Submitted to the Bulletin of the Australian Mathematical Society
doi:10.1017/S …

TWO PROBLEMS CONCERNING IRREDUCIBLE ELEMENTS IN RINGS OF INTEGERS OF NUMBER FIELDS

PAUL POLLACK and LEE TROUPE

Abstract

Let K be a number field with ring of integers $\mathbb{Z}_K$. We prove two asymptotic formulas connected with the distribution of irreducible elements in $\mathbb{Z}_K$. First, we estimate the maximum number of nonassociated irreducibles dividing a nonzero element of $\mathbb{Z}_K$ of norm not exceeding x (in absolute value), as $x \to \infty$. Second, we count the number of irreducible elements of $\mathbb{Z}_K$ of norm not exceeding x lying in a given arithmetic progression (again, as $x \to \infty$). When $K = \mathbb{Q}$, both results are classical; a new feature in the general case is the influence of combinatorial properties of the class group of K.

2010 *Mathematics subject classification:* primary 11R27; secondary 11N37, 11N45.

Keywords and phrases: irreducible, number field, factorization, ray class, Davenport constant.

1. Introduction

Let K be an algebraic number field with corresponding ring of integers $\mathbb{Z}_K$. In this paper, we take two well-known analytic results about rational prime numbers and prove generalizations for the irreducible elements of $\mathbb{Z}_K$. Our results can be seen as contributing to the program of understanding how combinatorial attributes of the class group of K influence factorization properties of the domain $\mathbb{Z}_K$, complementing prior work in this direction by A. Geroldinger, F. Halter-Koch, J. Kaczorowski, K. Martin, W. Narkiewicz, R. W. K. Odoni, P. Rémond, J. Śliwa, R. J. Valenza, and others. The relevant literature is summarized (often with full proofs) in the books of Geroldinger–Halter-Koch [2] and Narkiewicz [7].

For each nonzero $\alpha \in \mathbb{Z}_K$, we let $\nu(\alpha)$ denote the number of nonassociate irreducible elements of $\mathbb{Z}_K$ dividing α. We view $\nu(\cdot)$ as a generalization to $\mathbb{Z}_K$ of the classical arithmetic function $\omega(\cdot)$, which counts the number of distinct prime factors of its (rational integer) argument.

A 1940 theorem of Erdős and Kac asserts, roughly speaking, that $\omega(n)$ is normally distributed with mean $\log\log|n|$ and standard deviation $\sqrt{\log\log|n|}$. More precisely, for each fixed real u,

$$\frac{\#\{3 \le n \le x : \omega(n) \le \log\log n + u\sqrt{\log\log n}\}}{\#\{3 \le n \le x\}} \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{u} e^{-t^2/2}\,dt,$$

Research of the first-named author is supported by NSF award DMS-1402268.

as $x \to \infty$. This theorem of Erdős and Kac sharpens, in a striking way, the 1917 result of Hardy and Ramanujan [4] that $\omega(n)$ has normal order $\log\log n$. Recently [8], the first-named author proved the following generalization of Erdős–Kac: For every number field K, there are positive constants A and B, and a positive integer D, such that $\nu(\alpha)$ is normally distributed with mean $A(\log\log|N(\alpha)|)^D$ and standard deviation $B(\log\log|N(\alpha)|)^{D-1/2}$. The constants A, B, and D depend on K only through its class group. When the class group is trivial, $A = B = D = 1$, and so this result does indeed contain the original Erdős–Kac theorem.

While $\omega(n)$ is usually quite close to $\log\log n$, it occasionally gets much larger. For each $x \geq 2$, the maximum value of $\omega(n)$ on the integers $n \leq x$ is assumed when n is the product of a certain initial segment of primes. This easy observation, together with the prime number theorem, implies in a straightforward way (cf. [5, p. 471]) that

$$\max_{n\leq x} \omega(n) = (1+o(1))\frac{\log x}{\log\log x}, \tag{1.1}$$

as $x \to \infty$. Our first goal is to supply a corresponding description of the maximum value of $\nu(\alpha)$ for $\alpha \in \mathbb{Z}_K$ with $|N(\alpha)| \leq x$, for an arbitrary number field K. The answer in the general case is decidedly more interesting than the case $K = \mathbb{Q}$, and the proof, while similar in spirit, is correspondingly more subtle.

For a finite abelian group G (described multiplicatively), we let $D(G)$ denote the *Davenport constant of* G, i.e., the smallest positive integer with the property that any sequence of elements of G of length $D(G)$ possesses a nonempty subsequence whose product is the identity. We write D for the Davenport constant of the class group of K. (This is the same value of D that appears in the result from [8] quoted above.) We let h denote the class number of K. Our first main theorem is the following.

Theorem 1.1. *As $x \to \infty$, we have*

$$\max_{\alpha:\ 0<|N(\alpha)|\leq x} \nu(\alpha) = (1+o(1))\cdot M\cdot\left(\frac{\log x}{h\log\log x}\right)^D.$$

Here M is a positive constant depending only on the class group of K.

An explicit description of the constant M is given at the beginning of §4.

We turn now to our second theme, the distribution of irreducibles in arithmetic progressions. Let $\Pi(x)$ denote the count of nonassociate irreducibles $\pi \in \mathbb{Z}_K$ with $|N(\pi)| \leq x$. So when $K = \mathbb{Q}$, we have $\Pi(x) = \pi(x)$, the familiar rational prime counting function. It was shown by Rémond in 1966 [9, Chapter 2] that for any number field K,

$$\Pi(x) = (C+o(1))\frac{x}{\log x}(\log\log x)^{D-1}$$

for a constant $C > 0$ depending only on the class group of K. (We continue to use D for the Davenport constant of the class group.) When the class group is trivial, $C = D = 1$, and so this result contains the classical prime number theorem.

Our second main result is a corresponding generalization of the prime number theorem for arithmetic progressions. For $\mathfrak{m}$ a nonzero ideal of $\mathbb{Z}_K$ and α a nonzero element of $\mathbb{Z}_K$, we let $\Pi(x; \mathfrak{m}, \alpha)$ denote the following counting function of irreducibles:

$$\Pi(x; \mathfrak{m}, \alpha) = \#\{\text{principal ideals } (\pi) : |N\pi| \le x, \pi \text{ irred.}, \pi \equiv \alpha \pmod{\mathfrak{m}}, \text{ and } \frac{\pi}{\alpha} \gg 0\}.$$

Here the notation "$\gg 0$" indicates total positivity. (There will be no danger of confusion with Vinogradov's notation for orders of magnitude.) It is clear that if (α) and $\mathfrak{m}$ have a common principal ideal divisor in $\mathbb{Z}_K$ other than the unit ideal, then $\Pi(x; \mathfrak{m}, \alpha) \le 1$ for all x. If there is no such principal ideal, we will say that α and $\mathfrak{m}$ are *weakly relatively prime*. (We reserve the term *relatively prime* for the case when α and $\mathfrak{m}$ have no nonunit ideal divisors at all in common, or equivalently, for when α and $\mathfrak{m}$ are comaximal.)

