ANNALES DE L'INSTITUT FOURIER

BARUCH Z. MOROZ

On the distribution of integral and prime divisors with equal norms

Annales de l'institut Fourier, tome 34, n° 4 (1984), p. 1-17
<http://www.numdam.org/item?id=AIF_1984__34_4_1_0>

Ann. Inst. Fourier, Grenoble
34, 4 (1984), 1-17.

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 $\mathbf{Q}$, and fix an ideal class A_j in k_j, $1 \leqslant j \leqslant r$. Let

$$V(A) = \{\mathfrak{a} \mid \mathfrak{a}_j \in A_j,\ N_{k_1/k}\mathfrak{a}_1 = \cdots = N_{k_r/k}\mathfrak{a}_r\}$$

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 integrall 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 $k = \mathbf{Q}$ (compare [2] and the appendix to this paper).

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

$\mathfrak{o}$ is the ring of integers of L,
$\mathfrak{o}^*$ 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.

$\mathscr{P}$ is the set of prime divisors,
S_2 and S_1 are the sets of complex and real places of L,
$S = S_1 \cup S_2$, $|S_j| =: r_j$ $(j=1,2)$, $n = r_1 + 2r_2$,
$L_w = \begin{cases} \mathbf{R}, & w \in S_1 \\ \mathbf{C}, & w \in S_2 \end{cases}$ denotes the completion of L at $w \in S$,
$\|x\| = \begin{cases} |x|, & w \in S_1 \\ |x|^2, & w \in S_2 \end{cases}$ for $x \in L_w$.

Let us introduce the algebra $X = \prod_{w \in S} L_w$ of dimension n over $\mathbf{R}$, refered to as Minkowski space associated with L. Let $\psi: L \to X$ be the componentwise embedding of L in X. The group $\mathfrak{o}^*$ 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 $Y = X^*/\psi(\mathfrak{o}^*)$ 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 construction, as well as the results of [3]-[5] to be generalized here. Let $N: X \to \mathbf{R}_+$ and $N^{-1}: \mathbf{R}_+ \to X$ 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 $\psi(\mathfrak{o}^*)$, one obtains $Y = \mathbf{R}_+ \times Y_0$, where

$$Y_0 := X_0/\psi(\mathfrak{o}^*), \qquad X_0 := \{x \mid x \in X, N(x) = 1\}.$$

Let $\hat{Y}_0$ be the group of characters of Y_0 and $\lambda \in \hat{Y}_0$; one can regard λ as a character of X^* trivial on $\psi(\mathfrak{o}^*)$ and on $N^{-1}\mathbf{R}_+$. Thus

$$\lambda(x) = \prod_{w \in S} \|x_w\|^{it_w} \left(\frac{x_w}{|x_w|}\right)^{a_w}, \tag{1}$$

where $a_w \in Z$, $t_w \in \mathbf{R}$, x_w denotes the projection of x on L_w, and, moreover, $\lambda(\varepsilon x) = \lambda(x)$ for $\varepsilon \in \psi(\mathfrak{o}^*)$,

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

It follows from the Dirichlet theorem on units (compare [1], [6]) that $Y = \mathbf{R}_+ \times \mathfrak{T}_L \times (Z/2Z)^{r_0}$, where $\mathfrak{T}_L$ is a torus of dimension $n-1$, and $r_0 \leqslant r_1$. Therefore, $\hat{Y}_0 \cong Z^{n-1} \times (Z/2Z)^{r_0}$, and there exist characters $\lambda_1, \ldots, \lambda_{n-1}$ multiplicatively independent over Z and such that any $\lambda \in \hat{Y}_0$ has the form

$$\lambda = \prod_{v=1}^{n-1} \lambda_v^{m_v} \lambda', \qquad m_v \in \mathbf{Z}, \tag{2}$$

where $\lambda'(x) = \prod_{w \in S_1} \left(\frac{x_w}{|x_w|}\right)^{a_w}$, $a_w \in \{0,1\}$. The map ψ induces an embedding

$$\varphi : L^*/\mathfrak{o}^* \to Y$$

of the group of principal divisors $L^*/\mathfrak{o}^*$ of L in Y. Composing φ with the projection of Y on $\mathbf{R}_+ \times \mathfrak{T}_L$ one obtains an embedding

