ACTA ARITHMETICA
XLIII (1983)

# Some remarks on factorization in algebraic number fields

by

J. KACZOROWSKI (Poznań)

**1.** In this paper we shall be concerned with some quantitative aspects of the theory of factorization in algebraic number fields.

The method applied is of a more general character and probably can also be applied to other problems.

If $A$ is a set of algebraic integers belonging to the field $K$, then, for $x \geqslant 1$, $A(x)$ denotes the number of integers $a \in A$ such that $|N_{K/Q}(a)| \leqslant x$ and from each set of associated integers only one is counted.

Let $K$ be an algebraic number field with class number $h$ and class group $H(K) = \{X_1 = E, X_2, \ldots, X_h\}$. Denote by $R_K$ its ring of integers and let $M$ be the set of all irreducible elements of $R_K$. Further, let $F_k$ $k = 1, 2, \ldots$, be the set of all elements of $R_K$ which have at most $k$ distinct factorizations into irreducibles.

Similarly, let $G_k$ be the set of all elements of $R_K$ which have at most $k$ such factorizations of distinct lengths.

We denote further $F'_k = F_k \cap Z$ and $G'_k = G_k \cap Z$.

According to the definition of $A(x)$ the meaning of $M(x)$, $F_k(x)$, $G_k(x)$, $F'_k(x)$ and $G'_k(x)$ is clear.

Our first theorem refers to irreducible integers in the field $K$.

J. P. Rémond proved (see [20] and also [19], [16]) that for $x$ tending to infinity

$$M(x) \sim C\frac{x(\log\log x)^{D-1}}{\log x}, \tag{1.1}$$

where $C = C(K)$ is a positive constant and $D = D\big(H(K)\big)$ is the Davenport constant of the class group $H(K)$ (see [16]).

We shall prove the following improvement of this result.

THEOREM 1. *For* $x \geqslant e^e$ *and* $0 \leqslant q \leqslant c_0\dfrac{\sqrt{\log x}}{\log\log x}$, $q \in Z$ *we have*

$$M(x) = \frac{x}{\log x}\sum_{0\leqslant\mu\leqslant q}\frac{W_\mu(\log\log x)}{(\log x)^\mu} + O\left((c_1 q)^q\frac{x(\log\log x)^D}{(\log x)^{q+2}}\right), \tag{1.2}$$

*where* $c_0$ *and* $c_1$ *denote positive constants depending on* $K$, $W_\mu(x) \in C[x]$ *(polynomials with complex coefficients),* $\deg W_0(x) = D-1$ *and* $\deg W_\mu(x) \leqslant D$ *for* $\mu \geqslant 1$.

Our second theorem refers to the sets $G_k$.

Let $h \geqslant 3$. The asymptotic formula for $G_k(x)$ (as well as for $G'_k(x)$) was obtained by J. Śliwa in [23]. His result for $G_k(x)$ is as follows:

$$(1.3)\qquad G_k(x) \sim C\,\frac{x(\log\log x)^B}{(\log x)^A} \quad \text{for } x\to\infty,$$

where $A$, $B$, $C$ are positive constants depending on $K$ and $k$.

We shall prove the following theorem:

THEOREM 2. *Let* $h \geqslant 3$. *For* $x \geqslant e^e$, $k \geqslant 1$ *we have*

$$(1.4)\qquad G_k(x) = \frac{xW(\log\log x)}{(\log x)^A} + O_k\left(\frac{x(\log\log x)^{c_2}}{(\log x)^{A+\gamma_0}}\right),$$

*where* $W(x) \in C[x]$, $c_2 = c_2(k, K) > 0$, $A = A(k, K) > 0$ *and* $\gamma_0 = \min\left\{\frac{1}{h}, \frac{1}{h}\left(1-\cos\frac{2\pi}{h}\right)\right\}$.

Our method leads also to a much stronger but more complicated estimate for $G_k(x)$ than (1.4). We restrict ourselves here only to the simplest case.

Our third theorem refers to natural numbers which have a unique factorization in $K$.

Let $h > 1$. The asymptotic formula for $F'_1(x)$ was obtained by W. Narkiewicz in [14] and [16] for normal fields of prime degree and by R. W. K. Odoni in [18] in the general case. Odoni's result is as follows:

$$(1.5)\qquad F'_1(x) = \frac{x(\log\log x)^B}{(\log x)^C}\left(A + O\left(\frac{1}{\log\log x}\right)\right),$$

where $A$, $B$, $C$ depend upon $K$ and are positive.

Our method permits us to obtain the following stronger estimate:

THEOREM 3. *Let* $h > 1$. *For* $x \geqslant e^e$ *and* $0 \leqslant q \leqslant c_3\,\frac{\sqrt{\log x}}{\log\log x}$, $q \in Z$ *we have*

$$(1.6)\qquad F'_1(x) = \frac{x}{(\log x)^C}\sum_{0\leqslant\mu\leqslant q}\frac{P_\mu(\log\log x)}{(\log x)^\mu} + O\left((c_4 q)^q\,\frac{x(\log\log x)^{c_4}}{(\log x)^{C+q+1}}\right),$$

*where* $P_\mu(x) \in C[x]$ *and* $C$, $c_3$, $c_4$ *depend on* $K$ *and are positive.*

As regards other functions connected with the uniqueness of factorization, S. Allen in [1] gave an upper bound for $F'_k(x)$, $k \geqslant 1$, and J. Śliwa in [24] obtained an asymptotic formula for these functions.



W. Narkiewicz in [15] deduced certain asymptotics for $F_k(x)$.

Using our Main Lemma we can easily improve also those results.

It seems of importance to mention the constants appearing in (1.1)–(1.6). The constants in the exponents (also the degrees of the polynomials appearing there) usually depend on the structure of the group of ideal classes or on the structure of other groups, for instance on the Galois group $\mathrm{Gal}(\bar{K}_H/Q)$, where $\bar{K}_H$ is the Hilbert class field of $\bar{K}$, the normal hull of $K/Q$ (see [14], [15], [18], [23]).

If we want to determine these constants explicitly, we meet difficulties of combinatorial nature (see [17]). Hence the precise values of these constants are known only in some special cases.

