BARUCH Z. MOROZ

On the distribution of integral and prime divisors with equal norms


<http://www.numdam.org/item?id=AIF_1984__34_4_1_0>
ON THE DISTRIBUTION OF INTEGRAL 
AND PRIME DIVISORS 
WITH EQUAL NORMS

by B. Z. MOROZ (*)

This is an exposition of the material presented in my lectures given at 
Orsay in March 1983.

1.

Consider $r$ finite extensions $k_1, \ldots, k_r$ of an algebraic number field $k$, a finite extension of $\mathbb{Q}$, and fix an ideal class $A_j$ in $k_j$, $1 \leq j \leq r$. Let

$$V(A) = \{a | a_j \in A_j, \quad N_{k_i/k}a_1 = \cdots = N_{k_r/k}a_r\}$$

be the set of $r$-tuples of divisors having equal norms. Following E. Hecke, [1], one associates to a divisor of a number field a point in Minkowski space, the real vector space corresponding to this field; we study the distribution of integral and prime divisors in $V(A)$ regarded as points of a real manifold, in the spirit of [1]. For technical reasons we consider here only the case $k = \mathbb{Q}$ (compare [2] and the appendix to this paper).

We use the following notations: $\text{card } S$, or simply $|S|$, denotes the cardinality of a finite set $S$. Let $L$ be an algebraic number field of degree $n$ over $\mathbb{Q}$:

$v$ is the ring of integers of $L$, 
$v^*$ is its group of units, 
$I$ is the group of fractional divisors of $L$, 
$I_0$ is the monoid of integral divisors,

(*) Supported in part by a French Government visiting grant.
2 B. Z. MOROZ

\( \mathcal{P} \) is the set of prime divisors, 
\( S_2 \) and \( S_1 \) are the sets of complex and real places of \( L \), 
\( S = S_1 \cup S_2, \quad |S_j| = : r_j \ (j = 1, 2), \quad n = r_1 + 2r_2, \)

\[ L_w = \begin{cases} \mathbb{R}, & w \in S_1 \\ \mathbb{C}, & w \in S_2 \end{cases} \]

denotes the completion of \( L \) at \( w \in S \),

\[ ||x|| = \begin{cases} |x|, & w \in S_1 \\ |x|^2, & w \in S_2 \end{cases} \quad \text{for} \quad x \in L_w. \]

Let us introduce the algebra \( X = \prod_{w \in S} L_w \) of dimension \( n \) over \( \mathbb{R} \),

referred to as Minkowski space associated with \( L \). Let \( \psi : L \to X \) be

the componentwise embedding of \( L \) in \( X \). The group \( \mathfrak{u}^* \) of units acts

freely as a discrete group of transformations on the multiplicative group 
\( X^* = \prod_{w \in S} L_w^* \) of non-zero elements of \( X \); let 
\( Y = X^*/\psi(\mathfrak{u}^*) \) be the group

of its orbits. E. Hecke, [1], introduces « ideal numbers » (compare also, [3]-
[6]) and defines Größencharaktere to be able to study the distribution of

integral and prime divisors among the areas of \( Y \). We recall this

coloration, as well as the results of [3]-[5] to be generalized here. Let \( N : 
X \to \mathbb{R}_+ \) and \( N^{-1} : \mathbb{R}_+ \to X \) denote the norm map \( N : x \to \prod_{w \in S} ||x_w|| \)

and its right inverse \( N^{-1} : t \to (t^{1/n}, \ldots, t^{1/n}) \). Since \( N \) is trivial on

\( X(\mathfrak{u}^*) \), one obtains \( Y = \mathbb{R}_+ \times Y_0 \), where

\[ Y_0 : = X_0/\psi(\mathfrak{u}^*), \quad X_0 : = \{ x \mid x \in X, N(x) = 1 \}. \]

Let \( \tilde{Y}_0 \) be the group of characters of \( Y_0 \) and \( \lambda \in \tilde{Y}_0 \); one can regard \( \lambda \)

as a character of \( X^* \) trivial on \( \psi(\mathfrak{u}^*) \) and on \( N^{-1} \mathbb{R}_+ \). Thus

\[ \lambda(x) = \prod_{w \in S} ||x_w||^{a_w} \left( \frac{x_w}{|x_w|} \right)^{a_w}, \]

where \( a_w \in \mathbb{Z}, \quad t_w \in \mathbb{R}, \quad x_w \) denotes the projection of \( x \) on \( L_w \), and, 

moreover, \( \lambda(\varepsilon x) = \lambda(x) \) for \( \varepsilon \in \psi(\mathfrak{u}^*) \),

\[ \sum_{w \in S_1} t_w + 2 \sum_{w \in S_2} t_w = 0, \quad a_w \in \{0, 1\} \quad \text{for} \quad w \in S_1. \]