$$\varphi_0 : L^*/\mathfrak{o}^* \to \mathbf{R}_+ \times \mathfrak{T}_L .$$

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

$$f : I \to \mathbf{R}_+ \times \mathfrak{T}_L \tag{3}$$

which coincides with φ_0 on $L^*/\mathfrak{o}^*$. 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 $\mathbf{R}_+ \times \mathfrak{T}_L$. To be more precise, let us introduce a parametrisation of $\mathfrak{T}_L$ induced by the basic characters $\lambda_j(x) = \exp(2\pi i \varphi_j(x))$, $1 \leqslant j \leqslant n-1$, $0 \leqslant \varphi_j(x) < 1$, and identify a point $x \in \mathfrak{T}_L$ with its image $(\lambda_1(x), \ldots, \lambda_{n-1}(x)) \in T^{n-1}$, where T denotes the unit circle in $\mathbf{C}^*$. We call a subset

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

of $\mathfrak{T}_L$ *elementary* whenever $0 \leqslant \lambda_j < \lambda_j + \delta_j \leqslant 1$. A set $\tau \subseteq \mathfrak{T}_L$ 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 $(t) < \Delta^{-(n-1)}$,

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

where mes is the normalized Haar measure on $\mathfrak{T}_L$ (so that $\operatorname{mes}(\mathfrak{T}_L) = 1$) and $\partial\tau$ denotes the boundary of τ. 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* $\tau \subseteq \mathfrak{T}_L$ *and any ideal class* $A \in H$

$$\operatorname{card}\{\mathfrak{a} \mid \mathfrak{a} \in I_0,\ f(\mathfrak{a}) \in (0,x) \times \tau,\ \mathfrak{a} \in A\} = \frac{\omega_L \operatorname{mes}(\tau)}{h} x + O(x^{1-c_1})$$

$$\operatorname{card}\{\mathfrak{p} \mid \mathfrak{p} \in \mathscr{P},\ f(\mathfrak{p}) \in (0,x) \times \tau,\ \mathfrak{p} \in A\}$$
$$= \frac{\operatorname{mes}(\tau)}{h} \int_2^x \frac{dx}{\log x} + O(\exp(-c_2\sqrt{\log x})x),$$

where the constants $c_1, c_2 > 0$ *depend on* L, *but not on* $x \to \infty$, *and* ω_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

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

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 $\mathbf{R}_+$. The map

(3′) $$g' : I \to \mathbf{R}_+ \times T^{n-1}$$

given by

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

is compatible with (3) under the above identification of $\mathfrak{T}_L$ and 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^j, $\mathscr{P}_j$, $\mathfrak{T}_j$ and h_j denote the monoid of integral divisors, the set of prime divisors, the torus $\mathfrak{T}_{k_j}$ and the class number of k_j respectively; let $h = \prod_{j=1}^{r} h_j$ and $\mathfrak{T} = \mathfrak{T}_1 \times \cdots \times \mathfrak{T}_r$, moreover, let $\mathscr{P} = \{\mathfrak{p} \mid \mathfrak{p}_j \in \mathscr{P}_j\}$ and $I_0 = \{\mathfrak{a} \mid \mathfrak{a}_j \in I_0^j\}$ be the sets of r-tuples of prime and integral divisors respectively; let $K = k_1 \dots k_r$ be the composite of the fields $k_1, \dots, k_r$, let n_j and D_j be the degree $[k_j : \mathbf{Q}]$ and the discriminant of k_j and n be the degree $[K : \mathbf{Q}]$ of K. Consider the map

$$g_j : I_0^j \to \mathfrak{T}_j$$

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

$$g_j : \mathfrak{a}_j \mapsto (\mu_{j1}(\mathfrak{a}_j), \dots, \mu_{jn_j-1}(\mathfrak{a}_j)), \quad \mathfrak{a}_j \in I_0^j,$$

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

$$\text{(4)} \qquad Z(k_1, \dots, k_r; s) = \sum_{m=1}^{\infty} a_m^{(1)} \dots a_m^{(r)} m^{-s},$$

where $a_m^{(j)} = \text{card}\,\{\mathfrak{a}_j \mid \mathfrak{a}_j \in I_0^{(j)}, N_{k_j/\mathbf{Q}}\mathfrak{a}_j = m\}$ 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

$$\text{(5)} \qquad Z(k_1, \dots, k_r; s) = \frac{Z_K(s)}{L(s,\Phi)},$$

where $L(s,\Phi) = \prod_p \Phi^{(p)}(p^{-s})^{-1}$, $\Phi^{(p)}(t)$ is a rational function of t, p varies over rational primes, and, moreover, $\Phi^{(p)}(p^{-s}) \neq 0, \infty$ for $\operatorname{Re} s > \frac{1}{2}$; 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 $\operatorname{Re} s > \frac{1}{2}$.