It would also be interesting to determine explicitly the coefficients of the polynomials appearing in the above asymptotic formulas and to estimate the constants implied by the $O$-notation.

These constants depend on many parameters of the field, such as degree, discriminant, fundamental units, etc.

Estimating the constants in the remainder terms of (1.2), (1.4), (1.6) requires the application of an effective zero free region for the Hecke zeta function (compare [8]).

**2. The Main Lemma.** The basic role in the proofs of the theorems stated in 1 will be played by a lemma on the asymptotic behaviour of the coefficient sum of the series

$$(2.1)\qquad f(s) = \sum_{n=1}^{\infty} a_n n^{-s}, \quad s = \sigma + it,\ a_n \geqslant 0,$$

satisfying certain regularity conditions.

To make the formulation of the Main Lemma simpler we introduce a class $\mathscr{A}$ of functions represented by Dirichlet's series (2.1) having the following properties:

(i) For $1 \leqslant x < y$,

$$(2.2)\qquad \sum_{x\leqslant n\leqslant y} a_n \leqslant (y-x)\log^{c_5} y + O(y^\theta),$$

where $c_5 > 0$, $\theta < 1$ are constants depending on $f$.

From (i) it follows that the series (2.1) is convergent in the half-plane $\sigma > 1$.

(ii) For $\sigma > 1$,

$$(2.3)\qquad f(s) = \sum_{0\leqslant j\leqslant r}\frac{g_j(s)}{(s-1)^{w_j}}\log^{k_j}\frac{1}{s-1} + g_{r+1}(s),$$

where $k_j \geqslant 0$, $j = 0, \ldots, r$ are integers, $w_j = u_j + iv_j$, $j = 0, \ldots, r$ are complex numbers whose real parts are non-negative, the functions $g_j(s)$, $j = 0, 1, \ldots, r+1$ are regular for $\sigma > 1$ and can be continued analytically to regular and single-valued functions in the region

$$\sigma > 1 - \frac{c_6}{\log(|t|+2)}, \quad c_6 > 0. \tag{2.4}$$

Condition (ii) secures analytic continuation of $f(s)$ to the left of the line $\sigma = 1$.

(iii) In the region (2.4)

$$|g_j(s)| \leqslant (|t|+2)^{u_j} \log^{c_7}(|t|+3). \tag{2.5}$$

(iv) In (2.3) $w_0$ is a real number, $w_0 \geqslant u_1 \geqslant \ldots \geqslant u_r$ and, moreover, if $u_j = w_0$ for certain $j$, $0 \leqslant j \leqslant r$, then $w_j$ is also real.

It is convenient to distinguish the following two cases.

Case I. All $w_j$ are equal to zero. In this case we assume that $k_0 > k_1 > \ldots > k_r$ and $g_0(1) \neq 0$.

Case II. Not all $w_j$ vanish. If in this case $w_0 = w_1 = \ldots = w_{r_1}$ for certain $r_1 \leqslant r$ then we assume that $k_0 > k_1 > \ldots > k_{r_1}$ and $g_0(1) \neq 0$.

We can now formulate the

Main Lemma. *Let $f(s) \in \mathscr{A}$. Then for the summatory function*

$$S(x) = \sum_{n \leqslant x} a_n$$

*of (2.1), for $x \geqslant e^e$ and any integer $q$ satisfying $0 \leqslant q \leqslant c_8 \dfrac{\sqrt{\log x}}{\log\log x}$ we have the following estimates:*

*in case* I

$$S(x) = k_0 g_0(1) \frac{x}{\log x} \sum_{0 \leqslant \mu \leqslant q} \frac{P_\mu(\log\log x)}{(\log x)^\mu} + O\left((c_9 q)^q \frac{x(\log\log x)^{c_9}}{(\log x)^{q+2}}\right) \tag{2.6}$$

*where $P_\mu(x) \in C[x]$, $\deg P_\mu(x) \leqslant \max k_j$, $\deg P_0(x) = k_0 - 1$ and its leading coefficient is equal to* 1;

*in case* II

$$S(x) = \frac{g_0(1)}{\Gamma(w_0)} \frac{x}{(\log x)^{1-w_0}} \sum_{\mu \in M_q} \frac{Q_\mu(\log\log x)}{(\log x)^\mu} + O\left((c_9 q)^q \frac{x(\log\log x)^{c_9}}{(\log x)^{q+2-w_0}}\right), \tag{2.7}$$

*where $Q_\mu(x) \in C[x]$, $\deg Q_\mu(x) \leqslant \max k_j$, $\deg Q_0(x) = k_0$ and its leading coefficient is equal to* 1.

*$M_q$ denotes the finite set of complex numbers $\mu$ lying in the strip $0 \leqslant \operatorname{Re}\mu < q+1$ which are of the form $\mu = \nu + w_0 - w_j$, $\nu \in Z$, $0 \leqslant \nu \leqslant q$.*



*The constants implied by O-notation and the constants $c_8, c_9$ depend on $f$ and do not depend on $x$ and $q$.*

*The polynomials $P_\mu(x)$ and $Q_\mu(x)$ depend on $w_0, \ldots, w_r$, $k_0, \ldots, k_r$ and*

$$P_\mu(x) = \frac{1}{k_0 g_0(1)} W_\mu(x), \quad Q_\mu(x) = \frac{\Gamma(w_0)}{g_0(1)} W_\mu(x),$$

*where*

$$W_\mu(x) = \sum_{0 \leqslant j \leqslant r} \sum_{\substack{0 \leqslant \nu \leqslant q \\ \nu + w_0 - w_j = \mu}} \sum_{0 \leqslant \varkappa \leqslant k_j} A_{j\nu} B_{j\varkappa\nu} x^\varkappa.$$

*The numbers $A_{j\nu}$ are the coefficients of the Taylor expansion of $(1/s) g_j(s)$ in the neighbourhood of $s = 1$, and $B_{j\varkappa\nu}$ are given by*

$$B_{j\varkappa\nu} = (-1)^{k_j - \varkappa} \binom{k_j}{\varkappa} \frac{1}{2\pi i} \int_{\mathscr{C}_0} e^z z^{\nu - w_j} (\log z)^{k_j - \varkappa} dz$$

*where $\mathscr{C}_0$ denotes the curve of integration consisting of the segment $[-\infty, -1]$ of the lower side of the real axis, the circumference $C(0,1)$ and the segment $[-1, -\infty]$ of the upper side of the real axis.*

The ideas leading us to the Main Lemma can be found in many papers ([3], [4], [8]–[11], [18], [21], [22]) and the method of the proof of this lemma is classical.