It follows from the Dirichlet theorem on units (compare [1], [6]) that
\( Y = \mathbb{R}_+ \times \mathcal{I}_L \times (\mathbb{Z}/2\mathbb{Z})^0 \), where \( \mathcal{I}_L \) is a torus of dimension \( n - 1 \),

and \( r_0 \leq r_1 \). Therefore, \( \tilde{Y}_0 \cong Z^{n-1} \times (\mathbb{Z}/2\mathbb{Z})^0 \), and there exist
characters \( \lambda_1, \ldots, \lambda_{n-1} \) multiplicatively independent over \( \mathbb{Z} \) and such
that any $\lambda \in \mathcal{Y}_0$ has the form

$$\lambda = \prod_{v=1}^{n-1} \lambda_v^{m_v} \lambda', \quad m_v \in \mathbb{Z},$$

where $\lambda'(x) = \prod_{w \in S} \left(\frac{x_w}{|x_w|}\right)^{a_w}$, $a_w \in \{0,1\}$. The map $\psi$ induces an embedding

$$\varphi : L^* / o^* \to Y$$

of the group of principal divisors $L^*/o^*$ of $L$ in $Y$. Composing $\varphi$ with the projection of $Y$ on $\mathbb{R}^+ \times X_L$ one obtains an embedding

$$\varphi_0 : L^*/o^* \to \mathbb{R}^+ \times X_L.$$ 

Since the group $H := I/L^*$ of ideal classes is finite, one can define an embedding

$$f : I \to \mathbb{R}^+ \times X_L$$

which coincides with $\varphi_0$ on $L^*/o^*$. It follows from the work cited above (see, in particular, [1] and [3]-[5]) that both integral and prime divisors are asymptotically equidistributed when identified by means of (3) with points of the real manifold $\mathbb{R}^+ \times X_L$. To be more precise, let us introduce a parametrisation of $X_L$ induced by the basic characters $\lambda_j(x) = \exp(2\pi i \varphi_j(x))$, $1 \leq j \leq n - 1$, $0 \leq \varphi_j(x) < 1$, and identify a point $x \in X_L$ with its image $(\lambda_1(x), \ldots, \lambda_{n-1}(x)) \in T^{n-1}$, where $T$ denotes the unit circle in $\mathbb{C}^*$. We call a subset

$$\tau = \{x | \lambda_j \leq \varphi_j(x) < \lambda_j + \delta_j, 1 \leq j \leq n-1\}$$

of $X_L$ elementary whenever $0 \leq \lambda_j < \lambda_j + \delta_j < 1$. A set $\tau \subseteq X_L$ is called smooth if there exists a constant $C(\tau) > 0$ such that for every $\Delta > 0$ one can find a system $t = \{\tau_v\}$ of elementary sets with the following properties: card $t < \Delta^{-(n-1)}$,

$$\tau_v \cap \tau_{v'} = \emptyset \quad \text{for} \quad v \neq v', \quad \tau \subseteq \bigcup_{\tau_v \in t} \tau_v, \quad \text{mes}\left(\bigcup_{\tau_v \in t} \tau_v \cap \partial \tau\right) < C(\tau)\Delta,$$

where mes is the normalized Haar measure on $X_L$ (so that mes$(I_L)$ = 1) and $\partial \tau$ denotes the boundary of $\tau$. The following theorem has been proved by J. P. Kubilius, [4], and, a few years later, by T. Mitsui, [5].
THEOREM 1. — For any smooth set $\tau \subseteq \mathcal{I}_L$ and any ideal class $A \in H$

$$\text{card} \{a | a \in I_0, \ f(a) \in (0,x) \times \tau, \ a \in A\} = \frac{\omega_L \text{mes} (\tau)}{h} x + O(x^{1-\varepsilon})$$

$$\text{card} \{p | p \in \mathcal{P}, \ f(p) \in (0,x) \times \tau, \ p \in A\}$$

$$= \frac{\text{mes} (\tau)}{h} \int_x^\infty \frac{dx}{\log x} + O(\exp (-c_2 \sqrt{\log x} x),$$

where the constants $c_1, c_2 > 0$ depend on $L$, but not on $x \to \infty$, and $\omega_L$ denotes the residue of the zeta-function of $L$ at $s = 1$, $h = |H|$ is the class number of $L$.

The characters $\mu_j = \lambda_j \circ f$ are called basic Größencharaktere; the group

$$\hat{H} = \left\{ \mu | \mu = \chi \prod_{j=1}^{n-1} \mu_j^{m_j}, \ m_j \in \mathbb{Z}, \ \chi \in \hat{H} \right\},$$

where $\hat{H}$ is the group of ideal class characters, can be identified (see, e.g., [6]) with the set of unramified idele-class characters trivial on $R_+$. The map