THEOREM 2. — *If k_j is Galois over $\mathbf{Q}$ 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*

$$\operatorname{card}\{\mathfrak{a} \mid \mathfrak{a} \in \mathrm{V(A)} \cap \mathrm{I}_0,\ |\mathfrak{a}| < x,\ g(\mathfrak{a}) \in \tau\} = \frac{\omega_{\mathrm{K}} \operatorname{mes}(\tau)}{h\mathrm{L}(1,\Phi)} x + \mathrm{O}(x^{1-c_1}),$$

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

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

$$|\mathfrak{a}| : = \left(\sum_{j=1}^{r} \mathrm{N}_{k_j/\mathbf{Q}}\mathfrak{a}_j\right)^{\frac{1}{r}} \text{ for } \mathfrak{a} = \{\mathfrak{a}_1, \ldots, \mathfrak{a}_r \mid \mathfrak{a}_j \in \mathrm{I}_0^j\},$$

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

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

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

$$\mathrm{N}_{k_1/\mathbf{Q}}\mathfrak{a}_1 = \cdots = \mathrm{N}_{k_r/\mathbf{Q}}\mathfrak{a}_r \tag{6}$$

affects the probability of the event:

$$\text{« } \mathfrak{a}_1 \in \mathrm{A}_1, \ldots, \mathfrak{a}_r \in \mathrm{A}_r,\ g_1(\mathfrak{a}_1) \in \tau_1, \ldots, g_r(\mathfrak{a}_r) \in \tau_r \text{ »}$$

neither for r-tuples of integral, *nor* of prime divisors. On the other hand, Theorem 2 may be regarded as an assertion 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 $f_1(x_1,x_2) \leqslant \mathrm{N}$ *is equal to*

$$\mathrm{AN} + \mathrm{O}(\mathrm{N}^{1-c})$$

for some $\mathrm{A} > 0$, $c > 0$ *independent on* N.

It turns out that for two quadratic fields $(n_1=n_2=r=2)$

$$\mathrm{L}(s,\Phi) = \mathrm{L}(2s,\chi_0),$$

where $\chi_0(n) = \left(\frac{\mathrm{D}_1\mathrm{D}_2}{n}\right)$ (see, e.g., [13], § 5). Therefore we obtain the following result.

Proposition 4. — *Let* $k_j = \mathbf{Q}(\sqrt{\mathrm{D}_j})$, $j = 1,2$, $(\mathrm{D}_1,\mathrm{D}_2) = 1$. *Then*

$$\operatorname{card}\{\mathfrak{a} \mid \mathfrak{a} \in \mathrm{V}(\mathrm{A}) \cap \mathrm{I}_0,\ |\mathfrak{a}| < x, g(\mathfrak{a}) \in \tau\} = \frac{\omega_{\mathrm{K}} \operatorname{mes}(\tau)}{h\mathrm{L}(2,\chi_0)} x + \mathrm{O}(x^{1-c_1})$$

with $c_1 > 0$ *independent on* x.

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

2.

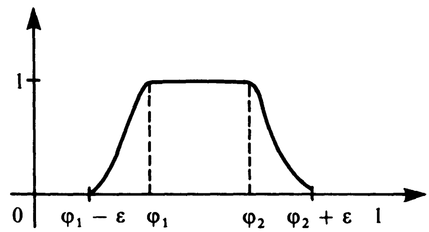
Further on we write $\mathrm{I}_0(\mathrm{K})$, $\mathscr{P}(\mathrm{K})$, $\mathrm{H}(\mathrm{K})$, $\mu(\mathrm{K})$ for the monoid of the integral divisors, set of prime divisors, class group and the set of basic Größencharaktere of K. Theorem 2 will be deduced from the following four lemmas.