A similar result has been obtained by E. J. Scourfield [21].

She assumes about the functions (2.1) that for $\sigma > 1$

$$f(s) = \{\zeta(s)\}^{1-\beta} \{\log \zeta(s)\}^u H(s) h(s) \tag{2.8}$$

where $0 < \beta \leqslant 1$, $u$ is a non-negative integer and $H(s)$ is a product of powers of Dirichlet $L$-functions associated with non-principal characters, which are non-negative powers of the logarithm of such functions, and $h(s)$ is a function holomorphic for $\sigma > 1/2$ and bounded for $\sigma > 1/2 + \delta$ $(\delta > 0)$.

Then she estimates $S(x)$, making various assumptions about $\beta$ and $u$. For instance, assuming that $0 < \beta < 1$, $u \geqslant 1$, she proves

$$S(x) = \frac{H(1) h(1)}{\Gamma(1-\beta)} \frac{x(\log\log x)^u}{\log^\beta x} + O\left(\frac{x(\log\log x)^{u-1/2}}{\log^\beta x}\right).$$

It follows that the assertion in E. J. Scourfield's theorem is weaker than the assertion of our lemma. On the other hand, it is easily seen that if $f(s)$ satisfies (2.8) then it satisfies conditions (ii)–(iv) in the definition of the class $\mathscr{A}$. It can be shown that in the case where $h(s)$ is an absolutely convergent Dirichlet series (which mostly takes place in applications) then condition (i) is also a consequence of (2.8).

Conditions (i)–(iv) could be modified. Namely we could replace (i) by the following weaker condition:

(i′) For any fixed constant $c_{10} > 0$ there exists a constant $c_{11} > 0$ such that for a sufficiently large $x$

$$\sum_{x \leqslant n \leqslant x + x\exp(-c_{10}\sqrt{\log x})} a_n \ll x\exp(-c_{11}\sqrt{\log x}).$$

It seems very probable that condition (i) can be completely eliminated. However, since this condition is easy to verify in most applications, we prefer to discuss this problem on another occasion.

Condition (iv) could be completely omitted, however, the formulation of the Main Lemma would then become more complicated.

We could also consider $q$ as a function of $x$. Then the number of terms in the asymptotic formula would depend on $x$ and the remainder would be of the magnitude

$$\ll x\exp(-c\sqrt{\log x}).$$

In this case we might also assume in (ii) that the functions could be continued analytically to larger regions and by the modification of (iii) we could get much smaller remainders (compare [9]).

**3. Proof of the Main Lemma.** The constants $c_{12}, c_{13}, \ldots$ will depend upon $f$.

Let $\delta := 1/\log x$. Consider the following arcs:

$$\begin{aligned}
&\mathscr{C}_1\colon\ \sigma = 1 - c_{12}/\log(|t|+2),\ t < -\delta,\ 0 < c_{12} < c_6,\\
&\mathscr{C}_2\colon\ t = -\delta,\ 1 - \big(c_{12}/\log(\delta+2)\big) \leqslant \sigma \leqslant 1,\\
&\mathscr{C}_3\colon\ s = 1 + \delta e^{i\varphi},\ -\pi/2 \leqslant \varphi \leqslant \pi/2,\\
&\mathscr{C}_4\colon\ t = \delta,\ 1 - \big(c_{12}/\log(\delta+2)\big) \leqslant \sigma \leqslant 1,\\
&\mathscr{C}_5\colon\ \sigma = 1 - \big(c_{12}/\log(|t|+2)\big),\ t > \delta,\\
&\mathscr{C}_1'\colon\ t = -\delta,\ \sigma \leqslant 1 - \big(c_{12}/\log(\delta+2)\big),\\
&\mathscr{C}_5'\colon\ t = \delta,\ \sigma \leqslant 1 - \big(c_{12}/\log(\delta+2)\big).
\end{aligned} \tag{3.1}$$

Finally denote

$$\mathscr{C} = \mathscr{C}_1 \cup \mathscr{C}_2 \cup \mathscr{C}_3 \cup \mathscr{C}_4 \cup \mathscr{C}_5 \quad \text{and} \quad \mathscr{C}' = \mathscr{C}_1' \cup \mathscr{C}_2 \cup \mathscr{C}_3 \cup \mathscr{C}_4 \cup \mathscr{C}_5'.$$

From (ii) it follows that for $s \in \mathscr{C}$

$$|f(s)| \ll \begin{cases} \log^{c_{13}} x & \text{for } |t| \leqslant 1,\\ \log^{c_{13}}(|t|+2) & \text{for } |t| > 1. \end{cases} \tag{3.2}$$



Using the Perron summation formula with weights $\log(x/n)$, we obtain for $x \geqslant e^e$

$$T(x) := \sum_{n \leqslant x} a_n \log\frac{x}{n} = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{x^s}{s^2} f(s)\,ds = \frac{1}{2\pi i}\int_{\mathscr{C}} \frac{x^s}{s^2} f(s)\,ds. \tag{3.3}$$

We have

$$\Big|\int_{\mathscr{C}_1 \cup \mathscr{C}_5} \frac{x^s}{s^2} f(s)\,ds\Big| \ll x\exp(-c_{14}\sqrt{\log x}). \tag{3.4}$$

Indeed

$$\Big|\int_{\mathscr{C}_1 \cup \mathscr{C}_5} \frac{x^s}{s^2} f(s)\,ds\Big| \leqslant 2\Big|\int_{\mathscr{C}_5} \frac{x^s}{s^2} f(s)\,ds\Big|$$
$$\ll \Big(\int_{\delta}^{1} + \int_{1}^{\exp(\sqrt{\log x})} + \int_{\exp(\sqrt{\log x})}^{\infty}\Big) \frac{x^\sigma}{|s|^2}|f(s)|\,|ds|.$$

By the use of (3.2) these integrals are easy to estimate and (3.4) follows.