$$(3') \quad g': I \to R_+ \times \mathbb{T}^{n-1}$$

given by

$$g': a \mapsto (N_{L/Q} a, \mu_1(a), \ldots, \mu_{n-1}(a))$$

is compatible with (3) under the above identification of $\mathcal{I}_L$ and $\mathbb{T}^{n-1}$. Theorem 1 may be viewed as a multidimensional equidistribution principle, in the spirit of the classic memoir of Hecke’s, [1]. We should like to refer to [8], [9], [10] for some applications of this principle. One can improve the error term in the second formula using the method of trigonometric sums (see, [3], chapter 2, and [7]). About thirty years ago Yu. V. Linnik suggested (and communicated to his colleagues and students, [11]) that one could generalize Theorem 1 to treat the integral and prime divisors in $V(A)$. As an example of this programme (compare [2] and references therein), we prove here the following result. Let $I_0$, $\mathcal{P}_j$, $\mathcal{I}_j$ and $h_j$ denote the monoid of integral divisors, the set of prime divisors, the torus $\mathcal{I}_{k_j}$ and the class number of $k_j$ respectively; let $h = \prod_{j=1}^r h_j$ and $\mathcal{I} = \mathcal{I}_1 \times \cdots \times \mathcal{I}_r$, moreover, let $\mathcal{P} = \{p | p_j \in \mathcal{P}_j\}$ and $I_0 = \{a | a_j \in I_0\}$ be the sets of $r$-tuples of prime and integral divisors.
respectively; let $K = k_1 \ldots k_r$ be the composite of the fields $k_1, \ldots, k_r$, let $n_j$ and $D_j$ be the degree $[k_j : \mathbb{Q}]$ and the discriminant of $k_j$ and $n$ be the degree $[K : \mathbb{Q}]$ of $K$. Consider the map

$$g_j : \mathcal{I}_0^j \to \mathcal{I}_j$$

induced by the embedding $(3')$, so that, when $\mathcal{I}_j$ is identified with $\mathbb{T}_j^{n_j-1}$,

$$g_j : a_j \mapsto (\mu_{j1}(a_j), \ldots, \mu_{j(n_j-1)}(a_j)), \quad a_j \in \mathcal{I}_0^j,$$

where $\{\mu_{j\ell} | 1 \leq \ell \leq n_j - 1\}$ is the set of basic Größencharaktere of $k_j$, $j = 1, \ldots, r$, and introduce a zeta-function

$$Z(k_1, \ldots, k_r; s) = \sum_{m=1}^{\infty} a_m^{(1)} \ldots a_m^{(r)} m^{-s},$$

where $a_m = \text{card} \{a_j | a_j \in \mathcal{I}_0^j, N_{k_j/\mathbb{Q}} a_j = m\}$ is the number of integral divisors of $k_j$ whose norm is equal to $m$. One can show (see [12], [13]) that if $n = \prod_{j=1}^{r} n_j$, then

$$Z(k_1, \ldots, k_r; s) = \frac{Z_K(s)}{L(s, \Phi)},$$

where $L(s, \Phi) = \prod_p \Phi(p^{-s})^{-1}$, $\Phi(p)(t)$ is a rational function of $t$, $p$ varies over rational primes, and, moreover, $\Phi(p)(p^{-s}) \neq 0$, $\infty$ for $\text{Re } s > \frac{1}{2}$; for almost all $p$ the function $\Phi(p)(t)$ is a polynomial of degree not larger than $n - 1$ and such that $\Phi(p)(0) = 1$, $\frac{d}{dt} \Phi(p)|_{t=0} = 0$. In particular, the Euler product

$$L(s, \Phi) = \prod_p \Phi(p)(p^{-s})^{-1}$$

converges absolutely for $\text{Re } s > \frac{1}{2}$.

**Theorem 2.** If $k_j$ is Galois over $\mathbb{Q}$ for every $j$, $n = \prod_{j=1}^{r} n_j$ and $(D_j, D_{\ell}) = 1$ for $j \neq \ell$ (the discriminants are pairwise coprime), then for
any smooth set $\tau \subseteq \mathfrak{T}$ one has

$$\text{card}\{a | a \in V(A) \cap I_0, |a| < x, g(a) \in \tau\} = \frac{\omega_k \operatorname{mes}(\tau)}{hL(1, \Phi)} x + O(x^{1-c_1})$$

$$\text{card}\{p | p \in V(A) \cap \mathfrak{P}, |p| = x, g(p) \in \tau\} = \frac{\operatorname{mes}(\tau)}{h} li(x) + O(x \exp(-c_2\sqrt{\log x}))$$

for some $c_1, c_2 > 0$ depending on $k_1, \ldots, k_r$, but not on $x \to \infty$, where

$$|a| := \left(\sum_{j=1}^{r} N_{k_j|Q} a_j\right)^{1/r} \text{ for } a = \{a_1, \ldots, a_r | a_j \in I_0\},$$

and

$$li(x) := \int_{2}^{x} \frac{du}{\log u}; \quad g = (g_1, \ldots, g_r).$$

One can view Theorem 2 as a statement about statistical independence of the fields $k_1, \ldots, k_r$. To be more precise, let

$$\tau = \tau_1 \times \cdots \times \tau_r, \quad \tau_j \subseteq \mathfrak{T}_j,$$

then (under the above assumptions) the probability to find $a \in V(A)$ with $g(a) \in \tau$ is equal to the product of the probabilities that $a_j \in A_j$ and $g_j(a_j) \in \tau_j$, $j = 1, \ldots, r$. Thus the condition

$$N_{k_1|Q} a_1 = \cdots = N_{k_r|Q} a_r \tag{6}$$

affects the probability of the event:

$$\langle a_1 \in A_1, \ldots, a_r \in A_r, g_1(a_1) \in \tau_1, \ldots, g_r(a_r) \in \tau_r \rangle$$

neither for $r$-tuples of integral, nor of prime divisors. On the other hand, Theorem 2 may be regarded as an assertions on representation of integers by decomposable forms. As a special case of this theorem ($n_1 = \cdots = n_r = 2$), one obtains the following result.