Lemma 1. — *Let* φ_1, φ_2, ε *satisfy the inequalities*

$$0 \leqslant \varphi_1 - \varepsilon < \varphi_1 < \varphi_2 < \varphi_2 + \varepsilon \leqslant 1.$$

There exists a real valued function $f \in \mathrm{C}^\infty[0,1]$ *such that* $0 \leqslant f(t) \leqslant 1$ for $t \in [0,1]$, $f(t) = 1$ *for* $t \in [\varphi_1,\varphi_2]$, $f(t) = 0$ *for* $t \notin [\varphi_1-\varepsilon,\varphi_2+\varepsilon]$,

$f'(t) \neq 0$ *for* $\varphi_1 - \varepsilon < t < \varphi_1$ *and* $\varphi_2 < t < \varphi_2 + \varepsilon$:



This is a well-known lemma of elementary calculus; we choose one of such functions to be denoted by $f(\varphi_1, \varphi_2, \varepsilon; .)$.

Let C_j, C_K be the idele class groups of k_j, K, and χ_j be an idele class character of k_j trivial on $\mathbf{R}_+$; we define an idele class character

$$(7) \qquad \chi := \prod_{j=1}^{r} \chi_j \circ N_{K/k_j}$$

in K, and an L-function

$$L(\chi_1, \ldots, \chi_r; s) := \sum_{\mathfrak{a} \in V} \chi_1(\mathfrak{a}_1) \ldots \chi_r(\mathfrak{a}_r) |\mathfrak{a}|^{-s},$$

where $V = \{\mathfrak{a} | \mathfrak{a}_j \in I_0^j, N_{k_1/Q}\mathfrak{a}_1 = \cdots = N_{k_r/Q}\mathfrak{a}_r\}$.

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* $L(s,\chi) = \sum_{\mathfrak{a} \in I_0(K)} \chi(\mathfrak{a}) N_{K/Q}\mathfrak{a}^{-s}$ *for* $\mathrm{Re}\, s > 1$, *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*

$$(8) \qquad \sum_{\mathfrak{a} \in V, |\mathfrak{a}| < x} \chi_1(\mathfrak{a}_1) \ldots \chi_r(\mathfrak{a}_r) = g(\chi) \frac{\omega_K x}{L(1,\Phi)} + O(a(\chi)^{\frac{3n+1}{2}} x^{1-c_1}),$$

$$(9) \qquad \sum_{\mathfrak{a} \in V \cap \mathcal{P}, |\mathfrak{a}| < x} \chi_1(\mathfrak{a}_1) \ldots \chi_r(\mathfrak{a}_r)$$

$$= g(\chi) \int_2^x \frac{dx}{\log x} + O\left(x \exp\left(-c_2 \frac{\log x}{\log a(\chi) + \sqrt{\log x}}\right)\right)$$

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; $\sum_{w \in S} (|a_w| + |b_w|) = : a(\chi)$, *when* χ *is given by*

$$\chi(\alpha) = \prod_{w \in S} \left(\frac{\alpha_w}{|\alpha_w|}\right)^{a_w} . |\alpha_w|^{ib_w} \tag{10}$$

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

Proof. – To prove (9) one remarks (see, e.g., [14], Lemma 1) that for any $\mathfrak{a} \in V \cap \mathscr{P}$ satisfying the condition « $|\mathfrak{a}| = q$ is a rational prime » there exists one and only one prime $\mathfrak{p} \in \mathscr{P}(K)$ such that $N_{K/k_j}\mathfrak{p} = \mathfrak{a}_j$. Therefore,

$$\begin{aligned} \sum_{\mathfrak{a} \in V \cap \mathscr{P}, |\mathfrak{a}| < x} \chi_1(\mathfrak{a}_1) \ldots \chi_r(\mathfrak{a}_r) &= \sum_{\substack{\mathfrak{a} \in V \cap \mathscr{P}, |\mathfrak{a}| = q \\ q < x}} \chi_1(\mathfrak{a}_1) \ldots \chi_r(\mathfrak{a}_r) + O(x^{1/2}) \\ &= \sum_{\mathfrak{p} \in \mathscr{P}(K),\ N_{K/Q}\mathfrak{p} < x} \chi(\mathfrak{p}) + O(x^{1/2}) \end{aligned}$$