Now choose $\xi := x\exp(-c_{15}\sqrt{\log x})$, $0 < c_{15} < c_{14}$.

Then

$$T(x+\xi) - T(x) = \log\big(1 + (\xi/x)\big)S(x) + H$$

and by (i)

$$H = \sum_{x < n \leqslant x+\xi} a_n \log\frac{x+\xi}{n} \ll x\log\Big(1 + \frac{\xi}{x}\Big)\exp(-c_{16}\sqrt{\log x}), \tag{3.5}$$

whence

$$S(x) = \log^{-1}\Big(1 + \frac{\xi}{x}\Big)\frac{1}{2\pi i}\int_{\mathscr{C}_2 \cup \mathscr{C}_3 \cup \mathscr{C}_4} \frac{(x+\xi)^s - x^s}{s^2} f(s)\,ds +$$
$$+ O\big(x\exp(-c_{17}\sqrt{\log x})\big).$$

Since

$$\log^{-1}\Big(1 + \frac{\xi}{x}\Big) = \frac{x}{\xi} + O(1) \quad \text{and} \quad (x+\xi)^s - x^s = s\xi x^{s-1} + O(\xi^2 x^{\sigma-2}),$$

it follows that

$$S(x) = \frac{1}{2\pi i}\int_{\mathscr{C}_2 \cup \mathscr{C}_3 \cup \mathscr{C}_4} \frac{x^s}{s} f(s)\,ds + O\big(x\exp(-c_{18}\sqrt{\log x})\big).$$

Applying (ii), we find that

$$(3.6)\qquad S(x) = \sum_{0\leqslant j\leqslant r} \frac{1}{2\pi i} \int_{\mathscr{C}_2\cup\mathscr{C}_3\cup\mathscr{C}_4} \frac{x^s g_j(s)}{s(s-1)^{w_j}} \log^{k_j}\frac{1}{s-1}\, ds + \frac{1}{2\pi i} \int_{\mathscr{C}_2\cup\mathscr{C}_3\cup\mathscr{C}_4} \frac{x^s}{s}\, g_{r+1}(s)\, ds + O\big(x\exp(-c_{19}\sqrt{\log x})\big).$$

If $\eta > 0$ is such that $K_\eta = \{s \mid |s-1| < \eta\}$ is contained in the region (2.4) and contains $\mathscr{C}_2\cup\mathscr{C}_3\cup\mathscr{C}_4$, then for any $q \geqslant 0$ and $s \in K_\eta$

$$\frac{1}{s}\, g_j(s) = \sum_{\nu\geqslant 0} A_{j\nu}(s-1)^\nu = \sum_{0\leqslant\nu\leqslant q} A_{j\nu}(s-1)^\nu + O(c_{20}^q |s-1|^{q+1}).$$

For every $j = 0, \ldots, r+1$ we have the estimate

$$\int_{\mathscr{C}_2\cup\mathscr{C}_3\cup\mathscr{C}_4} x^s(s-1)^{q+1-w_j}\log^{k_j}\frac{1}{s-1}\, ds \ll (q+1)\frac{x(\log\log x)^{c_{21}}}{(\log x)^{q+2-w_0}}$$

and thus

$$(3.7)\qquad S(x) = \sum_{0\leqslant j\leqslant r}\sum_{0\leqslant\nu\leqslant q} \frac{A_{j\nu}}{2\pi i} \int_{\mathscr{C}_2\cup\mathscr{C}_3\cup\mathscr{C}_4} x^s(s-1)^{\nu-w_j}\log^{k_j}\frac{1}{s-1}\, ds + \sum_{0\leqslant\nu\leqslant q} \frac{A_{r+1,\nu}}{2\pi i} \int_{\mathscr{C}_2\cup\mathscr{C}_3\cup\mathscr{C}_4} x^s(s-1)^\nu\, ds + O\left((c_{22}q)^q \frac{x(\log\log x)^{c_{23}}}{(\log x)^{q+2-w_0}}\right).$$

Since $q \leqslant c_8 \dfrac{\sqrt{\log x}}{\log\log x}$, the error term in (3.6) is smaller than that in (3.7).

In the above formula we replace the curve of integration by $\mathscr{C}'$; this involves an error

$$\ll R_q(x) = (c_{24}q)^q \frac{x(\log\log x)^{c_{25}}}{(\log x)^{q+2-w_0}}.$$

Let $\mathscr{C}'' = \mathscr{C}_1''\cup\mathscr{C}_2''\cup\mathscr{C}_3\cup\mathscr{C}_3''\cup\mathscr{C}_4''$ where

$\mathscr{C}_1''$: $t = 0$, $\sigma < 1-\delta$, $\arg s = -\pi$,

$\mathscr{C}_2''$: $s = 1+\delta e^{i\varphi}$, $-\pi \leqslant \varphi \leqslant -\pi/2$,

$\mathscr{C}_3''$: $s = 1+\delta e^{i\varphi}$, $\pi/2 \leqslant \varphi \leqslant \pi$,

$\mathscr{C}_4''$: $t = 0$, $\sigma < 1-\delta$, $\arg s = \pi$.

By Cauchy's theorem we can take $\mathscr{C}''$ in place of $\mathscr{C}'$ in (3.7).



We then make the substitution $z = (s-1)\log x$ and write

$$S(x) = \sum_{0\leqslant j\leqslant r}\sum_{0\leqslant\nu\leqslant q} \frac{A_{j\nu}x}{(\log x)^{\nu-w_j+1}} \frac{1}{2\pi i}\int_{\mathscr{C}_0} e^z z^{\nu-w_j}\log^{k_j}\left(\frac{\log x}{z}\right) dz + R_q(x)$$

$$= \sum_{0\leqslant j\leqslant r}\ \sum_{\substack{0\leqslant\nu\leqslant q\\ \nu-u_j<q-w_0+1}}\ \sum_{0\leqslant\varkappa\leqslant k_j} A_{j\nu}B_{j\varkappa\nu}\frac{x}{(\log x)^{\nu-w_j+1}}(\log\log x)^\varkappa + R_q(x)$$

$$= \frac{x}{(\log x)^{1-w_0}}\sum_{\mu\in M_q}\frac{W_\mu(\log\log x)}{(\log x)^\mu} + R_q(x),$$

where

$$W_\mu(x) = \sum_{0\leqslant j\leqslant r}\ \sum_{\substack{0\leqslant\nu\leqslant q\\ \nu+w_0-w_j=\mu}}\ \sum_{0\leqslant\varkappa\leqslant k_j} A_{j\nu}B_{j\varkappa\nu}x^\varkappa.$$

This shows that $W_\mu(x) \in C[x]$ and $\deg W_\mu(x) \leqslant \max k_j$. To compute $\deg W_0(x)$ we must treat the cases I and II separately.