**Proposition 3.** — Let $f_1, \ldots, f_r$ be binary positive definite primitive quadratic forms with pairwise co-prime fundamental discriminants. Then the number of integral solutions

$$(x_1, x_2, \ldots, x_{2r-1}, x_{2r})$$
of the system of equations
\[ f_1(x_1, x_2) = \cdots = f_r(x_{2r-1}, x_{2r}) \]
subject to the condition \( f_1(x_1, x_2) \leq N \) is equal to
\[ AN + O(N^{1-c}) \]
for some \( A > 0, \ c > 0 \) independent on \( N \).

It turns out that for two quadratic fields \((n_1 = n_2 = r = 2)\)
\[ L(s, \Phi) = L(2s, \chi_0), \]
where \( \chi_0(n) = \left( \frac{D_1D_2}{n} \right) \) (see, e.g., [13], §5). Therefore we obtain the following result.

**Proposition 4.** — Let \( k_j = \mathbb{Q}(\sqrt{D_j}), \ j = 1, 2, \ (D_1, D_2) = 1. \) Then
\[ \text{card} \{a | a \in V(A) \cap I_0, |a| < x, g(a) \in \tau\} = \frac{\omega_K \text{mes} (\tau)}{hL(2, \chi_0)} x + O(x^{1-c}) \]
with \( c_1 > 0 \) independent on \( x \).

We remark finally that the O-constants depend on \( \tau \) only through the «constant of smoothness» \( C(\tau) \), as can be readily observed from the proof of Theorem 2 given below.

2.

Further on we write \( I_0(K), \ \mathcal{P}(K), \ H(K), \ \mu(K) \) for the monoid of the integral divisors, set of prime divisors, class group and the set of basic Größencharaktere of \( K \). Theorem 2 will be deduced from the following four lemmas.

**Lemma 1.** — Let \( \varphi_1, \ \varphi_2, \ \varepsilon \) satisfy the inequalities
\[ 0 \leq \varphi_1 - \varepsilon < \varphi_1 < \varphi_2 < \varphi_2 + \varepsilon \leq 1. \]
There exists a real valued function \( f \in C^\infty[0,1] \) such that \( 0 \leq f(t) \leq 1 \) for \( t \in [0,1], \ f(t) = 1 \) for \( t \in [\varphi_1, \varphi_2], \ f(t) = 0 \) for \( t \notin [\varphi_1 - \varepsilon, \varphi_2 + \varepsilon] \),
This is a well-known lemma of elementary calculus; we choose one of such functions to be denoted by \( f(\varphi_1, \varphi_2, \varepsilon; \cdot) \).

Let \( C_j, C_k \) be the idele class groups of \( k_j, K \), and \( \chi_j \) be an idele class character of \( k_j \) trivial on \( \mathbb{R}_+ \); we define an idele class character

\[
\chi := \prod_{j=1}^{r} \chi_j \circ N_{K/k_j}
\]

in \( K \), and an L-function

\[
L(\chi_1, \ldots, \chi_r; s) := \sum_{a \in V} \chi_1(a_1) \cdots \chi_r(a_r)|a|^{-s},
\]

where \( V = \{a | a_j \in I_0^d, N_{k_j/k_0}a_1 = \cdots = N_{k_j/k_0}a_r \} \).

**Lemma 2.** If \( n = \prod_{j=1}^{r} n_j \), then \( L(\chi_1, \ldots, \chi_r; s) = L(s, \chi)L(s, \Phi)^{-1} \),
where \( L(s, \chi) = \sum_{a \in I_0(k)} \chi(a)N_{k_0/k}a^{-s} \) for \( \Re s > 1 \), and \( L(s, \Phi) \) as defined in (5) with \( \Phi(p) \) depending on \( \chi_1, \ldots, \chi_r \) and having the properties similar to those of the polynomials in (5).

This follows from the results cited before, [12] (or [13]).

**Lemma 3.** Let \( n = \prod_{j=1}^{r} n_j \), then

\[
\sum_{a \in V, |a| < x} \chi_1(a_1) \cdots \chi_r(a_r) = g(\chi) \frac{\omega_{k_1}}{L(1, \Phi)} + O(a(\chi)^{\frac{3n+1}{2}} x^{1-c_1}),
\]

\[
\sum_{a \in V \cap \mathcal{P}, |a| < x} \chi_1(a_1) \cdots \chi_r(a_r) = g(\chi) \int_{2}^{x} \frac{dx}{\log x} + O\left( x \exp \left( - c_2 \frac{\log x}{\log a(\chi) + \sqrt{\log x}} \right) \right)
\]
where \( c_1, c_2 > 0, \) \( g(\chi) = \begin{cases} 0, & \chi \neq 1 \\ 1, & \chi = 1 \end{cases} \) the O-constants and \( c_1, c_2 \) depend on \( k_1, \ldots, k_r, \) but not on \( \chi_1, \ldots, \chi_r \) unless \( \chi^2 = 1, \) nor on \( x; \) 