and (9) follows from estimates obtained in the work cited above (see [4], ch. I, § 8, lemma 4, or [5], § 2, lemma 6) (*). By a standard argument one obtains (see, e.g., [15], lemma 3.12)

$$\begin{aligned} A(x) := \sum_{\mathfrak{a} \in V, |\mathfrak{a}| < x} \chi_1(\mathfrak{a}_1) \ldots \chi_r(\mathfrak{a}_r) \\ = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \frac{x^s}{s} L(\chi_1, \ldots, \chi_r; s)\, ds + O_\varepsilon\left(\frac{x^{1+\varepsilon}}{T}\right), \end{aligned}$$

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

$$\begin{aligned} A(x) = \frac{1}{2\pi i} \int_{1/2+\varepsilon-iT}^{1/2+\varepsilon+iT} \frac{x^s}{s} L(s,\chi) L(s,\Phi)^{-1}\, ds + g(\chi) \frac{\omega_K x}{L(1,\Phi)} \\ + O_\varepsilon\left(\frac{x^{1+\varepsilon}}{T}\right) + O_\varepsilon\left(\int_{1/2+\varepsilon}^{c} (|L(\sigma+iT,\chi)| + |L(\sigma-it,\chi)|) \frac{x^\sigma}{T}\, d\sigma\right) \end{aligned}$$

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

(*) 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 Γ-function an estimate

$$L(\sigma+it,\chi) = O_\varepsilon\left((1+|t|)^{\frac{3n}{2}(1-\sigma+\varepsilon)} a(\chi)^{\frac{3n}{2}+\varepsilon}\right) \tag{11}$$

in the region $0 \leqslant \sigma \leqslant c$. 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* Q *for each* j, $n = \prod_{j=1}^{r} n_j$, $(D_j, D_\ell) = 1$ *for* $j \neq \ell$, $\chi = 1$, *and* χ_j *be unramified for each* j. *Then* $\chi_j = 1$ *for every* j.

Proof. — Let us assume first that χ_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)

$$\{(N_{K/k_1}A, \ldots, N_{K/k_r}A) | A \in H_K\} = H_1 \times \cdots \times H_r,$$

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 $N_{K/k_j}A = A_j$; $N_{K/k_\ell}A = 1$ for $\ell \neq j$. If $\chi = 1$, then

$$1 = \prod_{\ell=1}^{r} (\chi_\ell \circ N_{K/k_\ell})(A) = \chi_j(A_j);$$

and we see that $\chi_j = 1$. Assuming $\chi = 1$ we deduce now that χ_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

$$(\chi_j \circ N_{K/k_j})^{-1} = \prod_{\ell \neq j} \chi_\ell \circ N_{K/k_\ell}$$

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

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

$$f(\varphi_1,\varphi_2,\varepsilon;t) = \sum_{n=-\infty}^{\infty} c_n \exp(2\pi int),$$

so that

$$(12) \qquad c_0 = (\varphi_2-\varphi_1) + O(\varepsilon), \qquad c_n = O\left(\frac{1}{|n|^k\varepsilon^{k-1}}\right)$$

for any fixed integral $k \geqslant 1$.

PROPOSITION 5. — *Let*

$$\mathfrak{T} = \{\exp(2\pi i\varphi_1), \ldots, \exp(2\pi i\varphi_m) | 0 \leqslant \varphi_j < 1, j=1,\ldots,m\}$$

be a torus of dimension m; τ *be a smooth subset of* $\mathfrak{T}$, G *be a finite Abelian group with the group of characters* $\hat{G}$ *and*

$$\hat{\mathfrak{T}} = \{\lambda_1^{\ell_1} \ldots \lambda_m^{\ell_m} | \ell_j \in Z, \lambda_j : x \mapsto x_j\}$$

be the group of characters of $\mathfrak{T}$, $x = (\ldots, \exp(2\pi i\varphi_j) = x_j, \ldots) \in \mathfrak{T}$. *Consider a set* W *and three maps :*

$$g_1 : W \to \mathfrak{T}, \qquad g_2 : W \to G, \qquad N : W \to \mathbf{R}_+;$$