Case I. Since

$$W_0(x) = \sum_{0\leqslant j\leqslant r}\sum_{0\leqslant\varkappa\leqslant k_j} A_{j0}B_{j\varkappa 0}x^\varkappa,$$

the leading coefficient of this polynomial is

$$A_{00}B_{0k_00} = \frac{g_0(1)}{2\pi i}\int_{\mathscr{C}_0} e^z\, dz = 0.$$

The term $x^{k_0-1}$ has the coefficient

$$\sum_{\substack{0\leqslant j\leqslant r\\ k_j=k_0-1}} A_{j0}B_{j,k_0-1,0} + A_{00}B_{0,k_0-1,0} = k_0 g_0(1) \neq 0,$$

and we see that $\deg W_0(x) = k_0-1$. This proves the lemma in this case. It remains to prove our lemma in case II.

We have

$$W_0(x) = \sum_{0\leqslant j\leqslant r_1}\sum_{0\leqslant\varkappa\leqslant k_j} A_{j0}B_{j\varkappa 0}x^\varkappa$$

and the leading coefficient is

$$A_{00}B_{0k_00} = \frac{g_0(1)}{2\pi i}\int_{\mathscr{C}_0} e^z z^{-w_0}\, dz = \frac{g_0(1)}{\Gamma(w_0)} \neq 0.$$

Thus $\deg W_0(x) = k_0$ and the proof of the Main Lemma is completed.

**4. Dedekind and Hecke zeta function.** In what follows $b_1, b_2, \ldots$ denote positive constants which, as well as the constants implied by the $O$-notation, depend only upon $K$ unless their dependence upon other parameters is indicated.

Let $\chi$ be an arbitrary Hecke character of finite order. Denote by $\mathfrak{f}$ its conductor. The Hecke zeta function is defined for $s = \sigma+it$, $\sigma > 1$ by an absolutely convergent Dirichlet series

$$\zeta_K(s, \chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s},$$

the sum being taken over all non-zero ideals of $R_K$.

Taking $\chi = \chi_0$ (trivial character) and $\mathfrak{f} = R_K$, we obtain the Dedekind zeta function $\zeta_K(s)$.

We now list some basic results concerning the zeta-functions which appear explicitly or implicitly in [13].

I. The functions $\zeta_K(s, \chi)$ can be continued analytically over the whole complex plane as regular functions except $\zeta_K(s, \chi_0)$ which has a simple pole at $s = 1$.

II. In the region

$$\sigma > 1 - \frac{b_1(\mathfrak{f})}{\log(|t|+2)}$$

$\zeta_K(s, \chi)$ does not vanish.

III. In the above region for $|t| \geqslant 1$ we have

$$|\log \zeta_K(s, \chi)| \ll_{\mathfrak{f}} \log\log(|t|+e^e)$$

and

$$\log^{-b_2(\mathfrak{f})}(|t|+2) \ll |\zeta_K(s, \chi)| \ll \log^{b_2(\mathfrak{f})}(|t|+2).$$

**5. The ring $\Omega$.** Let $\Omega_0$ denote the ring of all Dirichlet series with abscissas of absolute convergence $< 1$.

Let $\Omega$ be the smallest ring which contains $\Omega_0$ and also all functions of the form:

(a) $\zeta_L^w(s)$, where $L$ runs over all finite extensions of rationals, $w$ is a complex number, and $\operatorname{Re} w \geqslant 0$,

(b) $\zeta_L^w(s, \chi)$, where $L$ is as above, $w$ is arbitrary complex number, and $\chi$ is a non-principal Hecke character of finite order,

(c) $\log^k \zeta_L(s, \chi)$, where $L$ is as above, $k$ is a natural number and $\chi$ is a Hecke character of finite order.

From the proof of the well-known Čebotarev density theorem [7] it follows that

$$\sum_{\mathfrak{p} \in \mathscr{P}} (N\mathfrak{p})^{-s} \in \Omega$$



for an arbitrary Čebotarev set of prime ideals $\mathscr{P}$. Note that the set of prime ideals belonging to a fixed class $X$ from $H(K)$ is a Čebotarev set.

The ring $\Omega$ defined above contains the most important functions which are used in the theory of numbers.

Let $A$ be any set of integral ideals of $R_K$. To avoid endless repetitions we adopt the following notation:

$$f_A(m) = \sum_{\substack{N\mathfrak{a}=m \\ \mathfrak{a}\in A}} 1, \quad m = 1, 2, \ldots,$$

$$\zeta(s, A) = \sum_{m \geqslant 1} \frac{f_A(m)}{m^s}, \quad \sigma > 1.$$

If $A \subset R_K$ and $A_0 := \{\mathfrak{a} \mid \mathfrak{a} = aR_K,\ a \in A\}$ then $\zeta(s, A) := \zeta(s, A_0)$.

