shows that for \( \langle t_1, \ldots, t_N \rangle \in \mathcal{A}(T_k) \)

\[
\log \left( \frac{s_1(T_k)! \ldots s_m(T_k)!}{t_1! \ldots t_N!} D_{i_1}^{t_1} \ldots D_{i_n}^{t_n} \right) = \left( \sum_{j=1}^{N} \mathcal{A}_j \right) T_k \log T_k - \sum_{j=1}^{N} \mathcal{A}_j \log T_j + O(T_k)
\]
as \( \sum_{j=1}^{N} t_j = O(T_k) \). Write

\[
\sum_{j=1}^{N} \mathcal{T}_j \log T_j = \sum_{j=1}^{N} \mathcal{T}_j \log T_j + \sum_{j>\mathcal{T}_j} \log T_j = \mathcal{S}_1 + \mathcal{S}_2.
\]

Clearly, \( \mathcal{S}_1 \leq N \frac{T_k}{\log T_k} \log T_k = O(T_k) \) and as \( \frac{T_k}{\log T_k} < t_j = O(T_k) \) implies

\[
\log T_k - \log t_j = O(\log T_k),
\]

\( \mathcal{N} \) - Acta Mathematica XXXVII
we get

$$S_k = \left[ \sum_{j \neq j \in P_k \log T_k} t_j \right] \log T_k + O \left( \left( \sum_{j \geq 1} t_j \right) \log \log T_k \right)$$

$$= \left( \sum_{j = 1}^N t_j \right) \log T_k + O \left( T_k \log \log T_k \right) + O \left( \left( \sum_{j \leq T_k} t_j \right) \log T_k \right)$$

$$= \left( \sum_{j = 1}^N t_j \right) \log T_k + O \left( T_k \log \log T_k \right),$$

which leads to

$$\log M(T_k) = \left( \sum_{j = 1}^m A_j \right) \log T_k - \left( \sum_{j = 1}^m a_j \left( \sum_{j = 1}^N t_j \right) \log T_k + O \left( T_k \log \log T_k \right) \right),$$

hence the equality

$$\sum_{j = 1}^m A_j = \frac{\lambda}{T_0}$$

would imply that for some choice of \( \langle t_1, \ldots, t_N \rangle \in \mathcal{A}(T_k) \) we would have

$$\sum_{j = 1}^m t_j = \left( \sum_{j = 1}^m A_j + o(1) \right) T_k$$

thus

$$\sum_{j = 1}^m t_j \left( \sum_{j = 1}^m a_j - 1 \right) = o(T)$$

but we have seen already that \( \sum_{j = 1}^m t_j \geq 2 \), and so the sum \( \sum_{j = 1}^m t_j \) would be

\( o(T_k) \), which is clearly impossible.

Now we prove our main result:

**Theorem.** If \( K \) is an algebraic number field with class number \( h \neq 1 \) and \( f(n) \) denotes the number of factorizations of \( n \) into irreducible integers of \( K \), then, with a certain constant \( C \) depending on the field \( K \), the function \( C \log \log \log \log n_k \) is a nondecreasing order for \( log \).

**Proof.** Let \( \{ n_k \} \) be the sequence given by the corollary to Lemma 1, let \( T_k = \log \log n_k \) and let \( s_i(T_k) = \Omega_i(n_k) \) for \( i = 1, 2, \ldots, m \). By Lemmas 2 and 3 we infer that

$$\log f(n_k) = \left( A \left( \mu_1, \ldots, \mu_m \right) + o(1) \right) \log \log n_k \log \log \log n_k$$

and similarly, with \( s_i(T_k) = a_i(n_k) - \lambda_i(n_k) \) for \( i = 1, 2, \ldots, m \), we get

$$\log f(n_k) \geq \left( A \left( \mu_1, \ldots, \mu_m \right) + o(1) \right) \log \log n_k \log \log \log n_k.$$
On the distribution function of certain sequences (mod 1)*

by

A. M. Ostrowski (Basel)

To the memory of P. Turán

§ 1. Introduction.

1. This paper arose from the consideration of the expression

\[ R_n(\eta) := R(\eta 12p(1-p)n + pn) + R(\eta 12p(1-p)n - pn) \]

with

\[ 0 < p < 1, \quad \eta > 0, \quad n \to \infty, \]

where \( R(x) \) denotes generally the fractional part of \( x \), lying in \( (0, 1) \).

The expression (1.1) occurs in the Probability Calculus. Namely, as has been shown by Uspensky [7] and Ostrowski [3], the sum

\[ \sum_{n=0}^{\infty} \left\lfloor \frac{n}{\eta} \right\rfloor (1-p)^{n-\left\lfloor \frac{n}{\eta} \right\rfloor} \quad (n-pn \leq \eta 12np(1-p)) \]

can be expressed in the form

\[ \frac{2}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-x^2} dx + e^{-\frac{1}{4p}} \frac{1-R_n(\eta)}{\sqrt{2p(1-p)n}} + O \left( \frac{1}{n} \right) \quad (n \to \infty) \]

where \( R_n \) is given by (1.1).

As a matter of fact a similar formula was first given by Laplace. However, the term \( R_n(\eta) \) was missing in Laplace’s deduction. The formula as it had been written down by Laplace was repeatedly used until the first quarter of this century. It was therefore of importance, that \( R_n(\eta) \) does not tend with \( n \to \infty \) to 0 but is everywhere dense in the interval between 0 and 2. This was announced in [3] and proved in [4].

2. Since, however, very often the sequences in such connection are, not only everywhere dense, but also uniformly distributed that is have a constant density in every point in the corresponding interval, it appears

* Sponsored in part by the Swiss National Science Foundation. Sponsored in part under the Grant DA-EPR-75-G-035 of the European Research Office, U.S.A., to the Institute of Mathematics, University of Basel.