\[
\sum_{w \in S} (|a_w| + |b_w|) = : a(\chi), \quad \text{when } \chi \text{ is given by}
\]

\[
\chi(\alpha) = \prod_{w \in S} \left( \frac{\alpha_w}{|\alpha_w|} \right)^{\omega_w} |\alpha_w|^{ib_w}
\]

for \( \alpha \equiv 1 \pmod{f(\chi)}, \alpha \in K^{*}, a_w \in Z, b_w \in R; \alpha_w \) denotes the image of \( \alpha \) in \( K_w \) for \( w \in S \) and \( f(\chi) \) is the conductor of \( \chi. \)

**Proof.** — To prove (9) one remarks (see, e.g., [14], Lemma 1) that for any \( a \in V \cap \mathcal{P} \) satisfying the condition \( |a| = q \) is a rational prime \( \) there exists one and only one prime \( p \in \mathcal{P}(K) \) such that \( N_{K/Q} p = a. \)

Therefore,

\[
\sum_{a \in V \cap \mathcal{P}, |a| < x} \chi_1(a_1) \ldots \chi_r(a_r) = \sum_{a \in V \cap \mathcal{P}, |a| = q} \chi_1(a_1) \ldots \chi_r(a_r) + O(x^{1/2})
\]

\[
= \sum_{p \in \mathcal{P}(K), N_{K/Q} p < x} \chi(p) + O(x^{1/2})
\]

and (9) follows from estimates obtained in the work cited above (see [4], ch. I, § 5, lemma 4, or [5], § 2, lemma 6) (*) By a standard argument one obtains (see, e.g., [15], lemma 3.12)

\[
A(x) := \sum_{a \in V, |a| < x} \chi_1(a_1) \ldots \chi_r(a_r) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{x^s}{s} L(\chi_1, \ldots, \chi_r, s) \, ds + O_\varepsilon \left( \frac{x^{1+\varepsilon}}{T} \right),
\]

where \( c = 1 + (\log x)^{-1}, \) \( T > 0. \) It follows from lemma 2 that

\[
A(x) = \frac{1}{2\pi i} \int_{1/2+\varepsilon-iT}^{1/2+\varepsilon+iT} \frac{x^s}{s} L(s, \chi)L(s, \Phi)^{-1} \, ds + g(\chi) \frac{\omega_x x}{L(1, \Phi)}
\]

\[
+ O_\varepsilon \left( \frac{x^{1+\varepsilon}}{T} \right) + O_\varepsilon \left( \int_{1/2+\varepsilon}^{c} \left( |L(\sigma+iT, \chi)| + |L(\sigma-it, \chi)| \right) \frac{x^s}{T} \, d\sigma \right)
\]

because \( L(s, \Phi)^{-1} = O_\varepsilon(1) \) for \( \text{Re } s > \frac{1}{2} + \varepsilon. \)

(*) Alternatively one can deduce (9) from lemma 2.
By a Phragmén-Lindelöf type of argument (compare, [6], pp. 92-93 and [5], pp. 14-15) one deduces from the functional equation for $L(s, \chi)$ and Stirling’s formula for the $\Gamma$-function an estimate

\[(11) \quad L(s + it, \chi) = O_e \left( (1 + |t|)^{3/2} a(\chi)^{3/2 + \varepsilon} \right) \]

in the region $0 \leq \sigma \leq c$. Substitution of (11) into the estimate for $A(x)$ we have just written out leads to (8).

**Lemma 4.** — Let $k_j$ be Galois over $\mathbb{Q}$ for each $j$, $n = \prod_{j=1}^{r} n_j$, $(D_j, D_r) = 1$ for $j \neq r$, $\chi = 1$, and $\chi_j$ be unramified for each $j$. Then $\chi_j = 1$ for every $j$.

**Proof.** — Let us assume first that $\chi_j$ is of finite order for every $j$; then, being unramified, it is an ideal class character. One can deduce from class field theory, [17], that (under the above conditions)

\[\{(N_{k_j/k_1}A, \ldots, N_{k_j/k_r}A)|A \in H_k\} = H_1 \times \cdots \times H_r,\]

where $H_j$ is the ideal class group of $k_j$; in particular, for any $A_j \in H_j$ there exists $A \in H_k$ such that $N_{k_j/k}A = A_j$; $N_{k_j/k}A = 1$ for $\ell \neq j$. If $\chi = 1$, then

\[1 = \prod_{\ell=1}^{r} (\chi_\ell \circ N_{k_j/k})(A) = \chi_j(A_j);\]

and we see that $\chi_j = 1$. Assuming $\chi = 1$ we deduce, now that $\chi_j$ is of finite order for any $j$. Let $G_j$ be the Galois group of $k_j$ and $G$ be the Galois group of $K$; since $n = \prod_{j=1}^{r} n_j$, we have $G \cong G_1 \times \cdots \times G_r$.