It is convenient to prove the following

Proposition 1. *If $A$ is a set of integral ideals of $K$ (or $A \subset R_K$) such that $\zeta(s, A) \in \Omega$, then $\zeta(s, A)$ satisfies conditions* (i)–(iii) *of the class $\mathscr{A}$.*

Proof. (i) follows from the well-known theorem of Landau, [12],

$$\sum_{N\mathfrak{a} \leqslant x} 1 = a_K x + O(x^{(n-1)/(n+1)}), \quad x \geqslant 1,$$

where

$$a_K = \operatorname*{res}_{s=1} \zeta_K(s) \quad \text{and} \quad n = [K:Q].$$

Indeed, for $1 \leqslant x < y$

$$\sum_{x \leqslant m \leqslant y} f_A(m) \leqslant \sum_{x \leqslant N\mathfrak{a} \leqslant y} 1 = a_K(y-x) + O(y^{(n-1)/(n+1)}).$$

If $\zeta(s, A) \in \Omega$ then $\zeta(s, A)$ is a sum of a finite number of terms of the form

$$g(s) \prod_L \zeta_L^{w_L}(s) \prod_{\chi \neq \chi_0} \zeta_{L_\chi}^{w_\chi}(s, \chi) \prod_\chi \log^{k_\chi} \zeta_{L_\chi}(s, \chi),$$

where $g(s) \in \Omega_0$, $\operatorname{Re} w_L \geqslant 0$, $k_\chi \in N$ and $L$ runs over a finite family of algebraic number fields, and the second and the third product is taken over a finite set of Hecke's characters.

Since

$$\zeta_L^{w_L}(s) = \frac{\big((s-1)\zeta_L(s)\big)^{w_L}}{(s-1)^{w_L}}$$

and for $\chi = \chi_0$

$$\log^{k_\chi} \zeta_{L_\chi}(s, \chi) = \sum_{0 \leqslant \nu \leqslant k_\chi} \binom{k_\chi}{\nu} \log^\nu \frac{1}{s-1} \log^{k_\chi - \nu}\big((s-1)\zeta_{L_\chi}(s, \chi)\big),$$

we have for $\sigma > 1$

$$\zeta(s, A) = \sum_{0\leqslant j\leqslant r} \frac{g_j(s)}{(s-1)^{w_j}} \log^{k_j}\frac{1}{s-1} + g_{r+1}(s).$$

From properties I–III of the zeta functions, it follows that $g_j(s)$ can be continued analytically to the region

$$\sigma > 1 - \frac{b_3}{\log(|t|+2)},$$

and in this region

$$|g_j(s)| \ll (|t|+2)^{u_j}\log^{b_4}(|t|+2).$$

This completes the proof of (ii) and (iii).

**6. Lemmas.** For a given natural number $i$, $1\leqslant i\leqslant h$, and an arbitrary integral ideal $\mathfrak{a}\neq R_K$ denote by $\Omega_i(\mathfrak{a}) = \Omega_{X_i}(\mathfrak{a})$ the number of prime ideals of $X_i$ dividing $\mathfrak{a}$, each counted according to its multiplicity, i.e.,

$$\Omega_i(\mathfrak{a}) = \sum_{\substack{\mathfrak{p}^k\|\mathfrak{a}\\ \mathfrak{p}\in X_i}} k.$$

Lemma 1. *Let $d_1, \ldots, d_h$ denote given non-negative (not all vanishing) rational integers. Then for the function*

$$F(x, d_1, \ldots, d_h) = \sum_{\substack{N\mathfrak{a}\leqslant x\\ \Omega_i(\mathfrak{a})=d_i\\ (i=1,\ldots,h)}} 1$$

*for $x\geqslant e^e$ and $q\in Z$ with $0\leqslant q\leqslant b_5\dfrac{\sqrt{\log x}}{\log\log x}$ we have the following formula:*

$$F(x, d_1, \ldots, d_h) = \frac{x}{\log x}\sum_{0\leqslant\mu\leqslant q}\frac{R_\mu(\log\log x)}{(\log x)^\mu} + O\left((b_6 q)^q\frac{x(\log\log x)^{b_6}}{(\log x)^{q+2}}\right)$$

*where $R_\mu(x)\in C[x]$, $\deg R_\mu(x)\leqslant d_1+\ldots+d_h$ for $\mu\geqslant 1$ and $\deg R_0(x) = d_1+\ldots+d_h-1$.*

Proof. Denote by $\mathscr{F} = \mathscr{F}(d_1, \ldots, d_h)$ the set of all ideals of $R_K$ for which $\Omega_i(\mathfrak{a}) = d_i$ holds for $i = 1, \ldots, h$.

Then for $\sigma > 1$ we have

$$\zeta(s, \mathscr{F}) = \prod_{1\leqslant i\leqslant h}\sum_{k\geqslant 1}\sum_{m_1\geqslant 1}\cdots\sum_{\substack{m_k\geqslant 1\\ m_1+\ldots+m_k=d_i}}\frac{1}{k!}\frac{P_i(m_1 s)\ldots P_i(m_k s)}{m_1\ldots m_k},$$



where

$$P_i(s) = \sum_{\mathfrak{p}\in X_i}(N\mathfrak{p})^{-s}\in\Omega,$$

and we observe that Lemma 1 follows from Proposition 1 and the Main Lemma (case I with $k_0 = d_1+\ldots+d_h$).

Lemma 2. *Let $h > 1$, $Y_1, \ldots, Y_m$, $1\leqslant m < h$ be given distinct classes of $H(K)$ and let $d_i\geqslant 0$ $(i = 1, \ldots, m)$ be rational integers such that $Y_1^{d_1}\ldots Y_m^{d_m}Y^{-1}$ belongs to the subgroup of $H(K)$ generated by $H(K)\setminus\{Y_1, \ldots, Y_m\}$. Here $Y$ denotes an arbitrary element of $H(K)$.*

*Let us put*

$$F_Y(x, d_1, \ldots, d_m) = \sum_{\substack{N\mathfrak{a}\leqslant x\\ \mathfrak{a}\in Y, \Omega_{Y_i}(\mathfrak{a})=d_i\\ (i=1,\ldots,m)}} 1.$$

*Then for $x\geqslant e^c$ we have*

$$F_Y(x, d_1, \ldots, d_m) = \frac{x}{(\log x)^{m/h}}V(\log\log x) + O\left(\frac{x(\log\log x)^{b_x}}{(\log x)^{m/h+\gamma}}\right),$$

*where $V(x)\in C[x]$, $\deg V(x) = d_1+\ldots+d_m$ and $\gamma = \dfrac{1}{h}\left(1-\cos\dfrac{2\pi}{h}\right)$.*

Proof (compare [23]). Let $\mathscr{F}_Y = \mathscr{F}_Y(d_1, \ldots, d_m)$ denote the set of all ideals of $R_K$ belonging to $Y$ for which $\Omega_{Y_i}(\mathfrak{a}) = d_i$ holds for $i = 1, \ldots, m$.

