J. Aust. Math. Soc. **79** (2005), 369–390

THE DISTRIBUTION OF THE IRREDUCIBLES IN AN ALGEBRAIC NUMBER FIELD

DAVID M. BRADLEY, ALI E. ÖZLÜK, REBECCA A. ROZARIO and C. SNYDER

(Received 26 January 2004; revised 18 November 2004)

Communicated by W. W. L. Chen

Abstract

We study the distribution of principal ideals generated by irreducible elements in an algebraic number field.

2000 *Mathematics subject classification*: primary 11R27.

1. Introduction

In an abstract algebra course, students learn that the concepts of prime and irreducible elements do not coincide in an integral domain without unique factorization. Usually, various examples are given in $\mathbb{Z}[\sqrt{-5}]$, for instance, showing the existence of irreducibles which are not prime. Of course, as every student knows any prime is irreducible and so generally there are more irreducibles than primes.

This difference leads naturally to two questions. First, can one give a characterization of irreducibles in familiar integral domains where unique factorization need not hold, such as the ring of integers in an algebraic number field? Second, how are the irreducibles distributed, again in an algebraic number field?

The problem of characterizing irreducibles involves, among many challenges, a good characterization of all the prime ideals in any given ideal class of the ideal class group of the field. This has a particularly nice solution when the Hilbert class field of the number field is an abelian extension of the field of rational numbers $\mathbb{Q}$, for class field theory shows us that the solution involves congruences, modulo certain

This manuscript is an extension of the third author's Masters thesis at University of Maine.

integers depending on only the field, for the rational primes contained in the prime ideals. (As a minor aside, we give a characterization of the irreducibles and primes in two imaginary quadratic number fields of class number two in the last section of this paper.) In other cases such a satisfactory characterization is not known and probably even nonexistent.

In this note, we study instead the distribution of irreducibles. First, we give a little background. Let K be an algebraic number field and denote by $M(x)$ the number of nonassociate irreducible elements α with $|N_{K/\mathbb{Q}}(\alpha)| \leq x$. In the 1960's, Rémond, [11], showed that

$$M(x) \sim C \frac{x}{\log x} (\log \log x)^{D-1}, \quad \text{as } x \to \infty,$$

where C is a positive constant not explicitly given and D is the Davenport constant which is a positive integer depending on only the structure of the ideal class group of K. Now, if we let $P(x)$ denote the number of nonassociate primes π with $|N_{K/\mathbb{Q}}(\pi)| \leq x$, then by a classical density result

$$P(x) \sim \frac{1}{h} \frac{x}{\log x},$$

where h is the class number of the field, that is, the order of the ideal class group. If $h > 1$ (so $D > 1$, see Section 2), then there are 'many more' irreducibles than primes. If $h = 1$, however, then the ring of integers is a unique factorization domain and hence the irreducibles and primes coincide. This is consistent with the estimates above once we observe that in this case, $C = 1$ and $D = 1$; see the next section for more on these constants.

Subsequently, Kaczorowski, [6], gave a major extension of Rémond's result, which we state here in simplified form:

$$M(x) = \frac{x}{\log x} \left(\sum_{j=0}^{D-1} m_j (\log \log x)^j \right) + O\left(\frac{x}{\log^2 x} (\log \log x)^c \right),$$

as $x \to \infty$, for some constant $c > 0$ and complex numbers m_j. In particular, $m_{D-1} = C$ the coefficient in Rémond's estimate. As in Rémond's case, the constants depend on K but are not explicitly given.

Later, Halter-Koch and Müller in joint work [5] showed, among many results, how to determine the constant C and as a result showed that it depends on only the class group of K.

This result prompted us to explore the dependence of some of the other coefficients in Kaczorowski's estimate on the arithmetic of K. In particular, we consider m_{D-2} and give an explicit expression for this coefficient. We then apply this to the special case of a number field with cyclic class group in which case we find that m_{D-2} contains explicit arithmetic information about the field and some of the subfields of its Hilbert class field. (We chose the case of cyclic class group due to the messy combinatorical arguments in the general case. It would still perhaps be of interest to see what happens in general.) Finally, we compute—more precisely, approximate—m_{D-2} for two imaginary quadratic number fields with class number two. Indeed, this calculation shows that more than just properties of the class group figure into the makeup of m_{D-2}.

2. A Dirichlet series associated with irreducibles

Let K be an algebraic number field, that is, a finite extension of the rational number field, $\mathbb{Q}$, and let $\mathcal{O}_K$ denote its ring of integers. We denote by $N(x)$ the norm of an element x from K to $\mathbb{Q}$. Also, we denote by $N\mathfrak{a}$ the norm of an ideal $\mathfrak{a}$ of $\mathcal{O}_K$. Furthermore, let $\mathrm{Cl} = \mathrm{Cl}(K)$ denote the class group of K and $h = h_K$ the class number, that is, the order of $\mathrm{Cl}(K)$.

In studying the distribution of the irreducibles, we introduce the following function.

DEFINITION 1. $\mu(s) = \sum_{(\alpha),\alpha \text{ irred.}} |N(\alpha)|^{-s}$, where s is a complex number with real part, $\sigma > 1$.

The sum runs over the principal ideals generated by irreducible elements of $\mathcal{O}_K$. We obviously do not wish to count all associates of an irreducible since there are infinitely many when the unit group is infinite, that is, anytime K is not $\mathbb{Q}$ or an imaginary quadratic number field.

Ultimately, we shall be interested in the 'summatory' function given by

DEFINITION 2. $M(x) = \sum_{(\alpha),\alpha \text{ irred.},|N(\alpha)|\le x} 1$, where x is any positive real number.

We shall first determine properties of $\mu(s)$ and then use a well-known Tauberian theorem to glean information about the distribution of $M(x)$.

To this end, consider the following. Write $\mathrm{Cl} = \{\mathfrak{c}_1 = 1, \mathfrak{c}_2, \ldots, \mathfrak{c}_h\}$.

DEFINITION 3. For each positive integer m, let

$$\mathscr{D}_m = \left\{ \underline{k} = (k_1, \ldots, k_h) \in \mathbb{N}_0^h : \prod_{j=1}^{h} \mathfrak{c}_j^{k_i} \overset{\min}{=} 1,\ k_1 + \cdots + k_h = m \right\},$$

where $\prod \mathfrak{c}_i^{k_i} \overset{\min}{=} 1$ means that $\prod \mathfrak{c}_i^{k_i} = 1$ and if $\prod \mathfrak{c}_i^{l_i} = 1$ for some l_i such that $0 \le l_i \le k_i$ for $i = 1, \ldots, h$, then $l_i = 0$ for all i or $l_i = k_i$ for all i. (Here $\mathbb{N}_0$ denotes the set of nonnegative integers.)

Notice that $\overset{\min}{=}$ guarantees that a product of elements is 1 but no nontrivial subproduct is 1. Hence the product gives a ‘minimal’ representation of 1.

Later on it will be more convenient to think of the elements of $\mathscr{D}_m$ as functions in the usual way; namely,

$$\mathscr{D}_m = \left\{\kappa : \mathrm{Cl} \to \mathbb{N}_0 \;\middle|\; \prod_{\mathfrak{c}\in\mathrm{Cl}} \mathfrak{c}^{\kappa(\mathfrak{c})} \overset{\min}{=} 1,\;\; \sum_{\mathfrak{c}} \kappa(\mathfrak{c}) = m\right\}.$$

DEFINITION 4. *The Davenport constant of* Cl, denoted by D or $D(\mathrm{Cl})$, is the largest positive integer m such that $\mathscr{D}_m$ is nonempty.

The Davenport constant is defined as above for any finite abelian group. In general, the relation between the Davenport constant and the structure of the group is not known. On the other hand, it is well known (and easy to prove) that the Davenport constant is no larger than the order of the group.

We now have the following proposition which gives a connection between irreducibles and prime ideals. First, we denote the set of nonzero prime ideals of $\mathscr{O}_K$ by $\mathscr{P}$.