The character

\[(\chi_j \circ N_{k_j/k})^{-1} = \prod_{\ell \neq j} \chi_\ell \circ N_{k_j/k}\]

is, therefore, $G_j$-invariant; since $[C_j : N_{k_j/k}C_K] = d_j$ is finite, we see that $\chi_j^{d_j}$ is $G_j$-invariant. Take $p \in \mathcal{P}_j$; since $\chi_j^{d_j}(p) = \chi_j^{d_j}(p^\gamma)$ for $\gamma \in G_j$, we see that $(\chi_j(p))^{d_j} = (\chi_j(p))^{d_j}$, where $N_{k_j/k}p = p^{d_j}$. But any idèle class character in $\mathbb{Q}$ is of finite order, and it follows, therefore, that $\chi_j^{d_j} = 1$ for some $\ell$. 
3.

Theorem 2 can be deduced from lemma 3 and lemma 4 on purely formal lines. It is an easy consequence of these lemmas and the following form of the Weyl's equidistribution principle (compare [1], p. 37, and [18], Satz 3). To state it we appeal to lemma 1 and write

\[ f(\phi_1, \phi_2, e; t) = \sum_{n=-\infty}^{\infty} c_n \exp(2\pi i nt), \]

so that

\[ c_0 = (\phi_2 - \phi_1) + O(e), \quad c_n = O\left( \frac{1}{|n|^k e^{-1}} \right) \]

for any fixed integral \( k \geq 1 \).

**Proposition 5.** — Let

\[ \mathcal{I} = \{\exp(2\pi i \phi_1), \ldots, \exp(2\pi i \phi_m)|0 \leq \phi_j < 1, j = 1, \ldots, m\} \]

be a torus of dimension \( m \); \( \tau \) be a smooth subset of \( \mathcal{I} \), \( G \) be a finite Abelian group with the group of characters \( \hat{G} \) and

\[ \mathcal{F} = \{\lambda^1 \ldots \lambda^m | \ell_j \in \mathbb{Z}, \lambda_j : x \mapsto x_j\} \]

be the group of characters of \( \mathcal{I} \), \( x = (\ldots, \exp(2\pi i \phi_j) = x_j, \ldots) \in \mathcal{I} \). Consider a set \( W \) and three maps:

\[ g_1 : W \to \mathcal{I}, \quad g_2 : W \to G, \quad N : W \to \mathbb{R}_+; \]

we denote by \( \hat{W} \) the set of functions on \( W \) defined by

\[ \hat{W} = \{\mu|\mu(a) = (\lambda \circ g_1)(a)(\lambda' \circ g_2)(a), \lambda \in \mathcal{F}, \lambda' \in \hat{G}\}, \]

where \( a \) varies over the elements of \( W \). If

\[ \sum_{N a < x} \chi(a) = g(\chi) A(x) + O(xB(x, a(\chi)^{-1}) \]

for \( \chi \in \hat{W} \), where

\[ g(\chi) = \begin{cases} 1, & \lambda = 1 \text{ and } \lambda' = 1; \\ 0, & \text{otherwise} \end{cases}, \quad A(x) = O(x), \quad a(\chi) = \sum_{j=1}^{m} |\ell_j| \]
for
\[ \chi = (\lambda \circ g_1)(\lambda' \circ g_2), \quad \lambda', \lambda \in \hat{G}, \quad \lambda = \prod_{j=1}^{m} \lambda_j, \]

then for any smooth subset \( \tau \) of \( \mathcal{I} \) and any \( \gamma \in G \) we have

\( \text{(14)} \) \( \text{card} \{a | a \in W, g_2(a) = \gamma, g_1(a) \in \tau, Na < x\} \)
\[ = A(x) \frac{\text{mes} (\tau)}{|G|} + O\left(\frac{x}{b(x)}\right), \]

where \( b(x) \) can be chosen to be equal to \( b_1(x)^v \) with \( v > 0 \), and \( b_1(x) \) is determined by

\[ \sum_{\ell_1, \ldots, \ell_m = -\infty}^{\infty} \frac{1}{B(x, a(\ell))} \alpha(\ell) = b_1(x)^{-1}, \quad a(\ell) = \sum_{j=1}^{m} |\ell_j| \]

with \( \alpha(\ell) = \prod_{j=1}^{m} \alpha_j(\ell_j), \quad \alpha_j(\ell_j) = \begin{cases} 1, & \ell_j = 0 \\ \ell_j^{-k}, & \ell_j \neq 0 \end{cases}, \) \( k \) can be chosen to be any positive integer.