From [23] it follows that $\zeta(s, \mathscr{F}_Y)\in\Omega$ and for $\sigma > 1$ we can write

$$\zeta(s, \mathscr{F}_Y) = (s-1)^{m/h-1}\left(\log\frac{1}{s-1}\right)^{d_1+\ldots+d_m}\sum_{\chi\in T}A^{(\chi)}(s) +$$
$$+(s-1)^{m/h-1}\Phi_0\left(\log\frac{1}{s-1}\right) + \sum_{\chi\notin T}(s-1)^{b(\chi)}\Phi_\chi\left(\log\frac{1}{s-1}\right),$$

where $T$ denotes a certain set of characters of $H(K)$, $\chi_0\in T$ and $\Phi_0$ and $\Phi_\chi$ are polynomials over the ring of all functions regular for $\sigma\geqslant 1$. The functions $A^{(\chi)}(s)$ and the coefficients of $\Phi_0$ and $\Phi_\chi$ are of the same type as the functions $g_j(s)$ in conditions (ii) and (iii) of class $\mathscr{A}$,

$$b(\chi) = \frac{1}{h}\sum_{1\leqslant i\leqslant m}\chi(Y_i)$$

and, for $\chi\notin T$, $-\mathrm{Re}\,b(\chi) < 1-m/h$.

Since for every class $Y_i$, $\chi(Y_i)$ is a $h$th root of unity, we can write for $\chi\notin T$

$$-\mathrm{Re}\,b(\chi)\leqslant 1-m/h-\gamma.$$

Moreover, for $\chi \in T$, $A^{(\chi)}(1) > 0$.

We see that we can apply case II of our Main Lemma. Putting $q = 0$ we obtain

$$F_Y(x, d_1, \ldots, d_m) = \frac{x}{(\log x)^{m/h}} \sum_{\mu \in M_0} \frac{V_\mu(\log\log x)}{(\log x)^\mu} + O\left(\frac{x(\log\log x)^{b_8}}{(\log x)^{m/h+1}}\right)$$

$$= \frac{x}{(\log x)^{m/h}} V_0(\log\log x) + O\left(\frac{x(\log\log x)^{b_7}}{(\log x)^{m/h+v_0}}\right),$$

where $v_0 > 0$ is the minimal real number for which there exists $\chi \notin T$ such that

$$v_0 = 1 - m/h + \operatorname{Re} b(\chi).$$

Thus $v_0 \geqslant \gamma$. Since $\deg V_0(x) = d_1 + \ldots + d_m$, this completes the proof.

Remark. If $Y_1^{d_1} \ldots Y_m^{d_m} Y^{-1}$ does not belong to the subgroup of $H(K)$ generated by $H(K) \setminus \{Y_1, \ldots, Y_m\}$, then $F_Y(x, d_1, \ldots, d_m) = 0$.

**7. Proof of Theorem 1.** Denote by $V$ the set of all sequences $[d_1, \ldots, d_h]$ such that

$$X_1^{d_1} \ldots X_h^{d_h}$$

equals $E$ and, moreover, the product

$$X_1^{e_1} \ldots X_h^{e_h} \quad (0 \leqslant e_i \leqslant d_i)$$

is equal to $E$ if and only if either all $e_i$'s are zero or $e_i = d_i$ holds for $i = 1, \ldots, h$.

Then

$$M(x) = \sum_{[d_1,\ldots,d_h] \in V} \sum_{\substack{N\mathfrak{a} \leqslant x \\ \Omega_i(\mathfrak{a}) = d_i \\ (i=1,\ldots,h)}} 1 = \sum_{[d_1,\ldots,d_h] \in V} F(x, d_1, \ldots, d_h)$$

and application of Lemma 1 completes the proof of Theorem 1.

**8. Proof of Theorem 2 (compare [23]).** For any system (see [23]), $S = \langle U, A \rangle$ ($A = \{A_X \mid X \in H(K) \setminus U\}$, $A_X$ positive integers) and $d \geqslant 0$ let us put

$$N_S = \{\mathfrak{a} \in R_K \mid \Omega_X(\mathfrak{a}) = A_X, \ (X \notin U)\},$$

$$N_S[d] = \{\mathfrak{a} \in N_S \mid \Omega_X(\mathfrak{a}) > d, \ (X \in U)\}.$$

There exists a finite set $L$ of systems such that with suitable integers $d_S$ $(S \in L)$ we have

$$G_k = \bigcup_{S \in L} N_S[d_S] \quad ([23], \text{ corollary to Lemma 9}).$$



Moreover, for any system $S = \langle U, A \rangle$ and $d \geqslant 0$ we have

$$N_S[d](x) = N_S(x) + O\left(\frac{x(\log\log x)^{b_9}}{(\log x)^{1-|U|/h+1/h}}\right) \quad \text{(compare [23], Lemma 9);}$$

thus by Lemma 2

$$N_S[d](x) = \frac{x V_S(\log\log x)}{(\log x)^{1-|U|/h}} + O\left(\frac{x(\log\log x)^{b_{10}}}{(\log x)^{1-|U|/h+\gamma_0}}\right),$$

where $V_S(x) \in C[x]$.

Let $S_1, S_2$ be two distinct systems and assume that the sets $N_{S_1}, N_{S_2}$ are both non-empty.

Of course $N_{S_1} \cap N_{S_2} = \emptyset$ or $N_{S_1} \cap N_{S_2} = N_{S_{12}}$ for a certain system $S_{12}$. The length of $S_{12}$ is less than the maximal length of $S_1$ and $S_2$.

This implies that

$$G_k(x) = \sum_{S \in L} N_S[d_S](x) + O\left(\frac{x(\log\log x)^{b_{11}}}{(\log x)^{1-t_k/h+1/h}}\right)$$

$$= \frac{x W(\log\log x)}{(\log x)^{1-t_k/h}} + O\left(\frac{x(\log\log x)^{b_{12}}}{(\log x)^{1-t_k/h+\gamma_0}}\right),$$

where $t_k = t_k(K)$ denotes the maximal length of the systems from $L$ and the proof of Theorem 2 is completed.