Theorem 1.2. *Let $\mathfrak{m}$ be a nonzero ideal of $\mathbb{Z}_K$ and let α be a nonzero element of $\mathbb{Z}_K$ with α and $\mathfrak{m}$ weakly relatively prime. Then there is a positive constant C' and a positive integer L such that, as $x \to \infty$,*

$$\Pi(x; \mathfrak{m}, \alpha) = (C' + o(1))\frac{x}{\log x}(\log\log x)^{L-1}.$$

We refer the reader to Theorem 5.1 for a more explicit form of this theorem, including precise definitions of the quantities C' and L.

It is obvious by comparison with Rémond's theorem that $L \le D$, for all choices of α and $\mathfrak{m}$. It will emerge from the proof that (for K fixed) the constants C' and L depend only on the gcd ideal $(\alpha, \mathfrak{m})$, with $L = D$ precisely when $(\alpha, \mathfrak{m})$ is the unit ideal. Consequently, 100% of irreducibles are (strongly) relatively prime to $\mathfrak{m}$, and those are asymptotically uniformly distributed among the strict ray classes modulo $\mathfrak{m}$ represented by principal ideals prime to $\mathfrak{m}$.

2. Background on the equidistribution of prime ideals in ray classes

In both of our main results, the key analytic input is a 1918 theorem of Landau [6] on the equidistribution of prime ideals in strict ray classes. We recall the setup here. For detailed proofs of the basic facts used about ray class groups, see the recent book of Childress [1, Chapter 3].

For a number field K, we let $\mathrm{Id}(K)$ and $\mathrm{PrinFrac}(K)$ denote the group of all fractional ideals of K and all principal fractional ideals of K, respectively. For each nonzero integral ideal $\mathfrak{m}$ of K, let

$$\mathrm{Id}_{\mathfrak{m}}(K) = \{\text{fractional ideals } \mathfrak{a} : \mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ for all prime ideals } \mathfrak{p} \mid \mathfrak{m}\},$$

and let

$$\mathrm{PrinFrac}_{\mathfrak{m}}^{+}(K) = \{\gamma\mathbb{Z}_K : \gamma \in K, \gamma \equiv 1 \bmod^{+} \mathfrak{m}\};$$

here the $\bmod^{+}$ notation means that $\mathrm{ord}_{\mathfrak{p}}(\gamma - 1) \ge \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$ for all prime ideals $\mathfrak{p} \mid \mathfrak{m}$ and that $\gamma \gg 0$. The strict ray class group of K modulo $\mathfrak{m}$ is defined by

$$\mathrm{Cl}_{\mathfrak{m}}(K) := \mathrm{Id}_{\mathfrak{m}}(K)/\mathrm{PrinFrac}_{\mathfrak{m}}^{+}(K).$$

The order of $\mathrm{Cl}_{\mathfrak{m}}(K)$, referred to as the *strict ray class number mod* $\mathfrak{m}$, is denoted $h_{K,\mathfrak{m}}$. We view the partition of ideals prime to $\mathfrak{m}$ into strict ray classes as analogous to the partition of rational integers coprime to m into residue classes mod m. (In fact, if $K = \mathbb{Q}$ and $\mathfrak{m} = (m)$, then $\mathrm{Cl}_{\mathfrak{m}}(K) \cong (\mathbb{Z}/m\mathbb{Z})^{\times}$, via the map $[ab^{-1}\mathbb{Z}_K] \mapsto ab^{-1} \bmod m$.)

For each strict ray class $C \in \mathrm{Cl}_{\mathfrak{m}}(K)$, we define the prime ideal counting function

$$\pi_K(x; C) := \sum_{\substack{\mathfrak{p}:\ N(\mathfrak{p}) \le x \\ \mathfrak{p} \in C}} 1.$$

Theorem 2.1 (Landau's equidistribution theorem). *Fix a $C \in \mathrm{Cl}_{\mathfrak{m}}(K)$. For all $x \ge 3$,*

$$\pi_K(x; C) = \frac{1}{h_{K,\mathfrak{m}}} \int_2^x \frac{dt}{\log t} + O_K(x \exp(-c_K \sqrt{\log x})).$$

Here c_K is a positive constant depending only on K.

The following remarks will be useful in our applications. Recall that the (ordinary) class group of K, here denoted $\mathrm{Cl}(K)$, is defined as $\mathrm{Id}(K)/\mathrm{PrinFrac}(K)$. The inclusion $\mathrm{Id}_{\mathfrak{m}}(K) \hookrightarrow \mathrm{Id}(K)$ induces an isomorphism

$$\mathrm{Cl}(K) = \mathrm{Id}(K)/\mathrm{PrinFrac}(K) \cong \mathrm{Id}_{\mathfrak{m}}(K)/\mathrm{PrinFrac}_{\mathfrak{m}}(K),$$

where $\mathrm{PrinFrac}_{\mathfrak{m}}(K) = \mathrm{Id}_{\mathfrak{m}}(K) \cap \mathrm{PrinFrac}(K)$. In particular, letting $h_K := \#\mathrm{Cl}(K)$ (the ordinary class number),

$$\begin{aligned} h_K = [\mathrm{Id}_{\mathfrak{m}}(K) : \mathrm{PrinFrac}_{\mathfrak{m}}(K)] &= \frac{[\mathrm{Id}_{\mathfrak{m}}(K) : \mathrm{PrinFrac}^{+}_{\mathfrak{m}}(K)]}{[\mathrm{PrinFrac}_{\mathfrak{m}}(K) : \mathrm{PrinFrac}^{+}_{\mathfrak{m}}(K)]} \\ &= \frac{h_{K,\mathfrak{m}}}{[\mathrm{PrinFrac}_{\mathfrak{m}}(K) : \mathrm{PrinFrac}^{+}_{\mathfrak{m}}(K)]}. \end{aligned}$$

Rearranging,

$$[\mathrm{PrinFrac}_{\mathfrak{m}}(K) : \mathrm{PrinFrac}^{+}_{\mathfrak{m}}(K)] = \frac{h_{K,\mathfrak{m}}}{h_K}. \tag{2.1}$$

Thus, the ratio $h_{K,\mathfrak{m}}/h_K$ can be interpreted as the number of strict ray classes modulo $\mathfrak{m}$ represented by principal ideals prime to $\mathfrak{m}$. Motivated by the analogy with Euler's totient function, we set

$$\Phi(\mathfrak{m}) := \frac{h_{K,\mathfrak{m}}}{h_K}.$$

Various earlier algebro-analytic results can be recovered as special cases of Theorem 2.1. For instance, we easily deduce the equidistribution of prime ideals relative to the ordinary class group $\mathrm{Cl}(K)$; in that case, the factor $\frac{1}{h_{K,\mathfrak{m}}}$ in Theorem 2.1 should be replaced with $\frac{1}{h_K}$. (To see this implication, take $\mathfrak{m} = (1)$ in Theorem 2.1 and note that, by (2.1), each ideal class modulo (1) is a union of $h_{K,(1)}/h_K$ strict ray classes mod (1).) Theorem 2.1 also implies the *prime ideal theorem*, that the total number of prime ideals of norm not exceeding x is asymptotically $\int_2^x dt/\log t$. (Sum over all $h_{K,\mathfrak{m}}$ strict ray classes.) Since these earlier theorems are also due to Landau, we shall refer to any and all of these results as "Landau's theorem".