**Proof.** — We deduce (14) from (13) for rectangular \( \tau \) by means of lemma 1 and then prove (14) for any smooth \( \tau \subseteq \mathcal{I} \). Let

\[ \tau = \{\varphi | \psi_j < \varphi_j < \psi_j + \delta_j, j = 1, \ldots, m\}. \]

Choose \( \varepsilon > 0 \) and set (using notations of lemma 1)

\[ f_j^+ (\varphi_j) = f (\psi_j, \psi_j + \delta_j, \varepsilon; \varphi_j), \quad f_j^- (\varphi_j) = f (\psi_j - \varepsilon, \psi_j + \delta_j, \varepsilon; \varphi_j), \]

\[ F^\pm = \prod_{j=1}^{m} f_j^\pm. \]

Let \( \mathcal{N} \) denote the left hand side in (14). Obviously,

\[ \sum_{Na < x}^{} F^-(g_1(a)) \leq \mathcal{N} \leq \sum_{Na < x}^{} F^+(g_1(a)). \]

On the other hand,

\[ \text{(16)} \sum_{Na < x}^{} \sum_{\gamma \in G} \frac{\chi(\gamma)}{|G|} F^\pm (g_1(a)) \chi(g_2(a)). \]
Write $f^\pm_j(t) = \sum_{n=\pm \infty}^{\infty} c^\pm_{nj} \exp(2\pi i nt)$ and denote the left hand side in (16) by $N^\pm$. It follows from (16) that

$$N^\pm = \sum_{\mu \in \mathcal{W}} c^\pm(\mu) \sum_{n < x} \mu(n),$$

where

$$c^\pm(\mu) = \frac{1}{|G|} \overline{\chi(\gamma)} \prod_{j=1}^{m} c^\pm_{\delta_j} \quad \text{for} \quad \mu = ((\lambda_{m}^{1} \ldots \lambda_{m}^{m}) \circ g_1)(\chi \circ g_2).$$

Equation (13) and estimate (12) give

$$N^\pm = \frac{1}{|G|} \left( \prod_{j=1}^{m} \delta_j \right) A(x) + O(x\varepsilon) + \sum_{\mu \in \mathcal{W}, \mu \neq 1} |c^\pm(\mu)| \left| \sum_{n < x} \mu(n) \right|$$

$$= A(x) \frac{\operatorname{mes}(\tau)}{|G|} + O(x\varepsilon) + O\left( \sum_{\mu \in \mathcal{W}} |c^\pm(\mu)| \right) B(x,a(\mu))^{-1} x.$$  

Thus

$$N^\pm = A(x) \frac{\operatorname{mes}(\tau)}{|G|} + O(x\varepsilon) + O(e^{-km}xb_1(x)^{-1}).$$

By choosing $e^{km+1} = b_1(x)^{-1}$ one obtains (14) with $b(x) = b_1(x)^{1/km+1}$.

Now let $\tau \subseteq \mathcal{X}$ be a smooth set and $t = \{ \tau_v \}$ a system of elementary sets with the properties

$$\operatorname{card}(t) < \Delta^{-m}, \quad \tau_\nu \cap \tau_\nu = \emptyset \quad \text{for} \quad \nu \neq \nu' ,$$

$$\tau \subseteq \bigcup_{\tau_\nu \in t} \tau_\nu , \quad \operatorname{mes}\left( \bigcup_{\tau_\nu \in t, \tau_\nu \neq \emptyset} \tau_\nu \right) < C(\tau) \Delta$$

for some $\Delta > 0$. Applying (14) to every $\tau_\nu \in t$ one obtains

$$N = A(x) \frac{\operatorname{mes}(\tau)}{|G|} + O(C(\tau) \Delta x) + O\left( \frac{x}{\Delta^m b(x)} \right),$$

and it is enough to choose $\Delta^{m+1} = \frac{1}{b(x)}$ to finish the proof.
To deduce Theorem 2 from Proposition 5 we take
\[ G = H_1 \times \cdots \times H_r, \]
where \( H_j \) denotes the ideal class group of \( k_j \), and define \( W \) to be either \( V(A) \cap I_0 \), or \( V(A) \cap \mathcal{P} \). By lemma 3, one can take
\[ A(x) = \frac{\omega_k}{L(1, \Phi)} x, \quad B(x, a(\chi)) = \frac{x^{\ell_1}}{a(\chi)^{\frac{3n+1}{2}}} \]
in the former case, and
\[ A(x) = \int_2^x \frac{dx}{\log x}, \quad B(x, a(\chi)) = \exp \left( \frac{c_2 \log x}{\log a(\chi) + \sqrt{\log x}} \right) \]
in the latter case. Lemma 4 assures that \( g(\chi) = 0 \) for a non-trivial character \( (\chi_1, \ldots, \chi_r) \) of \( H \); it can be checked easily that
\[ a(\chi) \leq c_3 \sum_{j=1}^r a(\chi_j) \]
for some constant \( c_3 \) depending only on the fields \( k_1, \ldots, k_r \), and that in both cases \( b(x) \) has the required form to assure the right error terms in theorem 2.

4.

The condition \( (D_j, D_i) = 1 \) for \( j \neq i \) in theorem 2 and in lemma 4 can be replaced by a weaker one: for every rational prime \( p \) one has \( (e_j(p), e_i(p)) = 1 \) for \( j \neq i \), where \( e_j(p) \) denotes the ramification degree of \( p \) in \( k_j \) (compare \([17]\)). Following the interpretation given to the scalar product of L-functions in \([19]\) one may try to interpret theorem 2 as a statement about distribution of integral points on algebraic tori. Finally we should like to refer to \([20]-[24]\), where the problem discussed here or similar questions were studied.

