ACTA ARITHMETICA
XXXVII (1980)

Normal order for a function associated with factorization into irreducibles

by

W. NARKIEWICZ (Wrocław)

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

$$\sum_{|N(a)|\leqslant x} f(a)$$

taken over a set of nonassociated integers a is asymptotically equal to $Cx\exp\{V(\log\log x, \log\log\log x)\}$ 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 $C_1(\log\log x)^D$. The constants C and C_1 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 $f(n)$, 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 $g(n)$, defined as the number of factorizations of n in K with distinct lengths, a nondecreasing normal order exists and may be taken to be equal to $C_2\log\log n$, where C_2 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 $C_3\log\log n\log\log\log n$, for the function $\log f(n)$ ($C_3 = C_3(K) > 0$). In the case of a quadratic K with $h = 2$ this result (with $C_3 = 1/4$) 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 $\omega_i(a)$ be the number of prime ideals from X_i which divide the ideal generated by a and similarly let $\Omega_i(a)$ be the number of those ideals counted according to their multiplicities. We shall need a property of the restrictions of ω_i, Ω_i 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 $i = 1, 2, \ldots, m$ and for every real t one has*

$$\mathcal{N}\left\{n \leqslant x:\ \frac{\Omega_i(n)-\mu_i\log\log n}{\sqrt{\log\log n}} \leqslant t\right\} = \frac{1}{\sqrt{2\pi}}\big(x+o(x)\big)\int_{-\infty}^{t}\exp\{-u^2\}\,du$$

and

$$\mathcal{N}\left\{n \leqslant x:\ \frac{\omega_i(n)-\mu_i\log\log n}{\sqrt{\log\log n}} \leqslant t\right\} = \frac{1}{\sqrt{2\pi}}\big(x+o(x)\big)\int_{-\infty}^{t}\exp\{-u^2\}\,du.$$

Proof. Note that the functions $\omega_i(n)$ are strongly additive, $\Omega_i(n)$ are completely additive, and $\Omega_i(p) = \omega_i(p) \leqslant 1$, 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

$$\sum_{p\leqslant x}\frac{\Omega_i(p)}{p} = \big(\lambda_i+o(1)\big)\log\log x,$$

$$\sum_{p\leqslant x}\frac{\omega_i(p)}{p} = \big(\lambda_i+o(1)\big)\log\log x$$

for $i = 1, 2, \ldots, m$.

COROLLARY. *There is a sequence of positive integers $n_1 < n_2 < \ldots$ of density one such that for $i = 1, 2, \ldots, m$ one has*

$$\lim_{k\to\infty}\frac{\Omega_i(n_k)}{\log\log n_k} = \lim_{k\to\infty}\frac{\omega_i(n_k)}{\log\log n_k} = \mu_k > 0. \ ■$$

A sequence $\langle Y_1, \ldots, Y_k\rangle$ of nonprincipal ideal classes is called a *complex* if the product $Y_1 \ldots Y_k$ equals E, the principal class. Two complexes which 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 $P_1P_2\ldots P_k$ of prime ideals with $P_i \in Y_i$ $(i = 1, 2, \ldots, k)$ is generated by an irreducible integer of K. Observe also that the number of irreducible complexes is finite, because no such complex can contain more than h elements. (If in 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 $\{\tau_1, \ldots, \tau_N\}$ be the set of all irreducible complexes and define a_{ij} for $i = 1, \ldots, N$; $j = 1, \ldots, m$ as the number of occurrences of the class X_j in the complex τ_i.

Moreover put

$$D_i = \prod_{j=1}^{m} a_{ij}!, \quad i = 1, 2, \ldots, N,$$

and for given nonnegative rational integers $s_1, \ldots, s_m$ denote by $\Lambda(s_1, \ldots, s_m)$ the set of all nonnegative rational solutions $(t_1, \ldots, t_N)$ of the system

$$(1)\qquad \sum_{i=1}^{N} a_{ij}t_i = s_j, \quad j = 1, 2, \ldots, m.$$

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 τ_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 K satisfying the inequalities $\omega_i(a) > h$ for $i = 1, 2, \ldots, m$. Then there exist constants*

$$0 \leqslant \lambda_1(a), \ldots, \lambda_m(a) \leqslant h$$

such that

$$\Psi\big(\omega_1(a)-\lambda_1(a), \ldots, \omega_m(a)-\lambda_m(a)\big) \leqslant f(a) \leqslant \Psi\big(\Omega_1(a), \ldots, \Omega_m(a)\big),$$

where for given $s_1, \ldots, s_m \in Z$

$$\Psi(s_1, \ldots, s_m) = \sum_{\langle t_1,\ldots,t_m\rangle\in\Lambda(s_1,\ldots,s_m)} \frac{s_1!\ldots s_m!}{t_1!\ldots t_N!}D_1^{-t_1}\ldots D_N^{-t_N}.$$