3. Anatomy of an irreducible

Since ideals of $\mathbb{Z}_K$ factor uniquely while elements typically do not, we will rephrase our questions about irreducible elements in ideal-theoretic terms. To make this translation, it is important to understand how irreducible elements decompose as products of prime ideals. We recall the basic results here (cf. [7, §9.1]).

Fix — once and for all — an ordering of the (ordinary) ideal classes, say $C_1, \dots, C_h$, where $h = h_K$.

We define a *type* as an h-tuple of nonnegative integers. Given a nonzero integral ideal $\mathfrak{a}$ of $\mathbb{Z}_K$, the *type of* $\mathfrak{a}$ is the tuple $(t_1, \dots, t_h)$, where t_i is the number of prime ideals dividing $\mathfrak{a}$ from the class C_i, counted with multiplicity. The type of a nonzero element of $\mathbb{Z}_K$ is defined as the type of the corresponding principal ideal.

Now let π be an irreducible element of $\mathbb{Z}_K$. Irreducibility implies that the prime ideal factorization of (π) has no nonempty proper subproduct equal to a principal ideal. Thus, if $\tau = (t_1, \dots, t_h)$ is the type of an irreducible, then τ has the property that $C_1^{t_1} \cdots C_h^{t_h}$ is trivial in $\mathrm{Cl}(K)$ but no proper nonempty subproduct is trivial. If $\tau = (t_1, \dots, t_h)$ is any type with this property and not all $t_i = 0$, we call τ an *irreducible type*.

Landau's theorem implies that every irreducible type $(t_1, \dots, t_h)$ is the type of an irreducible element. Indeed, if we multiply t_i prime ideals from the class C_i (for $i = 1, 2, \dots, h$), the result is a principal ideal, and each of its generators is an irreducible of the sought-after kind. (Landau's theorem is used here only to ensure the existence of at least one prime ideal in each ideal class.) Thus, the irreducible types are exactly the types of irreducibles.

Recall our notation D for the Davenport constant of $\mathrm{Cl}(K)$. It follows quickly from the definition of the Davenport constant that if $(t_1, \dots, t_h)$ is any irreducible type, then $t_1 + \cdots + t_h \le D$ (so that, in particular, there are only finitely many irreducible types) and that equality holds for some irreducible type. The quantity $t_1 + \cdots + t_h$ will be referred to as the *length* of $\tau = (t_1, \dots, t_h)$. We call an irreducible type with length D a *maximal irreducible type*.

4. The maximal order of ν: Proof of Theorem 1.1

Let $\mathcal{T}_{\max}$ denote the collection of maximal irreducible types, and consider the polynomial in $x_1, \dots, x_h$ defined by

$$P(x_1, \dots, x_h) = \sum_{\tau \in \mathcal{T}_{\max}} \prod_{i=1}^{h} \frac{x_i^{t_i}}{t_i!},$$

where we have written each τ as $(t_1, \dots, t_h)$. Note that P depends on K only via its class group. Let M denote the maximum value of P on the simplex

$$\Delta = \{(x_1, \dots, x_h) \in \mathbb{R}^h : x_i \ge 0 \ \ \forall i, \ \sum x_i \le h\}.$$

The value M exists, as the maximum of a polynomial on a compact set, and it is obvious that $M > 0$. We will show that Theorem 1.1 holds with this value of M.

The proof goes in two stages. First, we show the lower bound implicit in Theorem 1.1.

Lemma 4.1. *As $x \to \infty$,*

$$\max_{\alpha\colon 0<|N(\alpha)|\le x} \nu(\alpha) \ge (M - o(1))\Big(\frac{\log x}{h \log\log x}\Big)^D.$$

For the upper bound, it is convenient to extend the definition of ν as follows. For each nonzero ideal $\mathfrak{a}$ of $\mathbb{Z}_K$, we let $\nu(\mathfrak{a})$ denote the number of nonassociate irreducibles π for which (π) divides $\mathfrak{a}$. Thus, if $\mathfrak{a} = (\alpha)$, then $\nu(\mathfrak{a}) = \nu(\alpha)$.

Lemma 4.2. *For each nonzero integral ideal $\mathfrak{a}$ of $\mathbb{Z}_K$ with $N(\mathfrak{a}) \le x$,*

$$\nu(\mathfrak{a}) \le (M + o(1))\Big(\frac{\log x}{h \log\log x}\Big)^D.$$

Restricting to principal ideals in Lemma 4.2 yields the upper bound half of Theorem 1.1. Thus, it remains only to prove Lemmas 4.1 and 4.2.

4.1. Proof of Lemma 4.1. It is enough to show that for each fixed $\epsilon > 0$ and all $x > x_0(\epsilon)$, there is a nonzero $\alpha \in \mathbb{Z}_K$ with $|N(\alpha)| \le x$ and

$$\nu(\alpha) \ge (M - \epsilon)\left(\frac{\log x}{h \log\log x}\right)^D. \tag{4.1}$$

Let $\delta > 0$ be a parameter to be chosen later in terms of ϵ, and put $X = x^{1-\delta}$. We fix a point $(\gamma_1, \dots, \gamma_h) \in \Delta$ at which P achieves its maximum. Let $\mathfrak{a}$ be the (integral) ideal of $\mathbb{Z}_K$ defined by

$$\mathfrak{a} := \prod_{i=1}^{h} \prod_{\substack{\mathfrak{p} \in C_i \\ N(\mathfrak{p}) \le \gamma_i \log X}} \mathfrak{p}.$$

Landau's equidistribution theorem implies that each term of the inside product is of size $X^{\gamma_i/h + o(1)}$ (as $x \to \infty$); since $\sum \gamma_i \le h$,

$$N(\mathfrak{a}) \le X^{1+o(1)} = x^{1-\delta+o(1)}.$$

(To estimate the product we used a form of Landau's result where prime ideals are counted with weight $\log N(\mathfrak{p})$ rather than weight 1; this may be deduced by partial summation from Theorem 2.1 by a standard calculation.) This upper bound implies that, for x sufficiently large, $\mathfrak{a}$ has a principal multiple with norm at most x; indeed, it suffices to multiply $\mathfrak{a}$ by the smallest ideal in $[\mathfrak{a}]^{-1}$. So it is enough to show that $\nu(\mathfrak{a})$ is at least as large as the right-side of (4.1).