PROPOSITION 2.1. *For any complex s with $\sigma > 1$ and where $\sum_{\mathfrak{a}_i}$ is defined to be* 1 *whenever $k_i = 0$,*

$$\mu(s) = \sum_{m=1}^{D} \sum_{\underline{k}\in\mathscr{D}_m} \prod_{i=1}^{h} \sum_{\substack{\mathfrak{a}_i \\ \exists\, \mathfrak{p}_{i1},\dots,\mathfrak{p}_{ik_i}\in\mathscr{P}\cap\mathfrak{c}_i \\ \mathfrak{a}_i=\mathfrak{p}_{i1}\cdots\mathfrak{p}_{ik_i}}} N(\mathfrak{a}_i)^{-s}.$$

PROOF. For $\underline{k} \in \mathscr{D}_m$, define

$$\mathscr{A}_{\underline{k}} = \left\{\mathfrak{a} : \mathfrak{a} = \mathfrak{a}_1\cdots\mathfrak{a}_h,\, \mathfrak{a}_i = \mathfrak{p}_{i1}\cdots\mathfrak{p}_{ik_i},\ \text{some } \mathfrak{p}_{ij} \in \mathscr{P}\cap\mathfrak{c}_i\right\},$$

where $\mathfrak{a}_i = 1$, if $k_i = 0$. Now let $\mathscr{A} = \bigcup \mathscr{A}_{\underline{k}}$ where the union is over all $\underline{k}$ in $\bigcup_m \mathscr{D}_m$. By the uniqueness of the factorization of ideals into prime ideals, we see that this union is disjoint. Moreover, by the multiplicativity of the norms, we have

$$\sum_{m=1}^{D} \sum_{\underline{k}\in\mathscr{D}_m} \prod_{i=1}^{h} \sum_{\mathfrak{a}_i} N\mathfrak{a}_i^{-s} = \sum_{\mathfrak{a}\in\mathscr{A}} N\mathfrak{a}^{-s},$$

where $\mathfrak{a}_i$ are as above in the definition of $\mathscr{A}_{\underline{k}}$. Now notice that if $\mathfrak{a} \in \mathscr{A}$, then $\mathfrak{a} \in \mathscr{A}_{\underline{k}}$ for some $\underline{k} \in \mathscr{D}_m$. Thus the ideal class $[\mathfrak{a}]$ containing $\mathfrak{a}$ satisfies

$$[\mathfrak{a}] = \prod_{i=1}^{h} \mathfrak{c}_i^{\,k_i} \overset{\min}{=} 1,$$

by definition of $\mathscr{D}_m$. Hence $\mathfrak{a} = (\alpha)$ for some nonzero, nonunit integer α in K. But notice that α must be irreducible for otherwise $[\mathfrak{a}] = \prod_{i=1}^{h} \mathfrak{c}_i{}^{k_i} = 1$, would not be a minimal representation of 1.

Conversely, if α is irreducible, then $(\alpha) \in \mathscr{A}_{\underline{k}}$ for some $\underline{k}$; namely,

$$(\alpha) = \prod_{i=1}^{h} \prod_{j=1}^{k_i} \mathfrak{p}_{ij},$$

for some $k_i \in \mathbb{N}_0$ and $\mathfrak{p}_{ij} \in \mathscr{P} \cap \mathfrak{c}_i$. □

Next, we examine the right-hand sum in the proposition above. To this end we define the following family of polynomials.

Definition 5. Let k be a positive integer and $z_1, \ldots, z_k$ independent variables. Then

$$P_k(\underline{z}) = P_k(z_1, \ldots, z_k) = \sum_{\substack{(\nu_1, \ldots, \nu_k) \in \mathbb{N}_0^k \\ \sum j\nu_j = k}} \frac{1}{\nu_1! \cdots \nu_k! \, 1^{\nu_1} \cdots k^{\nu_k}} z_1^{\nu_1} \cdots z_k^{\nu_k}.$$

Moreover, let $P_0(\underline{z}) = 1$.

Proposition 2.2. *Let k be a positive integer and $x_1, x_2, x_3, \ldots$ be a sequence of independent variables. Moreover, for $j = 1, \ldots, k$, let $s_j = \sum_{i=1}^{\infty} x_i^j$. Then*

$$\sum_{\substack{(n_1, \ldots, n_k) \in \mathbb{N}^k \\ n_1 \leq \cdots \leq n_k}} x_{n_1} \cdots x_{n_k} = P_k(s_1, \ldots, s_k).$$

Proof. First we introduce some notation. Let $\underline{x}_{\underline{n}} = x_{n_1} \cdots x_{n_k}$ for any $\underline{n} = (n_1, \ldots, n_k) \in \mathbb{N}^k$. Let $T = \{\underline{n} \in \mathbb{N}^k : n_1 \leq \cdots \leq n_k\}$. Also, let S_k be the symmetric group on $\{1, \ldots, k\}$; for $\sigma \in S_k$, let $\sigma\underline{n} = (n_{\sigma(n_1)}, \ldots, n_{\sigma(n_k)})$. Next, let $C = C(\sigma)$ be the conjugacy class of σ in S_k, that is, $C(\sigma) = \{\gamma\sigma\gamma^{-1} : \gamma \in S^k\}$. Let

$$\sigma = \prod_{j=1}^{k} \eta_{j1} \cdots \eta_{j\nu_j}$$

be a factorization of σ into disjoint cycles, where $\nu_j \in \mathbb{N}_0$ and for each j and $i = 1, \ldots, \nu_j$, the permutations η_{ji} are the distinct j-cycles, say $\eta_{ji} = (a_{ji1} \cdots a_{jij})$ with $a_{jil} \in \{1, \ldots, k\}$, and with the convention that 1-cycles are included so that $\bigcup_{j,i} \{a_{ji1}, \ldots, a_{jij}\} = \{1, \ldots, k\}$. Recall that $\tau \in C(\sigma)$ if and only if τ has the same type of cycle decomposition, that is, if

$$\tau = \prod_{j=1}^{k} \eta'_{j1} \cdots \eta'_{j\nu'_j}$$

into disjoint cycles with the same conventions as above, then $\nu'_j = \nu_j$ for $j = 1, \ldots, k$, (see, for example [2]). Notice then that a conjugacy class in S_k is determined uniquely by a k-tuple, $(\nu_1, \ldots, \nu_k) \in \mathbb{N}_0^k$ with $\sum_{j=1}^k j\nu_j = k$. Any permutation in the conjugacy class has a cycle decomposition determined by the ν_j's as above. Moreover, recall that

$$\#C(\sigma) = \frac{k!}{\nu_1! \cdots \nu_k! 1^{\nu_1} \cdots k^{\nu_k}},$$

again see [2]. Furthermore, recall that the cardinality of the orbit of $\underline{n}$ under S_k, $S_k\underline{n} = \{\eta\underline{n} : \eta \in S_k\}$, is equal to $|S_k|/|S_k(\underline{n})|$ where $S_k(\underline{n}) = \{\eta \in S_k : \eta\underline{n} = \underline{n}\}$, the stabilizer subgroup of $\underline{n}$. Moreover, if $\underline{m} \in S_k\underline{n}$, then the stabilizer subgroups, $S_k(\underline{m})$ and $S_k(\underline{n})$, are conjugate and thus have the same cardinality.

Now for the proof: Notice that

$$\frac{1}{k!} \sum_{\sigma \in S_k} \sum_{\substack{\underline{m} \in \mathbb{N}^k \\ \sigma\underline{m} = \underline{m}}} x_{\underline{m}} = \frac{1}{k!} \sum_{C} \sum_{\sigma \in C} \sum_{\substack{\underline{m} \in \mathbb{N}^k \\ \sigma\underline{m} = \underline{m}}} x_{\underline{m}},$$

where $\sum_C$ is the sum over the conjugacy classes of S_k. Now notice that if we write $\sigma = \prod_{j=1}^k \eta_{j1} \cdots \eta_{j\nu_j}$ as above, then $\sum_{\underline{m} \in \mathbb{N}^k, \sigma\underline{m} = \underline{m}} x_{\underline{m}} = s_1^{\nu_1} \cdots s_k^{\nu_k}$, which is independent of the choice of $\sigma \in C$. Hence

$$\frac{1}{k!} \sum_{C} \sum_{\sigma \in C} \sum_{\substack{\underline{m} \in \mathbb{N}^k \\ \sigma\underline{m} = \underline{m}}} x_{\underline{m}} = \frac{1}{k!} \sum_{C} |C| \sum_{\substack{\underline{m} \in \mathbb{N}^k \\ \sigma\underline{m} = \underline{m}}} x_{\underline{m}}$$
$$= \frac{1}{k!} \sum_{\substack{(\nu_1, \ldots, \nu_k) \in \mathbb{N}_0^k \\ \sum_j \nu_j = k}} \frac{k!}{\nu_1! \cdots \nu_k! 1^{\nu_1} \cdots k^{\nu_k}} s_1^{\nu_1} \cdots s_k^{\nu_k} = P_k(s_1, \cdot, s_k).$$