we denote by $\hat{W}$ *the set of functions on* W *defined by*

$$\hat{W} = \{\mu | \mu(\mathfrak{a}) = (\lambda \circ g_1)(\mathfrak{a})(\lambda' \circ g_2)(\mathfrak{a}), \lambda \in \hat{\mathfrak{T}}, \lambda' \in \hat{G}\},$$

where $\mathfrak{a}$ *varies over the elements of* W. *If*

$$(13) \qquad \sum_{N\mathfrak{a}<x} \chi(\mathfrak{a}) = g(\chi)A(x) + O(xB(x,a(\chi))^{-1})$$

for $\chi \in \hat{W}$, *where*

$$g(\chi) = \begin{cases} 1, & \lambda=1 \text{ and } \lambda'=1 \\ 0, & \text{otherwise} \end{cases}; \qquad A(x) = O(x), \qquad a(\chi) := \sum_{j=1}^{m} |\ell_j|$$

for

$$\chi = (\lambda \circ g_1)(\lambda' \circ g_2), \qquad \lambda' \in \hat{G}, \qquad \lambda = \prod_{j=1}^{m} \lambda_j^{\ell_j},$$

then for any smooth subset τ *of* $\mathfrak{T}$ *and any* $\gamma \in G$ *we have*

$$(14) \quad \text{card}\,\{\mathfrak{a} \mid \mathfrak{a} \in W,\ g_2(\mathfrak{a}) = \gamma,\ g_1(\mathfrak{a}) \in \tau,\ N\mathfrak{a} < x\} = A(x)\frac{\text{mes}\,(\tau)}{|G|} + O\left(\frac{x}{b(x)}\right),$$

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

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

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

Proof. – We deduce (14) from (13) for rectangular τ by means of lemma 1 and then prove (14) for any smooth $\tau \subseteq \mathfrak{T}$. Let

$$\tau = \{\varphi \mid \psi_j \leqslant \varphi_j < \psi_j + \delta_j, j = 1, \ldots, m\}.$$

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

$$f_j^+(\varphi_j) = f(\psi_j, \psi_j + \delta_j, \varepsilon; \varphi_j),$$
$$f_j^-(\varphi_j) = f(\psi_j - \varepsilon, \psi_j - \varepsilon + \delta_j, \varepsilon; \varphi_j),$$
$$F^\pm = \prod_{j=1}^{m} f_j^\pm.$$

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

$$\sum_{\substack{N\mathfrak{a} < x \\ g_2(\mathfrak{a}) = \gamma}} F^-(g_1(\mathfrak{a})) \leqslant \mathcal{N} \leqslant \sum_{\substack{N\mathfrak{a} < x \\ g_2(\mathfrak{a}) = \gamma}} F^+(g_1(\mathfrak{a})).$$

On the other hand,

$$(16) \quad \sum_{\substack{N\mathfrak{a} < x \\ g_2(\mathfrak{a}) = \gamma}} F^\pm(g_1(\mathfrak{a})) = \frac{1}{|G|} \sum_{N\mathfrak{a} < x} \sum_{\chi \in \hat{G}} \overline{\chi(\gamma)}\, F^\pm(g_1(\mathfrak{a}))\chi(g_2(\mathfrak{a})).$$

Write $f_j^{\pm}(t) = \sum_{n=-\infty}^{\infty} c_{nj}^{\pm} \exp(2\pi int)$ and denote the left hand side in (16) by $\mathcal{N}^{\pm}$. It follows from (16) that

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

where

$$c^{\pm}(\mu) = \frac{1}{|G|} \bar{\chi}(\gamma) \prod_{j=1}^{m} c_{\ell_j j}^{\pm} \quad \text{for} \quad \mu = ((\lambda_1^{\ell_1} \ldots \lambda_m^{\ell_m}) \circ g_1)(\chi \circ g_2).$$

Équation (13) and estimate (12) give

$$\begin{aligned} \mathcal{N}^{\pm} &= \frac{1}{|G|}\left(\prod_{j=1}^{m} \delta_j\right) A(x) + O(x\varepsilon) + \sum_{\substack{\mu \in \hat{W} \\ \mu \neq 1}} |c^{\pm}(\mu)| \left| \sum_{Na < x} \mu(a) \right| \\ &= A(x) \frac{\operatorname{mes}(\tau)}{|G|} + O(x\varepsilon) + O\left(\sum_{\mu \in \hat{W}} |c^{\pm}(\mu)| \quad B(x, a(\mu))^{-1} x \right). \end{aligned}$$