We establish this bound by counting, for each maximal type τ, the number of nonassociated irreducibles π of type τ with $(\pi) \mid \mathfrak{a}$. Since $\mathfrak{a}$ is a product of distinct prime ideals, the number of these for a given τ is exactly

$$\prod_{i=1}^{h} \binom{\omega_i(\mathfrak{a})}{t_i}, \tag{4.2}$$

where $\omega_i(\mathfrak{a})$ is the number of distinct prime ideal divisors of $\mathfrak{a}$ from the class C_i. By Landau's theorem, for each i with $\gamma_i \neq 0$,

$$\begin{aligned}\omega_i(\mathfrak{a}) &= \sum_{\substack{\mathfrak{p}\in C_i \\ N(\mathfrak{p})\leq \gamma_i \log X}} 1 \\ &= (\gamma_i + o(1))\frac{\log X}{h \log\log X}. \qquad (4.3)\end{aligned}$$

The terms of the product (4.2) with $t_i = 0$ are identically 1; for the others,

$$\begin{aligned}\binom{\omega_i(\mathfrak{a})}{t_i} &= \frac{\omega_i(\mathfrak{a})(\omega_i(\mathfrak{a})-1)\cdots(\omega_i(\mathfrak{a})-(t_i-1))}{t_i!} \\ &= \frac{\omega_i(\mathfrak{a})^{t_i}}{t_i!} + O\Big(\Big(\frac{\log X}{\log\log X}\Big)^{t_i-1}\Big).\end{aligned}$$

As a consequence, the number of nonassociate irreducible divisors of $\mathfrak{a}$ of type τ is

$$\prod_{\substack{1\leq i\leq h \\ t_i\neq 0}} \frac{\omega_i(\mathfrak{a})^{t_i}}{t_i!} + O((\log X/\log\log X)^{D-1}). \qquad (4.4)$$

Suppose first that whenever $t_i \neq 0$, we have $\gamma_i \neq 0$. In that case, substituting in the estimate (4.3) for $\omega_i(\mathfrak{a})$ yields

$$\begin{aligned}\prod_{\substack{1\leq i\leq h \\ t_i\neq 0}} \frac{\omega_i(\mathfrak{a})^{t_i}}{t_i!} &= (1+o(1)) \prod_{\substack{1\leq i\leq h \\ t_i\neq 0}} \frac{\gamma_i^{t_i}}{t_i!}\Big(\frac{\log X}{h\log\log X}\Big)^{t_i} \\ &= \Big(\prod_{1\leq i\leq h} \frac{\gamma_i^{t_i}}{t_i!}\Big)\Big(\frac{\log X}{h\log\log X}\Big)^D + o\Big(\Big(\frac{\log X}{h\log\log X}\Big)^D\Big). \qquad (4.5)\end{aligned}$$

If $\gamma_i = 0$ for some i with $t_i \neq 0$, then $\prod_{1\leq i\leq h,\ t_i\neq 0} \frac{\omega_i(\mathfrak{a})^{t_i}}{t_i!} = 0 = \prod_{1\leq i\leq h} \frac{\gamma_i^{t_i}}{t_i!}$, and hence (4.5) remains valid.

Inserting (4.5) back into (4.4) and then summing over maximal types τ, we conclude that there are

$$M\Big(\frac{\log X}{h\log\log X}\Big)^D + o\Big(\Big(\frac{\log X}{h\log\log X}\Big)^D\Big)$$

nonassociate irreducible divisors of $\mathfrak{a}$. This expression is $\sim M(1-\delta)^D\big(\frac{\log x}{h\log\log x}\big)^D$. Choosing δ sufficiently small in terms of ϵ gives a lower bound exceeding the right-hand side in (4.1).

4.2. Proof of Lemma 4.2. Fix an ideal $\mathfrak{a}$ with $\nu(\mathfrak{a})$ maximal among all nonzero ideals with $N(\mathfrak{a}) \leq x$. We may assume that $\mathfrak{a}$ has the following property: Whenever a prime ideal $\mathfrak{p}$ divides $\mathfrak{a}$, every prime ideal $\mathfrak{p}'$ belonging to the same ideal class of $\mathfrak{p}$ with $N(\mathfrak{p}') < N(\mathfrak{p})$ also divides $\mathfrak{a}$. If not, then define a new ideal $\mathfrak{a}'$ by replacing $\mathfrak{p}$ by $\mathfrak{p}'$ in the ideal factorization of $\mathfrak{a}$; then $\mathfrak{a}'$ has the same number of irreducible divisors as $\mathfrak{a}$, and $N(\mathfrak{a}') < N(\mathfrak{a}) \leq x$. We can repeat this procedure as necessary until we obtain an ideal with the desired property.

We may restrict ourselves to counting irreducibles π dividing $\mathfrak{a}$ which are (a) of maximal type and (b) have (π) squarefree. Indeed, if either (a) or (b) fails, then (π) is composed of at most $D-1$ distinct prime ideals. The number of distinct prime ideals dividing $\mathfrak{a}$ is $\ll \log x/\log\log x$ (by a proof entirely analogous to that of (1.1)). Hence, the number of possibilities for the set of prime ideals dividing (π) is $\ll (\log x/\log\log x)^{D-1}$. Furthermore, having chosen the set of prime ideals dividing (π), the number of (π) composed of those prime ideals is $O(1)$; one can see this by noting, for instance, that the exponent to which each prime ideal can appear is bounded (e.g., by h). Thus, there are $\ll (\log x/\log\log x)^{D-1}$ irreducible divisors of $\mathfrak{a}$ not satisfying (a) and (b), and this will be negligible for us.

For each $1 \leq i \leq h$, define u_i so that the largest prime ideal dividing $\mathfrak{a}$ and belonging to the ideal class C_i has norm $u_i \log x$; if no such prime ideal exists, set $u_i = 0$. Set

$$\mathfrak{a}_0 := \prod_{\substack{1\leq i\leq h\\ u_i\neq 0}} \prod_{\substack{\mathfrak{p}\in C_i\\ N(\mathfrak{p})<u_i\log x}} \mathfrak{p}.$$

Notice that $\mathfrak{a}_0 \mid \mathfrak{a}$, and so

$$N(\mathfrak{a}_0) \leq N(\mathfrak{a}) \leq x.$$

If $u_i > 1/\log\log x$, then we may deduce from Landau's theorem that

$$\prod_{\substack{\mathfrak{p}\in C_i\\ N(\mathfrak{p})<u_i\log(x)}} N(\mathfrak{p}) \geq x^{u_i(1+o(1))/h}.$$

Hence,

$$\sum_{i:\ u_i>1/\log\log x} u_i \leq h + o(1). \tag{4.6}$$

Proceeding as in the lower bound argument, we see that the count of nonassociated irreducibles π dividing $\mathfrak{a}$ with (π) squarefree and π having a given maximal type $\tau = (t_1, \ldots, t_h)$ is

$$\begin{aligned}\prod_{i=1}^{h}\binom{\omega_i(\mathfrak{a})}{t_i} &= \prod_{\substack{1\leq i\leq h\\ t_i\neq 0}}\Big(\frac{\omega_i(\mathfrak{a})^{t_i}}{t_i!} + O\Big(\Big(\frac{\log x}{\log\log x}\Big)^{t_i-1}\Big)\Big)\\ &= \prod_{\substack{1\leq i\leq h\\ t_i\neq 0}}\frac{\omega_i(\mathfrak{a})^{t_i}}{t_i!} + O\Big(\Big(\frac{\log x}{\log\log x}\Big)^{D-1}\Big).\end{aligned}$$