On the other hand,

$$\sum_{\underline{n} \in T} x_{\underline{n}} = \sum_{\underline{n} \in T} \frac{1}{|S_k\underline{n}|} \sum_{\underline{m} \in S_k\underline{n}} x_{\underline{m}},$$

since $x_{\underline{m}} = x_{\underline{n}}$ for any $\underline{m} \in S_k\underline{n}$. Hence

$$\sum_{\underline{n} \in T} x_{\underline{n}} = \sum_{\underline{m} \in \mathbb{N}^k} \sum_{\substack{\underline{n} \in T \\ \underline{m} \in S_k\underline{n}}} \frac{1}{|S_k\underline{n}|} x_{\underline{m}} = \frac{1}{k!} \sum_{\underline{m} \in \mathbb{N}^k} \sum_{\substack{\underline{n} \in T \\ \underline{m} \in S_k\underline{n}}} |S_k(\underline{n})| \, x_{\underline{m}}$$
$$= \frac{1}{k!} \sum_{\underline{m} \in \mathbb{N}^k} \sum_{\substack{\underline{n} \in T \\ \underline{m} \in S_k\underline{n}}} |S_k(\underline{m})| x_{\underline{m}} = \frac{1}{k!} \sum_{\underline{m} \in \mathbb{N}^k} \sum_{\substack{\underline{n} \in T \\ \underline{m} \in S_k\underline{n}}} \sum_{\sigma \in S_k(\underline{m})} x_{\underline{m}}$$
$$= \frac{1}{k!} \sum_{\underline{m} \in \mathbb{N}^k} \sum_{\sigma \in S_k(\underline{m})} x_{\underline{m}} \sum_{\substack{\underline{n} \in T \\ \underline{m} \in S_k\underline{n}}} 1.$$

But $\sum_{\underline{n}\in T,\ \underline{m}\in S_k\underline{n}} 1 = 1$, since only one permutation of $\underline{m}$ can belong to T. Therefore,

$$\sum_{\underline{n}\in T} x_{\underline{n}} = \frac{1}{k!}\sum_{\underline{m}\in\mathbb{N}^k}\sum_{\substack{\sigma\in S_k\\ \sigma\underline{m}=\underline{m}}} x_{\underline{m}} = P_k(s_1,\ldots,s_k),$$

from above, as desired. □

Proposition 2.3. *Let k be a nonnegative integer and $\mathfrak{c}$ any class in* Cl. *Then*

$$\sum_{\substack{\mathfrak{a}\\ \exists\,\mathfrak{p}_1,\ldots,\mathfrak{p}_k\in\mathscr{P}\cap\mathfrak{c}\\ \mathfrak{a}=\mathfrak{p}_1\cdots\mathfrak{p}_k}} N(\mathfrak{a})^{-s} = P_k(\underline{z}),$$

where $z_j = \sum_{\mathfrak{p}\in\mathscr{P}\cap\mathfrak{c}} N\mathfrak{p}^{-js}$, for all $\mathrm{Re}(s) = \sigma > 1$.

Proof. For $k = 0$, both sides are equal to 1, for the left-hand side consists of one term, $\mathfrak{a} = \mathscr{O}_K$ which has norm equal to 1.

Assume $k > 0$. Write $\mathscr{P}\cap\mathfrak{c} = \{\mathfrak{p}_n : n\in\mathbb{N}\}$. For any $n\in\mathbb{N}$, let $x_n = N\mathfrak{p}_n^{-s}$. Then the proposition follows directly from Proposition 2.2, once we observe that N is multiplicative and all series involved converge absolutely, since $\sigma > 1$. □

We now have the following useful corollary to Proposition 2.3.

Corollary 2.4.

$$\mu(s) = \sum_{(\alpha),\ \alpha\ \mathit{irred.}} |N(\alpha)|^{-s} = \sum_{m=1}^{D}\sum_{\underline{k}\in\mathscr{D}_m}\prod_{i=1}^{h} P_{k_i}(z_{i1},\ldots,z_{ik_i}),$$

where $z_{ij} = \sum_{\mathfrak{p}_i\in\mathscr{P}\cap\mathfrak{c}_i} N\mathfrak{p}_i^{-js}$.

For the next proposition, write $z_{i1} = \sum_{\mathfrak{p}_i\in\mathscr{P}\cap\mathfrak{c}_i} N\mathfrak{p}_i^{-s} = l + g_i$, where $l = (1/h)\log(1/(s-1))$, and $g_i = g_i(s)$. It is well known that $g_i(s)$ is regular at $s = 1$. We then have

Proposition 2.5. *$\mu(s) = \sum_{\mu=0}^{D} c_\mu l^\mu$, where $c_\mu = \sum_{m=\max(1,\mu)}^{D}\sum_{\underline{k}\in\mathscr{D}_m} a_{\underline{k},\mu}$, where if $\underline{k} = (k_1,\ldots,k_h)$, then*

$$a_{\underline{k},\mu} = \sum_{\substack{\mu_1=0\\ \mu_1+\cdots+\mu_h=\mu}}^{k_1}\cdots\sum_{\mu_h=0}^{k_h}\prod_{i=1}^{h} b_{k_i,\mu_i}, \quad \mathit{with} \quad b_{k_i,\mu_i} = \sum_{\nu_{i1}=\mu_i}^{k_i}\frac{g_i^{\nu_{i1}-\mu_i}}{\mu_i!\,(\nu_{i1}-\mu_i)!}\rho_{k_i,\nu_{i1}},$$

where

$$\rho_{k_i,\nu_{i1}} = \sum_{\substack{(\nu_{i2},\dots,\nu_{ik_i})\in\mathbb{N}_0^{k_i-1}\\ \sum j\nu_{ij}=k_i-\nu_{i1}}} \frac{1}{\nu_{i2}!\cdots\nu_{ik_i}!2^{\nu_{i2}}\cdots k_i^{\nu_{ik_i}}}\, z_{i2}^{\nu_{i2}}\cdots z_{ik_i}^{\nu_{ik_i}},$$

if $k_i > 1$, *and we define* $\rho_{0,0} = 1$, $\rho_{1,1} = 1$, *and* $\rho_{1,0} = 0$.

PROOF. First use the definition of the polynomials $P_k(\underline{z})$ to expand $\mu(s)$ in Proposition 2.3, where the indices of summation are ν_{ij} for $i = 1,\dots,h$ and $j = 1,\dots,k_i$. Hence

$$\mu(s) = \sum_{m=1}^{D} \sum_{(k_1,\dots,k_h)\in\mathscr{D}_m} \prod_{i=1}^{h} \sum_{\substack{(\nu_{i1},\dots,\nu_{ik_i})\\ \sum j\nu_{ij}=k_i}} \frac{1}{\nu_{i1}!\cdots\nu_{ik_i}!1^{\nu_{i1}}\cdots k!^{\nu_{ik_i}}}(l+g_i)^{\nu_{i1}} z_{2i}{}^{\nu_{i2}}\cdots z_{k_i i}{}^{\nu_{ik_i}},$$

where $\sum_{(\nu_{i1},\dots,\nu_{ik_i})}\cdots = 1$, if $k_i = 0$. Now in the right-hand most sum above, sum over the ν_{i1} first in which case we get

$$\sum_{\substack{(\nu_{i1},\dots,\nu_{ik_i})\\ \sum j\nu_{ij}=k_i}} \frac{1}{\nu_{i1}!\cdots\nu_{ik_i}!1^{\nu_{i1}}\cdots k!^{\nu_{ik_i}}}(l+g_i)^{\nu_{i1}} z_{2i}{}^{\nu_{i2}}\cdots z_{k_i i}{}^{\nu_{ik_i}} = \sum_{\nu_{i1}=0}^{k_i} \frac{(l+g_i)^{\nu_{i1}}}{\nu_{i1}!}\rho_{k_i,\nu_{i1}},$$

with ρ as defined in the statement of the proposition. Next, expand $z_{i1}^{\nu_{i1}} = (l+g_i)^{\nu_{i1}}$ as

$$\sum_{\mu_i=0}^{\nu_{i1}} \binom{\nu_{i1}}{\mu_i} l^{\mu_i} g_i^{\nu_{i1}-\mu_i}.$$

Then

$$\sum_{\nu_{i1}=0}^{k_i} \frac{(l+g_i)^{\nu_{i1}}}{\nu_{i1}!}\rho_{k_i,\nu_{i1}} = \sum_{\nu_{i1}=0}^{k_i} \frac{1}{\nu_{i1}!} \sum_{\mu_i=0}^{\nu_{i1}} \binom{\nu_{i1}}{\mu_i} g_i^{\nu_{i1}-\mu_i}\rho_{k_i,\nu_{i1}} l^{\mu_i} = \sum_{\mu_i=0}^{k_i} b_{k_i,\mu_i} l^{\mu_i},$$

where the b are defined as above. But then

$$\prod_{i=1}^{h}\sum_{\mu_i=0}^{k_i} b_{k_i,\mu_i} l^{\mu_i} = \sum_{\mu_1=0}^{k_1}\cdots\sum_{\mu_h=0}^{k_h}\prod_{i=1}^{h} b_{k_i,\mu_i} l^{\mu_1+\cdots+\mu_h} = \sum_{\mu=0}^{m} a_{\underline{k},\mu} l^{\mu},$$

with the a as defined above.