Proof. Consider a factorization

$$(2)\qquad a = \pi_1 \ldots \pi_r$$

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

$$(\pi_i) = p_1^{b_1}\ldots p_s^{b_s} \to \langle\underbrace{\text{class of } p_1, \ldots, \text{class of } p_1}_{b_1\text{ times}}, \ldots, \underbrace{\text{class of } p_s, \ldots, \text{class of } p_s}_{b_s\text{ times}}\rangle$$

If now t_i denotes for $i = 1, 2, \ldots, N$ the number of irreducibles occurring in (2) which determine the irreducible complex τ_i, then obviously $\langle t_1, \ldots, t_N\rangle \in \Lambda\big(\Omega_1(a), \ldots, \Omega_m(a)\big)$.

Assume first that for $i = 1, 2, \ldots, m$ one has $\omega_i(a) = \Omega_i(a) = s_i$, i.e. the ideal (a) is not divisible by the square of a nonprincipal prime ideal, and let $\langle t_1, \ldots, t_N\rangle \in \Lambda(s_1, \ldots, s_m)$. If we write

$$(3)\qquad (a) = p_1^{(1)}\ldots p_{s_1}^{(1)}\ldots p_1^{(m)}\ldots p_{s_m}^{(m)} \quad (p_i^{(j)} \in X_j),$$

then we find that a has

$$\frac{s_1!\ldots s_m!}{t_1!\ldots t_N!}D_1^{-t_1}\ldots D_N^{-t_N} \tag{4}$$

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

$$(a) = \prod_{i=1}^{N}\prod_{s=1}^{t_i}\Big(\prod_{j=1}^{m}\prod_{r=1}^{a_{ij}} p^{(j)}_{k(r,i,s)}\Big)$$

and so induces permutations of each of the sets $\{1, \ldots, s_1\}$, $\{1, \ldots, s_2\}, \ldots$ $\ldots, \{1, \ldots, s_m\}$, giving hence $s_1!s_2!\ldots s_m!$ possibilities. However, certain of those 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 $D_1^{-t_1}\ldots D_N^{-t_N}$. One may also, for each $i = 1, \ldots, N$, permute the t_i brackets corresponding to the same irreducible complex τ_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 that in this case we may take $\lambda_i(a) = 0$ for $i = 1, 2, \ldots, m$ and we do not have to assume that $\omega_i(a) > h$ holds.

In the general case let $I = p_1\ldots p_g$ be the product of all distinct nonprincipal prime ideals dividing (a). Since by our assumption $g \geqslant h$, there is a principal divisor of I, say $I_0 = p_{i_1}\ldots p_{i_r}$, which we may choose in such a way that r is maximal. Obviously, $g-r < h$, so $r > \sum_{i=1}^{m}\omega_i(a)-h$, and if a_0 is a generator of I_0, then by the already proved part of the lemma we get

$$\Psi\big(\omega_1(a_0), \ldots, \omega_m(a_0)\big) \leqslant f(a_0) \leqslant f(a);$$

but

$$0 \leqslant \omega_i(a)-\omega_i(a_0) \leqslant h$$

so we may put

$$\lambda_i(a) = \omega_i(a)-\omega_i(a_0) \quad (i = 1, 2, \ldots, m).$$

Finally, let a_1 be any integer of K satisfying

$$\Omega_i(a_1) = \omega_i(a_1) = \Omega_i(a) \quad (i = 1, 2, \ldots, m).$$

Then by the already proved part of our lemma we get

$$f(a) \leqslant f(a_1) \leqslant \Psi\big(\Omega_1(a_1), \ldots, \Omega_m(a_m)\big) = \Psi\big(\Omega_1(a), \ldots, \Omega_m(a)\big). \ \blacksquare$$