To control the error terms, we used here that for each i,

$$\omega_i(\mathfrak{a}) = O(\log x/\log\log x), \tag{4.7}$$

which follows from having each $u_i \le 2h$, say (which in turn follows, for large x, from (4.6)). Suppose first that $u_i > 1/\log\log x$ for each index i with $t_i \neq 0$. Then for each i with $t_i \neq 0$, Landau's theorem shows that $\omega_i(\mathfrak{a}) = (1+o(1))\frac{u_i \log x}{h\log\log x}$, and so

$$\prod_{\substack{1\le i\le h\\ t_i\neq 0}} \frac{\omega_i(\mathfrak{a})^{t_i}}{t_i!} = \prod_{i=1}^{h} \frac{u_i^{t_i}}{t_i!}\Big(\frac{\log x}{h\log\log x}\Big)^D + o\Big(\Big(\frac{\log x}{h\log\log x}\Big)^D\Big).$$

Suppose now that some $u_i \le 1/\log\log x$. Then for this index i, we have $u_i \log x \le \log x/\log\log x$, so that (by Landau's theorem again)

$$\omega_i(\mathfrak{a}) = O\Big(\frac{\log x}{(\log\log x)^2}\Big).$$

It follows that

$$\prod_{\substack{1\le i\le h\\ t_i\neq 0}} \frac{\omega_i(\mathfrak{a})^{t_i}}{t_i!} \ll \left(\frac{\log x}{\log\log x}\right)^D (\log\log x)^{-1},$$

using the bound (4.7) for the other choices of i. In all cases, our count of (π) is at most

$$\prod_{i=1}^{h} \frac{u_i^{t_i}}{t_i!}\Big(\frac{\log x}{h\log\log x}\Big)^D + o\Big(\Big(\frac{\log x}{h\log\log x}\Big)^D\Big).$$

Summing over the maximal types τ, we conclude that

$$\nu(\mathfrak{a}) \le (P(u_1,\dots,u_h)+o(1))\Big(\frac{\log x}{h\log\log x}\Big)^D. \tag{4.8}$$

Since

$$\sum_{i=1}^{h} u_i = \sum_{i\colon\ u_i\le 1/\log\log x} u_i + \sum_{i\colon\ u_i > 1/\log\log x} u_i \le h + o(1),$$

the point $(u_1,\dots,u_h)$ gets arbitrarily close to a point of Δ as $x\to\infty$. By the definition of M and the uniform continuity of P (on a closed set slightly larger than Δ), we have that

$$P(u_1,\dots,u_h) \le M + o(1).$$

Inserting this into (4.8) completes the proof.

Example 4.3 (analysis of the main term in Theorem 1.1 when Cl(K) is cyclic). *Suppose that* Cl(K) *is cyclic of order h. Number the ideal classes as $C_1,\dots,C_h$, where C_i corresponds to* i mod h *under a fixed isomorphism of* Cl(K) *with* $\mathbb{Z}/h\mathbb{Z}$. *It is known that* $D(\mathrm{Cl}(K)) = h$ *and that the maximal types are* $(0,\dots,0,h,0,\dots,0)$, *where the h may appear in any of the $\phi(h)$ positions* $1\le i\le h$ *with* $\gcd(i,h)=1$ *(see [3,* Corollary 2.1.4, p. 24*]). Thus,*

$$P(x_1,\dots,x_h) = \sum_{\substack{1\le i\le h\\ \gcd(i,h)=1}} x_i^h/h!.$$

It is easily seen that the maximum of P on Δ occurs when $x_1 = h$ and all other x_i vanish, so that

$$M = h^h/h!.$$

We conclude that

$$\max_{\alpha\colon 0<|N(\alpha)|\le x} \nu(\alpha) = (1+o(1)) \cdot \frac{1}{h!}\Big(\frac{\log x}{\log\log x}\Big)^h,$$

as $x \to \infty$.

5. Irreducibles in arithmetic progressions: Proof of Theorem 1.2

Using the notation of Theorem 1.2, let $\mathfrak{g} := (\alpha, \mathfrak{m})$ be the gcd ideal of (α) and $\mathfrak{m}$. Clearly, each (π) counted in Theorem 1.2 is divisible by $\mathfrak{g}$. To proceed with the proof of that theorem, we need to tailor the structure theory of irreducibles introduced in §3 to irreducibles divisible by $\mathfrak{g}$.

We call a type $\tau = (t_1, \dots, t_h)$ *principal* if $C_1^{t_1} \cdots C_h^{t_h}$ is trivial in $\mathrm{Cl}(K)$. If τ and τ' are any two types, we say that τ' *is a subtype of* τ, and write $\tau' \preceq \tau$, if each component of τ' is less than or equal to the corresponding component of τ. Thus, an irreducible type is a principal type with no nonzero principal subtype.

Observe that if a type τ' has no nonzero principal subtype, then $\tau' \preceq \tau$ for some (not necessarily unique) irreducible type τ. Indeed, if $\tau' = (t_1', \dots, t_h')$ is not itself irreducible, we may take $\tau = (t_1', \dots, t_{j-1}', t_j' + 1, t_{j+1}', \dots, t_h')$, where j is chosen so that $C_1^{t_1'} \cdots C_h^{t_h'} = C_j^{-1}$. An irreducible type τ is said to be *maximal with respect to* τ' if $\tau' \preceq \tau$ and the length of τ is maximal among those irreducible types having τ' as a subtype.

We now return to the situation of Theorem 1.2. Since (α) and $\mathfrak{m}$ are weakly relatively prime, the type τ' of $\mathfrak{g} = (\alpha, \mathfrak{m})$ has no principal subtype. We now restate Theorem 1.2 in the form in which it will be proved, making explicit the constants in the asymptotic formula.

Theorem 5.1. *Let τ' be the type of $\mathfrak{g} := (\alpha, \mathfrak{m})$. As $x \to \infty$, we have*

$$\Pi(x; \mathfrak{m}, \alpha) \sim \frac{1}{N(\mathfrak{g})\Phi(\mathfrak{m}\mathfrak{g}^{-1})} \frac{L}{h^L}\Big(\sum_{\substack{\tau' \preceq \tau \\ \tau \text{ max'l w.r.t. } \tau'}} \frac{1}{t_1! \cdots t_h!}\Big) \frac{x}{\log x} (\log\log x)^{L-1},$$

where $\tau - \tau' = (t_1, \dots, t_h)$, and where L is the (common) length of the types $\tau - \tau'$.

Theorem 5.1 follows immediately from the next proposition, upon summing over all types τ maximal relative to τ'.

Proposition 5.2. *Keep the notation of Theorem 5.1. Let τ be a fixed irreducible type which is maximal with respect to τ'. The number of ideals of norm at most x generated by an irreducible element π of type τ with $\pi \equiv \alpha \pmod{\mathfrak{m}}$ and $\pi/\alpha \gg 0$ is asymptotically equal to*

$$\frac{1}{N(\mathfrak{g})\Phi(\mathfrak{m}\mathfrak{g}^{-1})} \frac{L}{h^L} \left(\prod_{j=1}^{h} \frac{1}{t_j!} \right) \frac{x}{\log x} (\log\log x)^{L-1}, \tag{5.1}$$

where $\tau - \tau' = (t_1, \dots, t_h)$ and $L = t_1 + \cdots + t_h$.

The proof of Proposition 5.2 depends on the following lemma, which allows us to restrict our attention to ideals divisible by a large prime factor.