But now $\sum_{\underline{k}\in\mathscr{D}_m}\sum_{\mu=0}^{m} a_{\underline{k},\mu} l^{\mu} = \sum_{\mu=0}^{m}\sum_{\underline{k}\in\mathscr{D}_m} a_{\underline{k},\mu} l^{\mu}$. Hence

$$\mu(s) = \sum_{m=1}^{D}\sum_{\mu=0}^{m}\sum_{\underline{k}\in\mathscr{D}_m} a_{\underline{k},\mu} l^{\mu} = \sum_{\mu=0}^{D}\left(\sum_{m=\max(1,\mu)}^{D}\sum_{\underline{k}\in\mathscr{D}_m} a_{\underline{k},\mu}\right) l^{\mu},$$

as desired. □

Now we rewrite the $a_{\underline{k},\mu}$ in Proposition 2.5 in a form more convenient for winning an explicit formula for c_μ for 'large' μ.

COROLLARY 2.6. *$\mu(s) = \sum_{\mu=0}^{D} c_\mu\, l^\mu$, where $c_\mu = \sum_{\nu=\max(1,\mu)-\mu}^{D-\mu} \sum_{\underline{k}\in\mathscr{D}_{\mu+\nu}} a_{\underline{k},\mu}$, with*

$$a_{\underline{k},\mu} = \sum_{\substack{\nu_1=0\\ \nu_1+\cdots+\nu_h=\nu}}^{k_1} \cdots \sum_{\nu_h=0}^{k_h} \prod_{i=1}^{h} \frac{1}{k_i!} \sum_{\lambda_i=0}^{\nu_i} \frac{k_i!}{(\nu_i-\lambda_i)!(k_i-\nu_i)!} g_i^{\nu_i-\lambda_i} \rho_{k_i,k_i-\lambda_i},$$

where (as above)

$$\rho_{k_i,k_i-\lambda_i} = \sum_{\substack{(\nu_{i2},\ldots,\nu_{ik_i})\in\mathbb{N}_0^{k_i-1}\\ \sum j\nu_{ij}=\lambda_i}} \frac{1}{\nu_{i2}!\cdots\nu_{ik_i}!\,2^{\nu_{i2}}\cdots k_i^{\nu_{ik_i}}} z_{i2}^{\nu_{i2}}\cdots z_{ik_i}^{\nu_{ik_i}}.$$

PROOF. (Sketch) In Propostion 2.5 change variables as follows: let $\nu = m-\mu$, let $\nu_i = k_i - \mu_i$, and let $\lambda_i = k_i - \nu_{i1}$. □

From this corollary we extract the following result.

COROLLARY 2.7. *Let $\mu(s) = \sum_{\mu=0}^{D} c_\mu l^\mu$. Then*

(i) $c_D = \sum_{\underline{k}\in\mathscr{D}_D} \prod_{i=1}^{h}(1/k_i!)$.
(ii) $c_{D-1} = \sum_{\underline{k}\in\mathscr{D}_{D-1}} \prod_{i=1}^{h}(1/k_i!) + \sum_{\underline{k}\in\mathscr{D}_D} \prod_{i=1}^{h}(1/k_i!) \sum_{j=1}^{h} k_j g_j$.
(iii) *If $D \geq 2$, then*

$$c_{D-2} = \sum_{\underline{k}\in\mathscr{D}_{D-2}} \prod_{i=1}^{h} \frac{1}{k_i!} + \sum_{\underline{k}\in\mathscr{D}_{D-1}} \prod_{i=1}^{h} \frac{1}{k_i!} \sum_{j=1}^{h} k_j g_j$$
$$+ \sum_{\underline{k}\in\mathscr{D}_D} \prod_{i=1}^{h} \frac{1}{k_i!} \left(\sum_{1\le j_1<j_2\le h} k_{j_1}k_{j_2} g_{j_1} g_{j_2} + \sum_{j=1}^{h} k_j(k_j-1)\left(\frac{g_j^2}{2} + \frac{z_{j2}}{2}\right)\right).$$

The proof is a straightforward application of the previous corollary.

We further obtain the following expressions for $\mu(s)$ for some fields with small class number.

COROLLARY 2.8. (i) *Suppose $D = 1$ whence $h = 1$. Then $\mu(s) = l + g_1$.*
(ii) *If $D = 2$ so $h = 2$, say $\mathrm{Cl} = \{1 = \mathfrak{c}_1, \mathfrak{c}_2\}$, then*

$$\mu(s) = \frac{1}{2} l^2 + (1+g_2) l + \left(g_1 + \frac{1}{2} g_2^2 + \frac{1}{2} z_{22}\right).$$

PROOF. In light of the formulas for the c_μ above, it suffices to compute $\mathscr{D}_m$ for each of the groups listed.

Let $\mathrm{Cl} = \{1 = \mathfrak{c}_1\}$. Then we have only one minimal representation of 1, namely $1 \overset{\min}{=} 1$, implying that $\mathscr{D}_1 = \{1\}$. Using this with the previous corollary yields (i).

Now let $\mathrm{Cl} = \{1 = \mathfrak{c}_1, a = \mathfrak{c}_2\}$. Then we have two minimal representations of 1, namely, $1 \overset{\min}{=} 1$, and $aa \overset{\min}{=} 1$ implying that $\mathscr{D}_1 = \{(1, 0)\}$ and $\mathscr{D}_2 = \{(0, 2)\}$, respectively. This yields (ii). □

3. The summatory function $M(x)$

Having established formal properties of the Dirichlet series $\mu(s)$, we now use well-known results relating a Dirichlet series to its associated summatory function as in [6]. We present the following weaker form of Kaczorowski's 'Main Lemma' given in [6], which will be sufficiently strong for our purposes.

Let $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be a Dirichlet series where $s = \sigma + it$ with a_n, σ, t real numbers and $a_n \geq 0$.

As in [6] we have the following definition.

DEFINITION 6. We let $\mathscr{A}$ be the set of those Dirichlet series f as above satisfying the following three additional properties:

(i) For all $x, y \in \mathbb{R}$ such that $1 \leq x < y$,

$$\sum_{x \leq n \leq y} a_n \leq (y - x) \log^{c_1} y + O(y^{\theta}),$$

for some $c_1 > 0, \theta < 1$ where the constants depend on f only.

(ii) There exists a nonnegative integer k and functions $g_j(s)$ for $j = 0, \ldots, k$, such that

$$f(s) = \sum_{j=0}^{k} g_j(s) \log^j \left(\frac{1}{s - 1}\right),$$

for $\sigma > 1$ and such that $g_k(1) \neq 0$ and $g_j(s)$ is regular for $\sigma > 1$ and can be analytically continued to a regular function in the region $\mathscr{R}$ given by

$$\mathscr{R} = \left\{s = \sigma + it : \sigma > 1 - \frac{c_2}{\log(|t| + 2)}\right\}$$

for some $c_2 > 0$.

(iii) In the region $\mathscr{R}$, $|g_j(s)| \ll \log^{c_3}(|t| + 3)$, for some $c_3 > 0$.

PROPOSITION 3.1 (Corollary to Kaczorowski's Main Lemma). *Let*

$$f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$$

be a Dirichlet series in class $\mathscr{A}$ as defined above. Let $S(x) = \sum_{n\le x} a_n$ be the summatory function associated with $f(s)$. Then for all $\epsilon > 0$ and all $x \ge e^e$,

$$S(x) = \frac{x}{\log x}\left(\sum_{j=0}^{k-1} e_j(\log\log x)^j\right) + O\left(\frac{x}{\log^{2-\epsilon} x}\right),$$

as $x \to \infty$, where the e_j are complex numbers given by

$$e_j = \sum_{\nu=j}^{k} \frac{\nu!}{j!} g_\nu(1) I_{\nu-j}, \quad \textit{with} \quad I_m = \frac{(-1)^m}{m!}\frac{1}{2\pi i}\int_{\mathscr{C}} e^z(\log z)^m\, dz,$$

where $\mathscr{C}$ is the path of integration consisting of the segment $(-\infty, -1]$ on the lower side of the real axis (so that the argument of $\log z$ is $-\pi$), the circumference of the unit circle taken counter-clockwise, and the segment $[-1, -\infty)$ on the upper side of the real axis.

The proof may be found in [6] where we take Case I and $q = 0$ in the Main Lemma.

LEMMA 3.2. *Let t be any positive real number with $t < 1$. Then*

(a) $I_0 = 0$,
(b) $\sum_{m=1}^{\infty} t^{m-1} I_m = \exp\left(\gamma t + \sum_{n=2}^{\infty}(-1)^{n-1}\zeta(n)t^n/n\right)$, *where $\gamma = 0.577\ldots$ is Euler's constant,*
(c) $I_1 = 1$ *and* $I_2 = \gamma$.