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 $\log\Psi(s_1, \ldots, s_m)$ 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 $i = 1, 2, \ldots$ $\ldots, m$ in such a way that the limit*

$$\lim_{k\to\infty} s_i(T_k)/T_k = A_i \tag{5}$$

exists and is positive for $i = 1, 2, \ldots, m$, and put

$$\Psi(T) = \Psi\big(s_1(T), \ldots, s_m(T)\big).$$

Then for k tending to infinity one has

$$\log\Psi(T_k) = \big(A+o(1)\big)T_k\log T_k$$

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

Proof. Write $\Lambda(T)$ for $\Lambda\big(s_1(T), \ldots, s_m(T)\big)$ and denote by $M(T)$ the maximal term in the sum defining $\Psi(T)$, thus

$$M(T) = \max_{\langle t_1,\ldots,t_N\rangle\in\Lambda(T)} \frac{s_1(T)!\ldots s_m(T)!}{t_1!\ldots t_N!}D_1^{-t_1}\ldots D_N^{-t_N}. \tag{6}$$

As the number of elements of $\Lambda(T_k)$ is $O(T_k^N)$, we obtain

$$\log\Psi(T_k) = \log M(T_k)+O(\log T_k),$$

and so it suffices to prove that $\log M(T_k) = \big(A+o(1)\big)T_k\log T_k$. Now Stirling's formula shows that for $\langle t_1, \ldots, t_N\rangle \in \Lambda(T_k)$

$$\log\left\{\frac{s_1(T_k)!\ldots s_m(T_k)!}{t_1!\ldots t_N!}D_1^{-t_1}\ldots D_N^{-t_N}\right\} = \Big(\sum_{i=1}^{m}A_i\Big)T_k\log T_k-\sum_{j=1}^{N}t_j\log t_j+O(T_k)$$

as $\sum_{j=1}^{N}t_j = O(T_k)$. Write

$$\sum_{j=1}^{N}t_j\log t_j = \sum_{\substack{j\\ |t_j|\leqslant \frac{T_k}{\log T_k}}} t_j\log t_j + \sum_{\substack{j\\ t_j > \frac{T_k}{\log T_k}}} t_j\log t_j = S_1+S_2.$$

Clearly, $S_1 \leqslant N\dfrac{T_k}{\log T_k}\log T_k = O(T_k)$ and as $\dfrac{T_k}{\log T_k} < t_j = O(T_k)$ implies

$$|\log T_k-\log t_j| = O(\log\log T_k),$$

we get

$$S_2 = \Big(\sum_{\substack{j\\ |t_j| > \frac{T_k}{\log T_k}}} t_j\Big)\log T_k + O\Big(\Big(\sum_{j=1}^{N} t_j\Big)\log\log T_k\Big)$$

$$= \Big(\sum_{j=1}^{N} t_j\Big)\log T_k + O(T_k\log\log T_k) + O\Big(\Big(\sum_{\substack{j\\ |t_j| \leqslant \frac{T_k}{\log T_k}}} t_j\Big)\log T_k\Big)$$

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

which leads to

(7) $$\log M(T_k) = \Big(\sum_{i=1}^{m} A_i\Big) T_k\log T_k - \Big(\min_{\langle t_1,\ldots,t_N\rangle \in A(T_k)} \sum_{j=1}^{N} t_j\Big)\log T_k + O(T_k\log\log T_k).$$

To evaluate the minimum appearing in the last formula note first that if $\hat{A}(T)$ denotes the set of all real nonnegative solutions of (1) with $s_i = s_i(T)$, then (cf. [1])

$$\min_{\langle t_1,\ldots,t_N\rangle \in A(T)} \sum_{j=1}^{N} t_j = \min_{\langle t_1,\ldots,t_N\rangle \in \hat{A}(T)} \sum_{j=1}^{N} t_j + O(1),$$

and secondly, that if T_0 is chosen sufficiently large then

$$\lambda = \min_{\langle t_1,\ldots,t_N\rangle \in \hat{A}(T_0)} \sum_{j=1}^{N} t_j$$

is positive and, as in [1], one arrives at

$$\min_{\langle t_1,\ldots,t_N\rangle \in A(T_k)} \sum_{j=1}^{N} t_j = \big(\lambda + o(1)\big)\frac{T_k}{T_0},$$

so that (7) implies

$$\log M(T_k) = \Big(\sum_{i=1}^{m} A_i - \frac{\lambda}{T_0}\Big) T_k\log T_k + o(T_k\log T_k)$$

and it remains to show that $\sum_{j=1}^{m} A_j > \lambda/T_0$.