Lemma 5.3. *Fix $k \in \mathbb{Z}^+$. As $x \to \infty$, the number of (integral) ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \leq x$ having k prime ideal factors (counted with multiplicity) which are not divisible by a prime ideal with norm exceeding $x^{1-1/\log\log x}$ is*

$$o\biggl(\frac{x(\log\log x)^{k-1}}{\log x}\biggr).$$

Proof of Lemma 5.3. The number of ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \leq x^{1-\frac{1}{2\log\log x}}$ is $O(x^{1-\frac{1}{2\log\log x}})$, which is negligible. Thus, we may restrict our attention to $\mathfrak{a}$ with $N(\mathfrak{a}) > x^{1-\frac{1}{2\log\log x}}$. When $k = 1$, there are no such $\mathfrak{a}$ meeting the conditions of the lemma, and so we may assume that $k \geq 2$. Write $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_k$, where $N(\mathfrak{p}_1) \leq \cdots \leq N(\mathfrak{p}_k)$. Then

$$N(\mathfrak{p}_k) > x^{1-\frac{1}{2\log\log x}} N(\mathfrak{p}_1 \cdots \mathfrak{p}_{k-1})^{-1}.$$

So if $N(\mathfrak{p}_k) \leq x^{1-1/\log\log x}$, then

$$\prod_{j=1}^{k-1} N(\mathfrak{p}_j) \geq x^{\frac{1}{2\log\log x}}.$$

This implies that $N(\mathfrak{p}_{k-1}) \geq x^{\frac{1}{2k\log\log x}}$. We fix $\mathfrak{p}_1, \dots, \mathfrak{p}_{k-1}$ and count the number of corresponding values of $\mathfrak{p}_k$. Since $x/N(\mathfrak{p}_1 \cdots \mathfrak{p}_{k-1}) \geq N(\mathfrak{p}_k) \geq x^{1/2k}$ (since $N(\mathfrak{p}_k)^k \geq N(\mathfrak{a}) \geq x^{1/2}$), we can use the prime ideal theorem to estimate the number of possibilities for $\mathfrak{p}_k$ given $\mathfrak{p}_1, \dots, \mathfrak{p}_{k-1}$ as

$$\ll \frac{x}{\log x} \frac{1}{N(\mathfrak{p}_1 \cdots \mathfrak{p}_{k-1})}.$$

We now sum on $\mathfrak{p}_1, \dots, \mathfrak{p}_{k-1}$. By the prime ideal theorem (with the error term of Theorem 2.1) and partial summation, we have

$$\sum_{N(\mathfrak{p}) \leq x} \frac{1}{N(\mathfrak{p})} = \log\log x + O(1);$$

this provides an upper bound for the sum on $\mathfrak{p}_j$ for $1 \leq j \leq k-2$. For the sum on $\mathfrak{p}_{k-1}$, we use the estimate

$$\sum_{x^{\frac{1}{2k\log\log x}} \leq N(\mathfrak{p}) \leq x} \frac{1}{N(\mathfrak{p})} = \log\log\log x + O(1).$$

Thus, we obtain an upper bound on the number of $\mathfrak{a}$ that is

$$\ll \frac{x(\log\log x)^{k-2}}{\log x} \log\log\log x,$$

which implies the lemma. □

The following lemma will reduce the problem of counting our ideals (π) to one of counting ideals of a certain type lying in a specific strict ray class.

Lemma 5.4. *Let $\mathfrak{a}$ be a nonzero integral ideal of $\mathbb{Z}_K$ divisible by $\mathfrak{g}$. Then $\mathfrak{a} = (\rho)$ for some $\rho \equiv \alpha \pmod{\mathfrak{m}}$ with $\rho/\alpha \gg 0$ if and only if $\mathfrak{a}\mathfrak{g}^{-1}$ and $(\alpha)\mathfrak{g}^{-1}$ represent the same element of $\mathrm{Cl}_{\mathfrak{m}\mathfrak{g}^{-1}}(K)$.*

Proof. First, suppose that $\mathfrak{a}$ admits a generator $\rho \equiv \alpha \pmod{\mathfrak{m}}$ with $\rho/\alpha \gg 0$. Then

$$\mathfrak{a}\mathfrak{g}^{-1} = (\rho/\alpha)\cdot((\alpha)\mathfrak{g}^{-1}). \tag{5.2}$$

We claim that

$$\rho/\alpha \equiv 1 \bmod^{+} \mathfrak{m}\mathfrak{g}^{-1}. \tag{5.3}$$

By assumption, $\rho/\alpha \gg 0$, so it remains to show that $\mathrm{ord}_{\mathfrak{p}}(\rho/\alpha - 1) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}\mathfrak{g}^{-1})$ for all $\mathfrak{p} \mid \mathfrak{m}\mathfrak{g}^{-1}$. If $\mathfrak{p}$ divides $\mathfrak{m}\mathfrak{g}^{-1}$, then $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) < \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$; since $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) = \min\{\mathrm{ord}_{\mathfrak{p}}(\alpha), \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})\}$, it must be that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) = \mathrm{ord}_{\mathfrak{p}}(\alpha)$, and

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}\mathfrak{g}^{-1}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}) - \mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) &= \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}) - \mathrm{ord}_{\mathfrak{p}}(\alpha)\\ &\leq \mathrm{ord}_{\mathfrak{p}}(\rho-\alpha) - \mathrm{ord}_{\mathfrak{p}}(\alpha) = \mathrm{ord}_{\mathfrak{p}}(\rho/\alpha - 1).\end{aligned}$$

In view of (5.2) and (5.3) , $\mathfrak{a}\mathfrak{g}^{-1}$ and $(\alpha)\mathfrak{g}^{-1}$ represent the same element of $\mathrm{Cl}_{\mathfrak{m}\mathfrak{g}^{-1}}(K)$, as long as $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\mathfrak{g}^{-1}) = \mathrm{ord}_{\mathfrak{p}}((\alpha)\mathfrak{g}^{-1}) = 0$ for all $\mathfrak{p} \mid \mathfrak{m}\mathfrak{g}^{-1}$. That $\mathrm{ord}_{\mathfrak{p}}((\alpha)\mathfrak{g}^{-1}) = 0$ for all $\mathfrak{p} \mid \mathfrak{m}\mathfrak{g}^{-1}$ is clear, since $\mathfrak{g}$ is the gcd of (α) and $\mathfrak{m}$. Since $\mathrm{ord}_{\mathfrak{p}}(\rho/\alpha - 1) > 0$ for all $\mathfrak{p} \mid \mathfrak{m}\mathfrak{g}^{-1}$, the strong triangle inequality yields

$$\mathrm{ord}_{\mathfrak{p}}(\rho/\alpha) = \mathrm{ord}_{\mathfrak{p}}((\rho/\alpha - 1) + 1) = 0$$

for such $\mathfrak{p}$. Thus, (5.2) implies that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a}\mathfrak{g}^{-1}) = 0$ for all $\mathfrak{p} \mid \mathfrak{m}\mathfrak{g}^{-1}$.