PROOF. Part (a) follows since $I_0 = \int_{\mathscr{C}} e^z\, dz = 0$.

With respect to Part (b), consider the formal sum

$$\sum_{m=0}^{\infty} t^m I_m = \frac{1}{2\pi i}\int_{\mathscr{C}} e^z e^{-t\log z}\, dz = \frac{1}{2\pi i}\int_{\mathscr{C}} e^z z^{-t}\, dz = \frac{1}{\Gamma(t)}.$$

But then since $I_0 = 0$, we have

$$\sum_{m=1}^{\infty} t^{m-1} I_m = \frac{1}{t\Gamma(t)} = \exp\left(\gamma t + \sum_{n=2}^{\infty}(-1)^{n-1}\zeta(n)\frac{t^n}{n}\right),$$

by [13].

Part (c) follows immediately from (b). □

COROLLARY 3.3. *Let e_j be defined as in Proposition 3.1. Then*

(i) *if $k \ge 1$, $e_{k-1} = k\, g_k(1)$,*
(ii) *if $k \ge 2$, $e_{k-2} = (k-1)g_{k-1}(1) + k(k-1)g_k(1)\,\gamma$.*

The proof is immediate from the preceding lemma and proposition.

We now apply these results to $\mu(s)$ to obtain information about $M(x)$. By [6], using results in [7], $\mu(s)$ belongs to the class $\mathscr{A}$.

We shall state a well-known result about $\sum_{\mathfrak{p}\in\mathfrak{c}}(1/N\mathfrak{p}^s)$, for $\mathfrak{c} \in \mathrm{Cl}$, but first we recall some definitions.

Let K be an algebraic number field of degree n over $\mathbb{Q}$ with class group $\mathrm{Cl}(K) = \mathrm{Cl}$ of order h. Let $\widehat{\mathrm{Cl}}$ denote the character group of Cl, that is, the group of homomorphisms from Cl into the multiplicative group $\mathbb{C}^*$. As usual, we denote the principal character, that is, the constant character 1, by either χ_0 or simply by 1.

Let χ be an arbitrary character on Cl, then we define the L-series

$$L(s,\chi) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{N\mathfrak{a}^s} \quad (\sigma > 1),$$

where the sum is over all (nonzero) integral ideals of K.

If $\chi = 1$, the principal character, then $L(s,\chi_0) = \zeta_K(s)$, the Dedekind zeta function of K.

As is well known, $L(s,\chi)$ converges absolutely and uniformally on compact subsets in the half plane $\sigma > 1$. Moreover, since the norm map N is completely multiplicative on the set of ideals of K, we have

$$L(s,\chi) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{N\mathfrak{p}^s}\right)^{-1},$$

for all $\sigma > 1$ and where the product is taken over all (nonzero) prime ideals of K. It is also well known that in the half plane $\sigma > 1 - 1/n$, the series for $L(s,\chi)$ converges, if $\chi \neq 1$, and $L(s,\chi)$ is regular there. On the other hand, $\zeta_K(s)$ has a continuation into the same half plane but with a simple pole at $s = 1$ with (nonzero) residue a_K.

Furthermore, in the region $\mathscr{R}_K$ given by

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

$L(s,\chi)$ does not vanish, where c_K depends on K but not on χ.

Now, since $L(s,\chi)$ is nonzero in the region above, we see that $\log L(s,\chi)$ is defined and regular in this region.

PROPOSITION 3.4. *Let* $\mathfrak{c}$ *be an ideal class of* Cl. *Then*

$$\sum_{\mathfrak{p}\in\mathfrak{c}} \frac{1}{N\mathfrak{p}^s} = \frac{1}{h}\log\zeta_K(s) + \frac{1}{h}\sum_{\substack{\chi \\ \chi\neq 1}} \overline{\chi}(\mathfrak{c})\log L(s,\chi) - \sum_{m=2}^{\infty}\sum_{\substack{\mathfrak{p} \\ \mathfrak{p}^m\in\mathfrak{c}}} \frac{1}{mN\mathfrak{p}^{ms}},$$

for $\sigma > 1$.

For a proof see, for example [8], (or just about any text on algebraic number theory).

Notice that this proposition allows us to analytically continue $\sum_{\mathfrak{p}\in\mathfrak{c}} N\mathfrak{p}^{-s}$ onto the region $\mathscr{R}_K$.

Corollary 3.5. *Let* $g_{\mathfrak{c}}(s) = \sum_{\mathfrak{p}\in\mathfrak{c}}(1/N\mathfrak{p}^s) - (1/h)\log(1/(s-1))$. *Then*

$$g_{\mathfrak{c}}(s) = \frac{1}{h}\log((s-1)\zeta_K(s)) + \frac{1}{h}\sum_{\substack{\chi\\ \chi\neq 1}} \overline{\chi}(\mathfrak{c})\log L(s,\chi) - \sum_{m=2}^{\infty}\sum_{\substack{\mathfrak{p}\\ \mathfrak{p}^m\in\mathfrak{c}}} \frac{1}{mN\mathfrak{p}^{ms}},$$

hence regular in $\mathscr{R}_K$. *In particular,*

$$g_{\mathfrak{c}}(1) = \frac{1}{h}\log a_K + \frac{1}{h}\sum_{\substack{\chi\\ \chi\neq 1}} \overline{\chi}(\mathfrak{c})\log L(1,\chi) - \sum_{m=2}^{\infty}\sum_{\substack{\mathfrak{p}\\ \mathfrak{p}^m\in\mathfrak{c}}} \frac{1}{mN\mathfrak{p}^{m}},$$

where a_K *is the residue of* $\zeta_K(s)$ *at* $s=1$.

Proof. Write $\zeta_K(s)$ as $(1/(s-1))(s-1)\zeta_K(s)$ and then apply log. □

We now apply this result to $M(x)$.

Proposition 3.6. *Let* K *be an algebraic number field with class number* h *and associated Davenport number* D. *Then*

$$M(x) = Dc_D h^{-D}\frac{x}{\log x}(\log\log x)^{D-1} + \frac{x}{\log x}\sum_{j=0}^{D-2} e_j(\log\log x)^j + O\left(\frac{x}{(\log x)^{3/2}}\right),$$

where the e_j *are given in Proposition* 3.1 *with* $g_j(s) = h^{-j}c_j(s)$.

Proof. The proof is immediate since $\mu(s) = \sum_{\mu=0}^{D} c_\mu(s)h^{-\mu}\big(\log(1/(s-1))\big)^{\mu}$. □

As an immediate corollary we have

Corollary 3.7. $M(x) \sim Dc_D h^{-D}(x/\log x)(\log\log x)^{D-1}$.

Compare this with [5, Theorem 1]. But we also get the following result.

Theorem 3.8. *For* $D \geq 2$,

$$M(x) = \frac{x}{\log x}\left(C(\log\log x)^{D-1} + B(\log\log x)^{D-2}\right) + O\left(E(x)\right),$$

where $C = Dc_D h^{-D}$ *and* $B = (D-1)c_{D-1}(1)h^{1-D} + D(D-1)c_D h^{-D}\gamma$, *with* γ, *Euler's constant, and where*

$$E(x) = \begin{cases} \dfrac{x}{\log x}(\log\log x)^{D-3} & \text{if } D \geq 3; \\ \dfrac{x}{(\log x)^{3/2}} & \text{otherwise}. \end{cases}$$

4. The special case of number fields with cyclic class group

We now investigate the asymptotic behavior of $M(x)$ when the number field K has cyclic class group Cl of order $h > 1$. Then we see, by Theorem 3.8, that in order to compute the coefficients C and B, we need to determine c_D and $c_{D-1}(s)$. First of all, notice that $D = h$, for we have already observed that $D \leq h$ for any Cl. But now since Cl is cyclic generated by $\mathfrak{c}$, say, then $\mathfrak{c}^h \overset{\min}{=} 1$, whence $h \leq D$ in this case.

Now by Corollary 2.7, we need to determine $\mathscr{D}_m$ for $m = D = h$ and $m = D-1 = h-1$.

To this end, we cite the following main result of [3].

PROPOSITION 4.1. *Let* $S = (a_1, \ldots, a_{n-k})$ *be a sequence of* $n-k$ *(not necessarily distinct) elements in* $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. *Suppose* $1 \leq k \leq n/6 + 1$ *and that* 0 *cannot be expressed as a sum over a nonempty subsequence of* S; *then there exist an integer* c *coprime to* n *and a permutation* σ *of the set* $\{1, 2, \ldots, n-k\}$ *such that* $ca_{\sigma(i)} = 1$ *for* $i = 1, \ldots, n-2k+1$, *and* $\sum_{i=n-2k+2}^{n-k} |a_{\sigma(i)}|_n \leq 2k-2$, *where* $|x|_n$ *denotes the least positive inverse image of* x *under the natural homomorphism from the additive group of integers onto* $\mathbb{Z}_n$.