**9. Proof of Theorem 3.** The proof of Theorem 3 follows *mutatis mutandis* from [18] if we apply the Main Lemma instead of the analytic argument used by R. W. K. Odoni.

We only mention that it is proved in [18], in view of the Čebotarev density theorem, that $\zeta(s, F_1') \in \Omega$ and that for $\sigma > 1$

$$\zeta(s, F_1') = \frac{\Phi\left(\log \frac{1}{s-1}\right)}{(s-1)^E},$$

where $\Phi$ is a function of the same type as $\Phi_0$ in the proof of Lemma 2 of the present paper.

### References


[1] S. Allen, *On the factorisation of natural numbers in an algebraic number field*, J. London Math. Soc. 11 (1975), pp. 294–300.

[2] H. Delange, *Généralisation du théorème de Ikehara*, Ann. Sci. École Norm. Sup. 71 (1954), pp. 213–242.

[3] — *Sur la distribution des entiers ayant certaines propriétés*, ibid. 73 (1956), pp. 15–74.

[4] H. Delange, *Sur des formules de Atle Selberg*, Acta Arith. 19 (1971), pp. 105–146.
[5] E. Fogels, *Zur Arithmetik quadratischer Zahlenkörper*, Wissenschaftliche Abhandlungen der Universität Riga, Kl. Math., Abt. 1 (1943), pp. 23–47.
[6] G. H. Hardy and M. Riesz, *The general theory of Dirichlet series*, Cambridge 1915.
[7] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Würzburg 1965.
[8] J. Kaczorowski, *On completely irreducible algebraic integers*, to appear in Coll. Math. Soc. János Bolyai 34.
[9] G. Kolesnik and E. G. Straus, *On the distribution of integers with a given number of prime factors*, Acta Arith. 37 (1980), pp. 181–199.
[10] Й. Кубилюс, *Вероятностные методы в теории чисел*, Вильнюс 1962.
[11] J. Kubilius, *On local theorems for additive number theoretic functions*, Abhandlungen aus Zahlentheorie und Analysis, edited by P. Turán, Berlin 1968.
[12] E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Leipzig 1918.
[13] — *Über Ideale und Primideale in Idealklassen*, Math. Z. 2 (1918), pp. 52–154.
[14] W. Narkiewicz, *On natural numbers having unique factorization in a quadratic number field*, Acta Arith. 12 (1966), pp. 1–22.
[15] — *Numbers with unique factorization in an algebraic number field*, ibid. 21 (1972), pp. 313–322.
[16] — *Elementary and analytic theory of algebraic numbers*, Warszawa 1974.
[17] — *Finite abelian groups and factorization problems*, Colloq. Math. 42 (1979), pp. 319–330.
[18] R. W. K. Odoni, *On a problem of Narkiewicz*, J. Reine Angew. Math. 288 (1976), pp. 160–167.
[19] J. P. Rémond, *Évaluations asymptotiques dans partitions certaines semi-groupes*, C. R. Acad. Sci. Paris 260 (1965), pp. 6250–6251; 262 (1966), pp. A271–A273.
[20] — *Étude asymptotique de certaines partitions dans certaines semi-groupes*, Ann. Sci. École Norm. Sup. 83 (1966), pp. 343–410.
[21] E. J. Scourfield, *On the divisibility of $\sigma_\nu(n)$*, Acta Arith. 10 (1964), pp. 245–286.
[22] A. Selberg, *Note on a paper by L. G. Sathe*, J. Indian Math. Soc. 18 (1954), pp. 83–87.
[23] J. Śliwa, *Factorizations of distinct lengths in algebraic number fields*, Acta Arith. 31 (1976), pp. 399–417.
[24] — *A note on factorization in algebraic number fields*, Bull. Acad. Polon. Sci., Sér. Sci. Math. Astronom. Phys. 24 (1976), pp. 313–314.

INSTITUTE OF MATHEMATICS OF THE ADAM MICKIEWICZ UNIVERSITY
Poznań, Poland

*Received on 13. 1. 1982*
*and in revised form on 18. 6. 1982* (1285)

ACTA ARITHMETICA
XLIII (1983)

# On the 2-primary part of a conjecture of Birch and Tate

by

JERZY URBANOWICZ (Warszawa)

**1. Introduction.** The conjecture of Birch and Tate states that

$$|K_2 O_F| = w_F \zeta_F(-1),$$

where $O_F$ is the ring of integers of a totally real number field $F$, $\zeta_F$ is the Dedekind zeta function of $F$, $K_2$ is the functor of Milnor, and

$$w_F = 2 \prod_{l \text{ prime}} l^{n(l)}.$$

Here $n(l)$ is the maximal integer $n \geq 0$ such that $F$ contains the maximal real subfield of the cyclotomic field $Q(\zeta_{l^n})$.

The conjecture has recently been proved for abelian fields $F$ by B. Mazur and A. Wiles [8], up to the 2-primary part. In the present paper we investigate the divisibility of $w_F\zeta_F(-1)$ by powers of 2 for real quadratic fields $F$. It enables us, in view of a paper by J. Browkin and A. Schinzel [3], to prove the 2-primary part of the conjecture for infinitely many fields.

I wish to express my sincere thanks to J. Browkin and A. Schinzel for many helpful suggestions and ideas used in this paper.

**2. Notation.** Let $F = Q(\sqrt{D})$, where $D$ is a positive square-free integer, and let $d$ be the discriminant of $F$. Denote by $\left(\frac{a}{b}\right)$ the Kronecker symbol, and let $P_2(x) = x^2 - x + 1/6$ be the second Bernoulli polynomial.

It is easy to see that $w_F = 24k$, where $k = D$ for $D = 2$ or $5$, and $k = 1$ otherwise.

For a positive number $x$ and a positive integer $n$ let $A(x, n)$ be the number of positive integers $\leqslant x$ that are prime to $n$.

We know that

$$A\left(\frac{mn}{2}, n\right) = \frac{m}{2}\varphi(n), \tag{1}$$