Acknowledgement. – We are grateful to Professor P. Deligne and Professor M. Gromov for several conversations related to this work, to Dr. R. Sczech for the reference \([6]\), and to the referee for numerous remarks and comments.

Appendix.

Following \([2]\) we discuss here the general situation making no a priori assumptions on \( k_j, \ 1 \leq j \leq r, \) and \( k \). As before, \( K \) denotes the
composite field of \( k_1, \ldots, k_r \). Given any idele-class character \( \chi_j : \mathbb{C}^* \to \mathbb{C}^* \) normalized by the conditions \( \chi_j \circ N^{-1} = 1 \) and \( |\chi_j(a)| = 1 \), put

\[
b_n(\chi_j) = \sum_{N_{k_j/k}=n} \chi_j(a),
\]

and define

\[
L(s; \chi_1, \ldots, \chi_r) = \sum_n b_n(\chi_1) \ldots b_n(\chi_r)|n|^{-s},
\]

where \( n, a \) vary over integral divisors of \( k, k_j \). It follows then from the results cited above (see [12], [13]) that

\[
(A.0) \quad L(s; \chi_1, \ldots, \chi_r) = \prod_{j=1}^{v} L(s, \psi_j) L(s, \Phi)^{-1},
\]

where \( L(s, \psi_j) \) are Hecke L-functions,

\[
(A.1) \quad L(s, \Phi) = \prod_p \Phi^{(p)}([p]^{-s})^{-1},
\]

\( \Phi^{(p)}(t) \) is a rational function such that \( \Phi^{(p)}(t) = 1 + t^2 g^{(p)}(t), \ g^{(p)} \in \mathbb{C}[t] \) for almost all \( p \) (here \( p \) varies over the prime divisors of \( k \)). Moreover, both \( \psi_1, \ldots, \psi_v \) and \( \Phi^{(p)} \) are exactly computable as soon as \( \chi_1, \ldots, \chi_r \) are given. In particular, the product \((A.1)\) converges absolutely for \( \Re s > \frac{1}{2} \) and

\[
L(s, \Phi) \neq 0, \ \infty
\]
in this half-plane. If \( k_1, \ldots, k_r \) are linearly disjoint over \( k \), then \( v = 1 \) and \( \psi_1 = \prod_{j=1}^{r} \chi_j \circ N_{k_j/k_j} \) is an idele-class character in \( K \); if \( r = 2 \) and \( k_1, k_2 \) are quadratic extensions of \( k \) with co-prime discriminants, then \( L(s, \Phi) = L(2s, \chi_0) \) for some idele class character \( \chi_0 \) of \( k \) (depending on \( \chi_1, \chi_2 \)). We now apply these results to obtain estimates for the sums

\[
S = \sum_{\substack{a \in V_0 \\ \ |a| \leq x}} \chi_1(a_1) \ldots \chi_r(a_r),
\]

\[
S_{pr} = \sum_{\substack{p \in V_{pr} \\ \ |p| \leq x}} \chi_1(p_1) \ldots \chi_r(p_r),
\]
where \( V_0 = \{a|N_{k_1}a_1 = \cdots = N_{k_r}a_r, a_j \in I_0^j\}, \)
\[
V_{\mathcal{P}} = \{p|p \in V_0, p_j \in \mathcal{P}\}.
\]
The implied constants in \( O \)-symbols depend on \( \chi_1, \ldots, \chi_r; \) this
dependence can be expressed in terms of \( a(\chi_1), \ldots, a(\chi_r) \) but we shall not
do it here. Let \( v_0 \) be the number of trivial \( \psi_j; \)
\[ v_0 = |\{j|\psi_j = 1\}|, \]
then
\[
(A.2) \quad S = \sum_{k=1}^{v_0} (\log x)^{k-1} c_k x + O(x^{1-\gamma}),
\]
\[
(A.3) \quad S_{\mathcal{P}} = v_0 \int_{2}^{x} \frac{dx}{\log x} + O(x \exp (-\gamma' \sqrt{\log x}))
\]
for some exactly computable constants \( c_1, \ldots, c_{v_0} \) and \( \gamma > 0, \gamma' > 0. \)

The estimates (A.2) and (A.3) follow from the properties of the \( L \)-
functions (A.0) and (A.1) along the same lines as the corresponding
estimates in the text.

BIBLIOGRAPHY

[1] E. Hecke, Eine neue Art von Zetafunktionen und ihre Beziehungen zur
[2] B. Z. Moroz, Distribution of integral ideals with equal norms in the fields of
algebraic numbers, I.H.E.S. Preprint, October 1982.
USSR, 31 (1952), 507-542.
Mathematics, 26 (1956), 1-42.
(MR 57 # 3092).
[8] Yu. V. Linnik, Ergodic properties of algebraic fields, Springer Verlag, 1968,
Chapter IX.
[9] E. P. Golubeva, On representation of large numbers by ternary quadratic


Manuscrit reçu le 27 avril 1983
révisé le 16 novembre 1983.

Dr. B. Z. Moroz,
Mathématique, Bât. 425
Université de Paris-Sud
Centre d’Orsay
91405 Orsay Cedex, France.