In particular, there are at least $n-2k+1$ *terms in* S *which are relatively prime to* n *and all congruent to one another modulo* n.

We use this result to prove the following lemma.

LEMMA 4.2. *Suppose* $\mathrm{Cl} = \langle \mathfrak{c} \rangle$. *Then*

$$\mathscr{D}_D = \{\kappa_k : 1 \leq k \leq h, (k, h) = 1\},$$

where $\kappa_k : \mathrm{Cl} \to \mathbb{N}_0$ *with* $\kappa_k(\mathfrak{c}^k) = h$ *and* $\kappa_k(\mathfrak{c}^l) = 0$ *otherwise*;

$$\mathscr{D}_{D-1} = \{\lambda_k : 1 \leq k \leq h, (k, h) = 1\},$$

where $\lambda_k : \mathrm{Cl} \to \mathbb{N}_0$ *with* $\lambda_k(\mathfrak{c}^k) = h-2$, $\lambda_k(\mathfrak{c}^{2k}) = 1$, *and* $\lambda_k(\mathfrak{c}^l) = 0$ *otherwise.*

PROOF. We start by determining the elements of $\mathscr{D}_D$. Suppose $\mathfrak{c}_1, \ldots, \mathfrak{c}_h \in \mathrm{Cl}$ and $\prod_{i=1}^h \mathfrak{c}_i \overset{\min}{=} 1$. Then the h sequences $S_j = (\mathfrak{c}_1, \ldots, \hat{\mathfrak{c}_j}, \ldots, \mathfrak{c}_h)$ (where $\mathfrak{c}_j$ is omitted) satisfy the hypotheses of Proposition 4.1 with $k = 1$. Hence in each S_j there are at least $h-1$ terms which are equal and generating Cl. Hence, we must have $\mathfrak{c}_1 = \cdots = \mathfrak{c}_h = \mathfrak{c}$ and $\langle \mathfrak{c} \rangle = \mathrm{Cl}$. Thus $\mathscr{D}_D$ is as stated above.

Now consider $\mathscr{D}_{D-1}$. Suppose $\mathfrak{c}_1, \dots, \mathfrak{c}_{h-1} \in \mathrm{Cl}$ and $\prod_{i=1}^{h-1} \mathfrak{c}_i \overset{\min}{=} 1$. Then the $h-1$ sequences $S_j = (\mathfrak{c}_1, \dots, \hat{\mathfrak{c}}_j, \dots, \mathfrak{c}_{h-1})$ satisfy the hypotheses above with $k = 2$ provided $h \geq 6$. (For $h < 6$ the lemma follows by a straightforward calculation.) Hence, assume $h \geq 6$ in which case in each S_j there are at least $h-3$ terms which are equal and generate Cl. But then, without loss of generality, $\mathfrak{c}_1 = \cdots = \mathfrak{c}_{h-2} = \mathfrak{c}$ where $\langle \mathfrak{c} \rangle = \mathrm{Cl}$. Thus $\mathfrak{c}^{h-2}\mathfrak{d} = 1$ for some $\mathfrak{d} \in \mathrm{Cl}$; whence $\mathfrak{d} = \mathfrak{c}^2$, as desired. □

This lemma along with Corollary 2.7 and Theorem 3.8 yields the following proposition.

PROPOSITION 4.3. *Let K be an algebraic number field with cyclic class group* $\mathrm{Cl} = \langle \mathfrak{c} \rangle$ *of order $h > 1$. Then*

$$M(x) = \frac{x}{\log x}\left(C(\log\log x)^{h-1} + B(\log\log x)^{h-2}\right) + O\left(E(x)\right),$$

where $C = \varphi(h)/((h-1)!h^h)$, and

$$B = \frac{\varphi(h)}{(h-2)!h^h}\gamma + \frac{h-1}{h^{h-1}}\left(\frac{\varphi(h)}{(h-2)!}a(h) + \frac{1}{(h-1)!}\sum_{\substack{k=1\\(k,h)=1}}^{h} g_{\mathfrak{c}^k}(1)\right),$$

where $a(h) = 1/2$, if $h = 3$, and $a(h) = 1$, otherwise; and where $g_{\mathfrak{c}}$ is as appears in Corollary 3.5.

The proof follows immediately from Corollary 2.7 and Theorem 3.8. (Notice that when $h = 3$, $|\mathscr{D}_2| = 1$, not $\varphi(h)$.)

We now give an (partially) arithmetic interpretation of $\sum_{\substack{k=1\\(k,h)=1}}^{h} g_{\mathfrak{c}^k}(1)$. First, we introduce some notation.

Once again assume K has cyclic class group $\mathrm{Cl} = \langle \mathfrak{c} \rangle$ and let L be the Hilbert class field of K. For each divisor d of h let L_d denote the intermediate field in the extension L/K of degree d over K. (Since by class field theory $\mathrm{Gal}(L/K) \simeq \mathrm{Cl}$ and Cl is cyclic, L_d is uniquely determined.) Notice in particular that $L_1 = K$ and $L_h = L$. Finally, let a_{L_d} be the residue of the Dedekind zeta function $\zeta_{L_d}(s)$ at $s = 1$.

THEOREM 4.4. *Given the assumptions of the previous paragraph,*

$$\sum_{\substack{k=1\\(k,h)=1}}^{h} g_{\mathfrak{c}^k}(1) = \sum_{d|h} \frac{\mu(d)}{d} \log a_{L_d} - \sum_{\substack{m\geq 2\\ \langle[\mathfrak{p}^m]\rangle=\mathrm{Cl}}} \sum_{\mathfrak{p}} \frac{1}{mN\mathfrak{p}^m}.$$

PROOF. By Corollary 3.5 we have

$$\sum_{\substack{k=1\\(k,h)=1}}^{h} g_{\mathfrak{c}^k}(s) = \frac{\varphi(h)}{h}\log\big((s-1)\zeta_K(s)\big) + \frac{1}{h}\beta(s) - \sum_{m=2}^{\infty}\sum_{\substack{k=1\\(k,h)=1}}^{h}\sum_{\substack{\mathfrak{p}\\ \mathfrak{p}^m\in\mathfrak{c}^k}} \frac{1}{mN\mathfrak{p}^{ms}},$$

where

$$\beta(s) = \sum_{\substack{\chi\\ \chi\neq 1}}\sum_{\substack{k=1\\(k,h)=1}}^{h} \overline{\chi}(\mathfrak{c}^k)\log L(s,\chi).$$

For $j = 0, \ldots, h-1$, let χ_j be the character on Cl determined by $\chi_j(\mathfrak{c}) = \zeta_h^j$ for ζ_h a primitive hth root of unity. More generally, let $\chi_{d,j}$ be the character on Cl determined by $\chi_{d,j}(\mathfrak{c}) = \zeta_d^j$, for any positive integer d dividing h. Also let

$$c_n(j) = \sum_{\substack{k=1\\(k,h)=1}}^{h} \zeta_h^{jk},$$

the usual Ramanujan sum. Then

$$\beta(s) = \sum_{j=1}^{h-1} c_h(-j)\log L(s,\chi_j).$$

But the Ramanujan sum has the explicit representation (see, for example, [4, page 238])

$$c_n(j) = \varphi(h)\frac{\mu(h/(h,j))}{\varphi(h/(h,j))},$$

and thus

$$\begin{aligned}\beta(s) &= \varphi(h)\sum_{\nu\mid h}\frac{\mu(\nu)}{\varphi(\nu)}\sum_{\substack{j=1\\(h,j)=h/\nu}}^{h-1}\log L(s,\chi_j)\\ &= \varphi(h)\sum_{\nu\mid h}\frac{\mu(\nu)}{\varphi(\nu)}\sum_{\substack{j=1\\p(h,j)=h/\nu}}^{h}\log L(s,\chi_j) - \varphi(h)\log\zeta_K(s).\end{aligned}$$

Now, by [8, page 230], we have

$$\log\zeta_{L_d}(s) = \sum_{\nu\mid d}\sum_{\substack{j \bmod \nu\\(j,\nu)=1}}\log L(s,\chi_{\nu,j}).$$

But then by Möbius inversion,

$$\sum_{\substack{j \bmod h\\(h,j)=h/\nu}}\log L(s,\chi_j) = \sum_{\substack{j \bmod \nu\\(j,\nu)=1}}\log L(s,\chi_{\nu,j}) = \sum_{d\mid\nu}\mu(\nu/d)\log\zeta_{L_d}(s).$$