Thus

$$\mathcal{N}^{\pm} = A(x) \frac{\operatorname{mes}(\tau)}{|G|} + O(x\varepsilon) + O(\varepsilon^{-km} x b_1(x)^{-1}).$$

By choosing $\varepsilon^{km+1} = b_1(x)^{-1}$ one obtains (14) with $b(x) = b_1(x)^{1/km+1}$. Now let $\tau \subseteq \mathfrak{T}$ be a smooth set and $t = \{\tau_\nu\}$ a system of elementary sets with the properties

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

$$\tau \subseteq \bigcup_{\tau_\nu \in t} \tau_\nu, \qquad \operatorname{mes}\left(\bigcup_{\tau_\nu \cap \tau \neq \varnothing} \tau_\nu \right) < C(\tau) . \Delta$$

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

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

and it is enough to choose $\Delta^{m+1} = \dfrac{1}{b(x)}$ 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 $V(A) \cap \mathscr{P}$. By lemma 3, one can take

$$A(x) = \frac{\omega_K}{L(1,\Phi)} x, \qquad B(x,a(\chi)) = \frac{x^{c_1}}{a(\chi)^{\frac{3n+1}{2}}}$$

in the former case, and

$$A(x) = \int_2^x \frac{dx}{\log x}, \qquad B(x,a(x)) = \exp\left(\frac{c_2 \log x}{\log a(\chi) + \sqrt{\log x}}\right)$$

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 $a(\chi) \leqslant c_3 \sum_{j=1}^{r} a(\chi_j)$ 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 $(D_j, D_\ell) = 1$ for $j \neq \ell$ 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, $1 \leqslant j \leqslant r$, and k. As before, K denotes the composite field of $k_1, \ldots, k_r$. Given any idele-class character $\chi_j : C_j \to \mathbf{C}^*$ normalized by the conditions $\chi_j \circ N^{-1} = 1$ and $|\chi_j(\alpha)| = 1$, put

$$b_{\mathfrak{n}}(\chi_j) = \sum_{N_{k_j/k}\mathfrak{a} = \mathfrak{n}} \chi_j(\mathfrak{a}),$$

and define

$$L(s;\chi_1,\ldots,\chi_r) = \sum_{\mathfrak{n}} b_{\mathfrak{n}}(\chi_1) \ldots b_{\mathfrak{n}}(\chi_r)|\mathfrak{n}|^{-s},$$

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

$$\text{(A.0)} \qquad L(s;\chi_1,\ldots,\chi_r) = \prod_{j=1}^{\nu} L(s,\psi_j)L(s,\Phi)^{-1},$$

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

$$\text{(A.1)} \qquad L(s,\Phi) = \prod_p \Phi^{(p)}(|p|^{-s})^{-1},$$

$\Phi^{(p)}(t)$ is a rational function such that $\Phi^{(p)}(t) = 1 + t^2 g^{(p)}(t)$, $g^{(p)} \in \mathbf{C}[t]$ for almost all p (here p varies over the prime divisors of k). Moreover, both $\psi_1, \ldots, \psi_\nu$ 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 $\operatorname{Re} s > \frac{1}{2}$ and

$$L(s,\Phi) \neq 0, \infty$$

in this half-plane. If $k_1, \ldots, k_r$ are linearly disjoint over k, then $\nu = 1$ and $\psi_1 = \prod_{j=1}^{r} \chi_j \circ N_{K/k_j}$ 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 χ_0 of k (depending on χ_1, χ_2). We now apply these results to obtain estimates for the sums

$$S = \sum_{\substack{\mathfrak{a} \in V_0 \\ |\mathfrak{a}| < x}} \chi_1(\mathfrak{a}_1) \ldots \chi_r(\mathfrak{a}_r),$$

$$S_{pr} = \sum_{\substack{\mathfrak{p} \in V_{pr} \\ |\mathfrak{p}| < x}} \chi_1(\mathfrak{p}_1) \ldots \chi_r(\mathfrak{p}_r),$$

where $V_0 = \{\mathfrak{a} \mid N_{k_1/k}\mathfrak{a}_1 = \cdots = N_{k_r/k}\mathfrak{a}_r, \mathfrak{a}_j \in I_0^j\}$,

$$V_{pr} = \{\mathfrak{p} \mid \mathfrak{p} \in V_0, \mathfrak{p}_j \in \mathscr{P}\}.$$