We now turn to the converse implication. Suppose that $\mathfrak{a}\mathfrak{g}^{-1}$ and $(\alpha)\mathfrak{g}^{-1}$ represent the same element of $\mathrm{Cl}_{\mathfrak{m}\mathfrak{g}^{-1}}(K)$. Then $\mathfrak{a}\mathfrak{g}^{-1} = \gamma(\alpha)\mathfrak{g}^{-1}$, where $\gamma \in K$ satisfies $\gamma \equiv 1 \bmod^{+} \mathfrak{m}\mathfrak{g}^{-1}$. Thus $\mathfrak{a} = \gamma\alpha\mathbb{Z}_K$; since $\mathfrak{a}$ is integral, $\rho := \gamma\alpha \in \mathbb{Z}_K$. The proof is completed by showing that $\rho/\alpha \gg 0$ and that $\rho \equiv \alpha \pmod{\mathfrak{m}}$.

Since $\gamma \equiv 1 \bmod^{+} \mathfrak{m}\mathfrak{g}^{-1}$, we have $\rho/\alpha = \gamma \gg 0$. To prove the congruence for ρ mod $\mathfrak{m}$, we start by noticing if $\mathfrak{p} \mid \mathfrak{m}\mathfrak{g}^{-1}$, then

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}(\rho - \alpha) = \mathrm{ord}_{\mathfrak{p}}(\alpha) + \mathrm{ord}_{\mathfrak{p}}(\gamma - 1) &\geq \mathrm{ord}_{\mathfrak{p}}(\alpha) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}\mathfrak{g}^{-1})\\ &= \mathrm{ord}_{\mathfrak{p}}(\alpha) + \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}) - \mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}).\end{aligned}$$

If $\mathfrak{p} \mid \mathfrak{m}$ but $\mathfrak{p} \nmid \mathfrak{m}\mathfrak{g}^{-1}$, then $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$. Since $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) = \min\{\mathrm{ord}_{\mathfrak{p}}(\alpha), \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})\}$, it follows that $\mathrm{ord}_{\mathfrak{p}}(\alpha) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$. Moreover, since $\mathfrak{g} \mid \mathfrak{a} = (\rho)$, we know that for these same $\mathfrak{p}$,

$$\mathrm{ord}_{\mathfrak{p}}(\rho) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{g}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m});$$

hence,

$$\mathrm{ord}_{\mathfrak{p}}(\rho - \alpha) \geq \min\{\mathrm{ord}_{\mathfrak{p}}(\rho), \mathrm{ord}_{\mathfrak{p}}(\alpha)\} \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}).$$

Putting the above arguments together shows that $\mathrm{ord}_{\mathfrak{p}}(\rho - \alpha) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m})$ for all $\mathfrak{p} \mid \mathfrak{m}$, and so $\rho \equiv \alpha \pmod{\mathfrak{m}}$. □

5.1. Proof of Proposition 5.2. We are to count the number of ideals (π) of bounded norm where π is an irreducible of type τ with $\pi \equiv \alpha \pmod{\mathfrak{m}}$ and $\pi/\alpha \gg 0$. Rather than count these (π) directly, it is more convenient to count values of $\mathfrak{j} := (\pi)\mathfrak{g}^{-1}$.

By Lemma 5.4, the integral ideals $\mathfrak{j}$ which arise are precisely those of type $\tau - \tau'$ with $\mathfrak{j}$ relatively prime to $\mathfrak{m}\mathfrak{g}^{-1}$ and lying in the strict ray class of $(\alpha)\mathfrak{g}^{-1}$ modulo $\mathfrak{m}\mathfrak{g}^{-1}$. Moreover, the condition that $N(\pi) \leq x$ corresponds to the constraint that $N(\mathfrak{j}) \leq X := x/N(\mathfrak{g})$.

We first prove an upper bound on the number of these $\mathfrak{j}$ that matches the asymptotic formula claimed in Proposition 5.2.

Since $\mathfrak{j}$ has type $\tau - \tau'$, which is of length L, the $\mathfrak{j}$ under consideration are products of L prime ideals (possibly with repetition). By Lemma 5.3, we can assume one of these prime ideals has norm exceeding $X^{1-1/\log\log X}$, at the cost of excluding $o(X(\log\log X)^{L-1}/\log X)$ values of $\mathfrak{j}$, which is negligible. Thus,

$$\mathfrak{j} = \mathfrak{p}_1 \cdots \mathfrak{p}_L,$$

where the prime ideals $\mathfrak{p}_i$ are comaximal with $\mathfrak{m}\mathfrak{g}^{-1}$, and where $N(\mathfrak{p}_L) > X^{1-1/\log\log X}$.

Recall that $t_1, \dots, t_h$ are defined by the equation $\tau - \tau' = (t_1, \dots, t_h)$. Since $\mathfrak{j}$ has type $\tau - \tau'$, the class C_i of $\mathfrak{p}_L$ must satisfy $t_i > 0$. We fix an index i $(1 \leq i \leq h)$ with $t_i > 0$ and bound the number of $\mathfrak{j}$ with $\mathfrak{p}_L$ belonging to C_i.

Write $\mathfrak{j} = \mathfrak{j}_0\mathfrak{p}_L$. Then $\mathfrak{j}_0$ is a product of $L-1$ prime ideals (with multiplicity), t_j of which belong to the class C_j for $j \neq i$, and $t_i - 1$ of which belong to the class C_i. Moreover, given $\mathfrak{j}_0$, the strict ray class of $\mathfrak{p}_L$ modulo $\mathfrak{m}\mathfrak{g}^{-1}$ is uniquely determined as the class of $(\alpha)\mathfrak{g}^{-1}\mathfrak{j}_0^{-1}$. Since $N(\mathfrak{j}_0\mathfrak{p}_L) = N(\mathfrak{j}) \leq X$, we also have that

$$N(\mathfrak{p}_L) \leq \frac{X}{N(\mathfrak{j}_0)}.$$

Noting that $X/N(\mathfrak{j}_0) \geq N(\mathfrak{p}_L) \geq X^{1-1/\log\log X}$, Landau's equidistribution theorem (for strict ray classes modulo $\mathfrak{m}\mathfrak{g}^{-1}$) implies that the number of possibilities for $\mathfrak{p}_L$ given $\mathfrak{j}_0$ is

$$\leq (1+o(1))\frac{X/N(\mathfrak{j}_0)}{h_{K,\mathfrak{m}\mathfrak{g}^{-1}}\log(X/N(\mathfrak{j}_0))} \leq \Big(\frac{1}{h_{K,\mathfrak{m}\mathfrak{g}^{-1}}} + o(1)\Big)\frac{1}{N(\mathfrak{j}_0)}\frac{x}{N(\mathfrak{g})\log x}.$$

(Recall that $X = x/N(\mathfrak{g})$.) Now sum on $\mathfrak{j}_0$. The contribution of nonsquarefree values of $\mathfrak{j}_0$ to $\sum \frac{1}{N(\mathfrak{j}_0)}$ is zero unless $L \geq 3$, in which case it is

$$\leq \Bigg(\sum_{N(\mathfrak{p})\leq x} \frac{1}{N(\mathfrak{p})^2}\Bigg)\Bigg(\sum_{N(\mathfrak{p})\leq x}\frac{1}{N(\mathfrak{p})}\Bigg)^{L-3} \ll (\log\log x)^{L-3}.$$