Thus

$$\begin{aligned}
&\varphi(h)\sum_{\nu\mid h}\frac{\mu(\nu)}{\varphi(\nu)}\sum_{\substack{j=1\\(h,j)=h/\nu}}^{h}\log L(s,\chi_j)\\
&\quad=\varphi(h)\sum_{\nu\mid h}\sum_{d\mid\nu}\frac{\mu(\nu)}{\varphi(\nu)}\mu\left(\frac{\nu}{d}\right)\log\zeta_{L_d}(s)=\varphi(h)\sum_{d\mid h}\log\zeta_{L_d}(s)\sum_{\substack{\nu\mid h\\d\mid\nu}}\frac{\mu(\nu)\mu(\nu/d)}{\varphi(\nu)}\\
&\quad=\varphi(h)\sum_{d\mid h}\log\zeta_{L_d}(s)\mu(d)\sum_{\substack{\nu\mid h\\d\mid\nu}}\frac{\mu^2(\nu)}{\varphi(\nu)}=\varphi(h)\sum_{d\mid h}\log\zeta_{L_d}(s)\frac{h}{\varphi(h)}\frac{\mu(d)}{d}\\
&\quad=h\sum_{d\mid h}\frac{\mu(d)}{d}\log\zeta_{L_d}(s),
\end{aligned}$$

since

$$\sum_{\substack{\nu\mid h\\d\mid\nu}}\frac{\mu^2(\nu)}{\varphi(\nu)}=\frac{h}{\varphi(\nu)}\frac{\mu^2(d)}{d},$$

see, for example, [1, Lemma 3]. Hence

$$\beta(s)=h\sum_{d\mid h}\frac{\mu(d)}{d}\log\zeta_{L_d}(s)-\varphi(h)\log\zeta_K(s).$$

Now notice that

$$\begin{aligned}
\lim_{\sigma\to1^+}\beta(s)&=h\sum_{d\mid h}\frac{\mu(d)}{d}\log(s-1)\zeta_{L_d}(s)-\varphi(h)\log(s-1)\zeta_K(s)\\
&\qquad-\left(h\sum_{d\mid h}\frac{\mu(d)}{d}-\varphi(h)\right)\log(s-1)\\
&=h\sum_{d\mid h}\frac{\mu(d)}{d}\log a_{L_d}-\varphi(h)\log a_K,
\end{aligned}$$

since $\varphi(h)=h\sum_{d\mid h}\mu(d)/d$. This gives us the result. □

5. Examples

The coefficient C of $M(x)$ depends on the class group of K, more precisely, on the Davenport constant and the order of the class group. On the other hand, the coefficient B seems to depend more intrinsically on the arithmetic for the field K. In this section we consider approximating B for two imaginary quadratic number fields of class number 2, namely, $K_1 = \mathbb{Q}(\sqrt{-5})$ and $K_2 = \mathbb{Q}(\sqrt{-15})$ to see if the B are unequal. But before we carry out the calculations in these special cases, we consider Proposition 4.3 for the case where $h = 2$.

COROLLARY 5.1. *Let K be a number field with class number* 2. *Denote by $\mathfrak{c}$ the nonprincipal ideal class of* Cl. *Finally, let L be the Hilbert class field of K. Then*

$$M(x) = \frac{1}{4}\frac{x}{\log x}\log\log x + \frac{1}{4}(2(1+g_{\mathfrak{c}}(1))+\gamma)\frac{x}{\log x} + O\left(\frac{x}{(\log x)^{3/2}}\right),$$

where γ is Euler's constant and

$$g_{\mathfrak{c}}(1) = \log a_K - \frac{1}{2}\log a_L - \sum_{\substack{m\geq 3\\ m\equiv 1(2)}}\sum_{\mathfrak{p}\in\mathfrak{c}}\frac{1}{mN\mathfrak{p}^m}.$$

We need to compute a_K, a_L, and $S = \sum_{\substack{m\geq 3\\ m\equiv 1(2)}}\sum_{\mathfrak{p}\in\mathfrak{c}} 1/(mN\mathfrak{p}^m)$.

To this end, let F be any algebraic number field. Then the residue of $\zeta_F(s)$ at $s = 1$ is

$$a_F = \frac{2^{r_1}(2\pi)^{r_2}R_F h_F}{w_F\sqrt{|d_F|}},$$

where r_1 and r_2 are the number of inequivalent real and complex embeddings of F into $\mathbb{C}$, respectively; R_F is the regulator of F; h_F its class number; w_F the number of roots of unity in $\mathscr{O}_F$; and d_F is the discriminant of F.

For $K_1 = \mathbb{Q}(\sqrt{-5})$, $r_1 = 0$, $r_2 = 1$, $R_{K_1} = 1$, $w_{K_1} = 2$, and $d_{K_1} = -20$, and hence $a_{K_1} = \pi/\sqrt{5}$.

For $K_2 = \mathbb{Q}(\sqrt{-15})$, $r_1 = 0$, $r_2 = 1$, $R_{K_2} = 1$, $w_{K_2} = 2$, and $d_{K_2} = -15$, and hence $a_{K_2} = 2\pi/\sqrt{15}$.

The Hilbert class fields of $\mathbb{Q}(\sqrt{-5})$ and $\mathbb{Q}(\sqrt{-15})$ are $L_1 = \mathbb{Q}(\sqrt{-5}, \sqrt{5})$ and $L_2 = \mathbb{Q}(\sqrt{-15}, \sqrt{5})$, respectively. To compute a_{L_i} in these two cases, we first notice that $r_1 = 0$ and $r_2 = 2$. To compute the other invariants, we shall use the fact that L_i are CM-fields, which will allow us to compute the regulators R_L, and the fact that $\mathrm{Gal}(L_i/\mathbb{Q}) \simeq C(2)\times C(2)$, the Klein four group, which will give us a way to compute the class numbers.

To this end, let $L^+ = L\cap\mathbb{R} = \mathbb{Q}(\sqrt{5})$ in both cases $L = L_i$. Now $R_{L^+} = \log((1+\sqrt{5})/2)$ and by [12, Proposition 4.16] (for example) $R_L = (1/Q)2\log((1+\sqrt{5})/2)$, where $Q = (E_L : W_L E_{L^+}) \in \{1, 2\}$ with E_F and W_F the group of units, respectively, roots of unity in $\mathscr{O}_F$ for any number field F. But in our two cases, $Q = 1$; see [10, Theorem 1]. Thus in both cases

$$R_L = 2\log\frac{1+\sqrt{5}}{2}.$$

By [8, Proposition 17, page 68] (for example) we see that $d_{L_1} = 20^2$ and $d_{L_2} = 15^2$.

Finally, to compute the class numbers, we use Kuroda's class number formula:

$$h_L = \frac{1}{2} q(L) h_1 h_2 h_3,$$

where the h_i are the class numbers of the three quadratic subfields of L, and $q(L) = (E_L : E_1 E_2 E_3)$ with E_i the group of units in the quadratic subfields, see, for example, [9]. In our cases, $h_1 h_2 h_3 = 2$ and since L/K is unramified $q(L) = 1$, [10, Theorem 1]. Hence in both cases $h_L = 1$.

Therefore,

$$a_{L_1} = \frac{\pi^2}{10} \log\left(\frac{1+\sqrt{5}}{2}\right) \quad \text{and} \quad a_{L_2} = \frac{4\pi^2}{15} \log\left(\frac{1+\sqrt{5}}{2}\right).$$

Next, we need to approximate the two series

$$S_i := \sum_{\substack{m \geq 3 \\ m \equiv 1(2)}} \sum_{\mathfrak{p} \in \mathfrak{c}_i} \frac{1}{m N\mathfrak{p}^m}$$

for the fields K_i, $i = 1, 2$ and where $\mathrm{Cl}(K_i) = \langle \mathfrak{c}_i \rangle$. Now, since

$$\sum_{\substack{m \geq 3 \\ m \equiv 1(2)}} \frac{1}{m z^m} = \frac{1}{2}\left(\frac{\log(z+1)}{\log(z-1)} - \frac{2}{z}\right),$$

we see that

$$S = \sum_{\mathfrak{p} \in \mathfrak{c}} \sum_{\substack{m \geq 3 \\ m \equiv 1(2)}} \frac{1}{m N\mathfrak{p}^m} = \sum_{\mathfrak{p} \in \mathfrak{c}} \frac{1}{2}\left[\log\left(\frac{N\mathfrak{p}+1}{N\mathfrak{p}-1}\right) - \frac{2}{N\mathfrak{p}}\right].$$