Evidently $\sum_{j=1}^{m} A_j \geqslant \lambda/T_0$ and as $\sum_{i=1}^{N} a_{ij}t_i = \big(A_j + o(1)\big)T_k$, we have

$$\sum_{i=1}^{N} t_i \sum_{j=1}^{m} a_{ij} = \Big(\sum_{j=1}^{m} A_j + o(1)\Big) T_k;$$

hence the equality

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

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

$$\sum_{i=1}^{N} t_i = \Big(\sum_{j=1}^{m} A_j + o(1)\Big) T_k$$

thus

$$\sum_{i=1}^{N} t_i\Big(\sum_{j=1}^{m} a_{ij} - 1\Big) = o(T)$$

but we have seen already that $\sum_{j=1}^{m} a_{ij} \geqslant 2$, and so the sum $\sum_{i=1}^{m} t_i$ 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 if $f(n)$ 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 $C\log\log n\log\log\log\log n_k$ is a nondecreasing order for $\log f(n)$.*

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

$$\log f(n_k) \leqslant \big(A(\mu_1,\ldots,\mu_m) + o(1)\big)\log\log n_k\log\log\log\log n_k$$

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

$$\log f(n_k) \geqslant \big(A(\mu_1,\ldots,\mu_m) + o(1)\big)\log\log n_k\log\log\log\log n_k. \blacksquare$$

References

[1] S. Allen and P. A. B. Pleasants, *The number of different lengths of irreducible factorization of a natural number in an algebraic number field*, Acta Arith. 36 (1980), pp. 59–86.

[2] И. П. Кубилюс, *Вероятностные методы в теории чисел*, Вильнюс 1962.

[3] W. Narkiewicz, *Factorization of natural numbers in some quadratic number fields*, Coll. Math. 16 (1967), pp. 257–268.

[4] W. Narkiewicz and J. Śliwa, *Normal orders for certain functions associated with factorizations in number fields*, Coll. Math. 38 (1978), pp. 323–328.

[5] R. W. K. Odoni, *On a problem of Narkiewicz*, Journ. Reine Angew. Math. 288 (1976), pp. 160–167.
[6] P. Rémond, *Étude asymptotique de certaines partitions dans certains semi-groupes*, Ann. Scient. École Norm. Sup. 83 (1966), pp. 343–410.
[7] J. Rosiński and J. Śliwa, *The number of factorizations in an algebraic number field*, Bull. Acad. Pol. Sci., sér. math. phys. et astr. 24 (1976), pp. 821–826.

INSTITUTE OF MATHEMATICS, WROCŁAW UNIVERSITY

Received on 13. 5. 1977
and in revised form on 1. 12. 1977 (940)

ACTA ARITHMETICA
XXXVII (1980)

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

$$(1.1)\qquad R_n(\eta) := R\left(\eta\sqrt{2p(1-p)n}+pn\right)+R\left(\eta\sqrt{2p(1-p)n}-pn\right)$$

with

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

where $R(x)$ denotes generally the fractional part of x, lying in $\langle 0,1)$. The expression (1.1) occurs in the Probability Calculus. Namely, as has been shown by Uspensky [7] and Ostrowski [3], the sum

$$\sum_{\nu=0}^{n}\binom{n}{\nu}p^{\nu}(1-p)^{n-\nu}\qquad \left(|\nu-pn|\leqslant\eta\sqrt{2np(1-p)}\right)$$

can be expressed in the form

$$\frac{2}{\sqrt{\pi}}\int_0^{\eta}e^{-x^2}dx+e^{-\eta^2}\frac{1-R_n(\eta)}{\sqrt{2\pi p(1-p)n}}+O\left(\frac{1}{n}\right)\qquad(n\to\infty)$$

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 annonced 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-ERO-75-G-035 of the European Research Office, U.S.A., to the Institute of Mathematics, University of Basel.