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 ν_0 be the number of trivial ψ_j:

$$\nu_0 = |\{j \mid \psi_j = 1\}|,$$

then

$$\text{(A.2)} \qquad S = \sum_{k=1}^{\nu_0} (\log x)^{k-1} c_k \, x + O(x^{1-\gamma}),$$

$$\text{(A.3)} \qquad S_{pr} = \nu_0 \int_2^x \frac{dx}{\log x} + O(x \exp(-\gamma' \sqrt{\log x}))$$

for some exactly computable constants $c_1, \ldots, c_{\nu_0}$ 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 Bezeihungen zur Verteilung der Primzahlen, *Math. Zeitschrift*, 6 (1920), 11-51.

[2] B. Z. Moroz, Distribution of integral ideals with equal norms in the fields of algebraic numbers, *I.H.E.S. Preprint*, October 1982.

[3] H. Rademacher, Primzahlen reel-quadratischer Zahlkörper in Winkelräumen *Math. Annalen*, 111 (1935), 209-228.

[4] J. P. Kubilius, One some problems in geometry of numbers, *Math. Sbornik USSR*, 31 (1952), 507-542.

[5] T. Mitsui, Generalized Prime Number Theorem, *Japanese Journal of Mathematics*, 26 (1956), 1-42.

[6] H. Hasse, Zetafunktionen und L-funktionen zu Funktionenkörpern vom Fermatschen Typus, § 9, Gesammelte Werke, Bd. II, p. 487-497.

[7] T. Mitsui, Some prime number theorems for algebraic number fields, *Proc. Sympos. Res. Inst. Math. Sci.*, Kyoto Univ., Kyoto 1977, N. 294, p. 100-123 (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 forms, *Doklady Acad. of Sci. of the U.S.S.R.*, 191 (1970), 519-521.

[10] W.-Ch. W. Li, On converse theorems for GL(2) and GL(1), *American Journal of Mathematics*, 103 (1981), 883.

[11] Yu. V. Linnik, Private communications.

[12] N. Kurokawa, On Linnik's Problem, *Proc. Japan Academy*, 54 A (1978), 167-169 (see also: Tokyo Institute of Technology Preprint, 1977).

[13] B. Z. Moroz, Scalar products of L-functions with Grössencharacters, *J. für die reine und angewandte Mathematik*, Bd. 332 (1982), 99-117.

[14] B. Z. Moroz, On the convolution of L-functions, *Mathematika*, 27 (1980), 312-320.

[15] E. C. Titchmarsh, *Theory of Riemann Zeta-function*, Oxford, 1951.

[16] H. Fogels, On the zeros of Hecke's L-functions I, *Acta Arithmetica*, 7 (1961/62), 87-106.

[17] W.-Ch. W. Li, B. Z. Moroz, On ideal classes of number fields containing integral ideals of equal norms, *Journal of Number Theory*, to appear.

[18] H. Weyl, Über die Gleichverteilung von Zahlen mod Eins. *Math. Annalen*, 77 (1916), 313-352.

[19] P. K. J. Draxl, L-funktionen Algebraischer Tori, *Journal of Number Theory*, 3 (1971), 444-467.

[20] A. I. Vinogradov On the extension to the left half-plane of the scalar product of Hecke's L-series with Grössencharacters, *Izvestia U.S.S.R. Acad. of Sci., Math. Series*, 29 (1965), 485-492.

[21] P. K. J. Draxl, Functions L et représentation simultanée d'un nombre premier par plusieurs formes quadratiques, Séminaire Delange-Pisot-Poitou, 12e année, 1970/71.

[22] K. Chandrasekharan, R. Narasimhan, The approximate functional equation for a class of zeta-functions, *Math. Ann.*, 152 (1963), 30-64.

[23] K. Chandrasekharan, A. Good, On the number of Integral Ideals in Galois Extensions, *Monatshefte für Mathematik*, 95 (1983), 99-109.

[24] R. A. Rankin, Sums of powers of cusp form coefficients, *Math. Ann.*, 263 (1983), 227-236.

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.