We now truncate the series S at $N\mathfrak{p} < x$ for $x > 3$ and estimate the truncation error by a little elementary calculus. To this end, we write $S = S(x) + E(x)$, where

$$S(x) := \sum_{\substack{\mathfrak{p} \in \mathfrak{c} \\ N\mathfrak{p} < x}} \frac{1}{2}\left[\log\left(\frac{N\mathfrak{p}+1}{N\mathfrak{p}-1}\right) - \frac{2}{N\mathfrak{p}}\right]$$

and

$$E(x) = \sum_{\substack{\mathfrak{p} \in \mathfrak{c} \\ N\mathfrak{p} \geq x}} \sum_{\substack{m \geq 3 \\ m \equiv 1(2)}} \frac{1}{m N\mathfrak{p}^m}.$$

Now, notice that

$$\sum_{\substack{\mathfrak{p} \in \mathfrak{c} \\ N\mathfrak{p} \geq x}} \frac{1}{m N\mathfrak{p}^m} < \sum_{k \geq x} \frac{2}{m k^m} < \int_{x-1}^{\infty} \frac{2}{m t^m}\, dt = \frac{2}{m(m-1)(x-1)^{m-1}},$$

since $N\mathfrak{p} = k$ can occur at most twice (when $p\mathscr{O}_K$ splits where $\mathfrak{p}|p$). Hence

$$\begin{aligned}|E(x)| &\leq \sum_{m=3}^{\infty} \frac{2}{m(m-1)(x-1)^{m-1}} \\ &< \frac{1}{3}\sum_{m=3}^{\infty} \frac{1}{(x-1)^{m-1}} = \frac{1}{3(x-1)(x-2)} < \frac{1}{3(x-2)^2}.\end{aligned}$$

Next, to approximate $S(x)$, we need to find out which prime ideals are not principal in $\mathscr{O}_{K_i}$. But since the L are abelian over $\mathbb{Q}$, the prime ideals that are nonprincipal are determined by congruences on the rational primes contained in these ideals. We now review this procedure. We consider the case $K = K_1$. Let $(d_K/\ )$ denote the Kronecker symbol and suppose $\mathfrak{p}|p$, p a positive rational prime; then $(d_K/p) = -1$ if and only if $\mathfrak{p} = p\mathscr{O}_K$, that is, p is inert in K. By reciprocity, this occurs when $p \equiv 11, 13, 17, 19 \bmod 20$. Hence in this case, $\mathfrak{p}$ is a principal ideal. Therefore, if $\mathfrak{p}$ is nonprincipal, then $(d_K/p) = 1$ or 0, that is, p splits or is ramified, respectively, in K. Suppose first that $p\mathscr{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$, for distinct prime ideals $\mathfrak{p}$ and $\overline{\mathfrak{p}}$. Then by properties of the Hilbert class field of K, $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are nonprincipal if and only if $\mathfrak{p}\mathscr{O}_L$ is a prime ideal. For K_1, this happens if and only if $(-20/p) = 1$ and $(-1/p) = -1$, that is, if and only if $p \equiv 3, 7 \bmod 20$. (Notice then that $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are principal when $p \equiv 1, 9 \bmod 20$.) On the other hand, the ramified primes in K_1 are the (unique) prime ideals dividing 2 and 5. But if $\mathfrak{p}|5$ then $\mathfrak{p} = \sqrt{-5}\mathscr{O}_{K_1}$, which is principal; whereas if $\mathfrak{p}|2$, then $\mathfrak{p}$ is nonprincipal, since otherwise $\mathfrak{p} = (a + b\sqrt{-5})\mathscr{O}_{K_1}$ for some $a, b \in \mathbb{Z}$, in which case $2 = N\mathfrak{p} = a^2 + 5b^2$, which is absurd. Similarly, for K_2, $\mathfrak{p}$ is nonprincipal when $(-15/p) = 1$ and $(-3/p) = -1$, that is, when $\mathfrak{p}|p$ where $p \equiv 2, 8 \bmod 15$, and for $p = 3, 5$ (ramified case). (On the other hand, $\mathfrak{p}$ is principal whenever $p \equiv 1, 4, 7, 11, 13, 14 \bmod 15$.)

Thus,

$$S_1(x) = \frac{1}{2}\left[\log 3 - 1\right] + \sum_{\substack{p<x \\ p\equiv 3,7(20)}} \left[\log\left(\frac{p+1}{p-1}\right) - \frac{2}{p}\right]$$

and

$$S_2(x) = \frac{1}{2}\log 3 - \frac{1}{3} - \frac{1}{5} + \sum_{\substack{p<x \\ p\equiv 2,8(15)}} \left[\log\left(\frac{p+1}{p-1}\right) - \frac{2}{p}\right].$$

To approximate S to four decimal places, say, we use

$$|E(x)| < \frac{1}{3(x-2)^2} < 0.5 \times 10^{-4},$$

in which case we may take $x = 84$. Then notice that $p \equiv 3, 7 \bmod 20$ with $p < 84$ if and only if $p = 3, 7, 23, 43, 47, 67, 83$. Also $p \equiv 2, 8 \bmod 15$ with $p < 84$ if and only if $p = 2, 17, 23, 47, 53, 83$. Hence $S_1 \approx S_1(84) \approx 0.077827$ and $S_2 \approx S_2(84) \approx 0.232435$ good to four decimal places.

On the other hand,

$$\log a_{K_i} - \frac{1}{2}\log a_{L_i} \approx \begin{cases} 0.71229745 & \text{for } i = 1; \\ 0.36572386 & \text{for } i = 2. \end{cases}$$

Therefore, $g_{\mathfrak{c}_1}(1) \approx 0.6343$ and $g_{\mathfrak{c}_2}(1) \approx 0.1333$.

This shows that the coefficient B differs for these two quadratic number fields.

Finally, as promised in the introduction, we characterize the primes and irreducibles in $\mathbb{Z}[\sqrt{-5}\,]$ and $\mathbb{Z}[\sqrt{-15}\,]$ in terms of rational primes.

PROPOSITION 5.2. (a) *An element π is prime in $\mathbb{Z}[\sqrt{-5}\,]$ if and only if $\pi \mid p$ a positive rational prime such that $p = 5$ or $p \equiv 1, 9, 11, 13, 17, 19 \bmod 20$.*
(b) *π is prime in $\mathbb{Z}[\sqrt{-15}\,]$ if and only if $p \equiv 1, 4, 7, 11, 13, 14 \bmod 15$.*
(c) *α is irreducible but not prime in $\mathbb{Z}[\sqrt{-5}\,]$ if and only if $|N(\alpha)| = p_1 p_2$ where p_1, p_2 are positive rational primes such that $p_i = 2$ or $p_i \equiv 3, 7 \bmod 20$.*
(d) *α is irreducible but not prime in $\mathbb{Z}[\sqrt{-15}\,]$ if and only if $|N(\alpha)| = p_1 p_2$ where $p_i = 3, 5$ or $p_i \equiv 2, 8 \bmod 15$.*

References

[1] D. M. Bradley, A. E. Özlük and C. Snyder, 'On a class number formula for real quadratic number fields', *Bull. Austral. Math. Soc.* **65** (2002), 259–270.
[2] D. S. Dummit and R. M. Foote, *Abstract algebra*, 2nd edition (Prentice Hall, Upper Saddle River, NJ, 1999).
[3] W. D. Gao, 'The structure of two classes of sequences in $\mathbb{Z}_n$', *Adv. in Math. (China)* **22** (1993), 348–353.
[4] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 5th edition (Academic Press, Boston, 1994).
[5] F. Halter-Kocha and W. Müller, 'Quantitative aspects of non-unique factoriztion; A general theory with applications to algebraic function fields', *J. Reine Angew. Math.* **421** (1991), 159–188.
[6] J. Kaczorowski, 'Some remarks on factorization in algebraic number fields', *Acta Arith.* **43** (1983), 53–68.
[7] E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale* (Chelsea Pub. Co., New York, 1949).
[8] S. Lang, *Algebraic number theory* (Addison-Wesley, London, 1970).
[9] F. Lemmermeyer, 'Kuroda's class number formula', *Acta Arith.* **66** (1994), 245–260.
[10] ———, 'Ideal class groups of cyclotomic number fields I', *Acta Arith.* **72** (1995), 347–359.
[11] J. P. Rémond, 'Étude asymptotique de certaines partitions dans certaines semi-groups', *Ann. Sci. École Norm. Sup.* **83** (1966), 343–410.
[12] L. Washington, *Introduction to cyclotomic fields* (Springer, New York, 1982).

[13] J. W. Wrench, Jr., ‘Concerning two series for the gamma function’, *Math. Comp.* **22** (1968), 617–626.

Department of Mathematics and Statistics
University of Maine
Orono, Maine 04469
USA
e-mail: bradley@math.umaine.edu
ozluk@math.umaine.edu
snyder@math.umaine.edu

19 Balsam Drive
Bangor
Maine 04401
USA
e-mail: rebecca.rozario@umit.edu