The contribution of squarefree values of $\mathfrak{j}_0$ to $\sum \frac{1}{N(\mathfrak{j}_0)}$ is, by the multinomial theorem,

$$\leq \Bigg(\prod_{\substack{1\leq j\leq h\\ j\neq i}} \frac{1}{t_j!}\Bigg(\sum_{\substack{N(\mathfrak{p})\leq x\\ \mathfrak{p}\in C_j}}\frac{1}{N(\mathfrak{p})}\Bigg)^{t_j}\Bigg)\cdot\frac{1}{(t_i-1)!}\Bigg(\sum_{\substack{N(\mathfrak{p})\leq x\\ \mathfrak{p}\in C_i}}\frac{1}{N(\mathfrak{p})}\Bigg)^{t_i-1}.$$

By Landau's theorem and partial summation, $\sum_{\substack{N(\mathfrak{p})\le x\\ \mathfrak{p}\in C}} \frac{1}{N(\mathfrak{p})} = \frac{1}{h}\log\log x + O(1)$ for any ideal class C. Putting this in above, we find that

$$\sum \frac{1}{N(\mathfrak{j}_0)} \le (1+o(1))\left(t_i \prod_{j=1}^{h} \frac{1}{t_j!}\right)\left(\frac{1}{h}\log\log x\right)^{L-1},$$

so that the number of corresponding $\mathfrak{j}$ is

$$\le (1+o(1))\frac{1}{N(\mathfrak{g})h_{K,\mathfrak{m}\mathfrak{g}^{-1}}h^{L-1}}\left(t_i \prod_{j=1}^{h} \frac{1}{t_j!}\right)\frac{x}{\log x}(\log\log x)^{L-1}.$$

Now sum on i with $t_i \neq 0$. Since $\sum_{i:\ t_i\neq 0} t_i = \sum_i t_i = L$, we conclude that the total number of $\mathfrak{j}$ is

$$\le (1+o(1))\frac{L}{N(\mathfrak{g})h_{K,\mathfrak{m}\mathfrak{g}^{-1}}h^{L-1}}\left(\prod_{j=1}^{h} \frac{1}{t_j!}\right)\frac{x}{\log x}(\log\log x)^{L-1}.$$

Recalling that $\Phi(\mathfrak{m}\mathfrak{g}^{-1}) = h_{K,\mathfrak{m}\mathfrak{g}^{-1}}/h$, we see that

$$\frac{L}{N(\mathfrak{g})h_{K,\mathfrak{m}\mathfrak{g}^{-1}}h^{L-1}} = \frac{1}{N(\mathfrak{g})\Phi(\mathfrak{m}\mathfrak{g}^{-1})}\cdot\frac{1}{h^L}.$$

Making this substitution in the previous display, our upper bound matches the expression (5.1) from Proposition 5.2.

The proof of the lower bound in Proposition 5.2 is similar. Fix $i \in \{1,2,\dots,h\}$ with $t_i > 0$. Let $\mathfrak{p}_1,\dots,\mathfrak{p}_{L-1}$ be distinct prime ideals not dividing $\mathfrak{m}\mathfrak{g}^{-1}$ whose norms belong to the interval $[2, X^{1/\log\log X}]$, with t_j of these $\mathfrak{p}_j$ belonging to the class C_j for $j \neq i$, and $t_i - 1$ of the $\mathfrak{p}_j$ belonging to the class C_i. Let $\mathfrak{p}_L$ be a prime ideal with

$$X^{1/2} \le N(\mathfrak{p}_L) \le X/N(\mathfrak{p}_1\cdots\mathfrak{p}_{L-1})$$

belonging to the strict ray class modulo $\mathfrak{m}\mathfrak{g}^{-1}$ of $(\alpha)\mathfrak{g}^{-1}\mathfrak{p}_1^{-1}\cdots\mathfrak{p}_{L-1}^{-1}$. Define

$$\mathfrak{j} = \mathfrak{p}_1\cdots\mathfrak{p}_L.$$

Let us see that $\mathfrak{j}$ satisfies the conditions set down at the start of the proof. The ideal $\mathfrak{g}\mathfrak{j}$ is principal, since it is lies in the same strict ray class modulo $\mathfrak{m}\mathfrak{g}^{-1}$ as the principal ideal (α). This implies that $\mathfrak{p}_L \in C_i$. Indeed, let $\mathfrak{p}$ be a prime ideal from C_i. Then $\mathfrak{p}_1\cdots\mathfrak{p}_{L-1}\mathfrak{p}$ has type $(t_1,\dots,t_h) = \tau - \tau'$, so that $\mathfrak{g}\mathfrak{p}_1\cdots\mathfrak{p}_{L-1}\mathfrak{p}$ has type τ. Since τ is an irreducible type, $\mathfrak{g}\mathfrak{p}_1\cdots\mathfrak{p}_{L-1}\mathfrak{p}$ is principal, and hence so is

$$(\mathfrak{g}\mathfrak{p}_1\cdots\mathfrak{p}_{L-1}\mathfrak{p})(\mathfrak{g}\mathfrak{j})^{-1} = \mathfrak{p}\mathfrak{p}_L^{-1}.$$

But this is only possible if $\mathfrak{p}_L \in C_i$. It follows that $\mathfrak{j}$ has type $\tau - \tau'$. By construction, $\mathfrak{j}$ is relatively prime to $\mathfrak{m}\mathfrak{g}^{-1}$, lies in the strict ray class of $(\alpha)\mathfrak{g}^{-1}$ modulo $\mathfrak{m}\mathfrak{g}^{-1}$, and satisfies $N(\mathfrak{j}) \le X$.

So the proof of Proposition 5.2 will be complete if we show that the number of $\mathfrak{j}$ yielded by this construction is as large as the expression (5.1). By Landau's equidistribution theorem, given $\mathfrak{p}_1, \ldots, \mathfrak{p}_{L-1}$, the number of possibilities for $\mathfrak{p}_L$ is at least

$$(1 + o(1))\frac{x}{h_{K,\mathfrak{m}\mathfrak{g}^{-1}} N(\mathfrak{g}) \log x} \frac{1}{N(\mathfrak{p}_1 \cdots \mathfrak{p}_{L-1})},$$

as $x \to \infty$. We again sum on possible tuples $\mathfrak{p}_1, \ldots, \mathfrak{p}_{L-1}$. If we ignore the distinctness condition, then the sum on the $\mathfrak{p}_j$ is at least

$$\Big(\frac{1}{h} \log\log(X^{1/\log\log X}) + O(1)\Big)^{L-1} = (1 + o(1))\frac{1}{h^{L-1}}(\log\log x)^{L-1}.$$

But the terms with $\mathfrak{p}_j = \mathfrak{p}_{j'}$ for any pair $1 \leq j \neq j' \leq L-1$ contribute only $O((\log\log X)^{L-3})$ to the sum. Hence, we may omit the distinctness condition without changing the asymptotic formula for the sum. We divide by $(t_i - 1)! \prod_{1 \leq j \leq h,\ j \neq i} t_j!$ to avoid overcounting and conclude as in the proof of the upper bound.

Example 5.5. *Let* $K = \mathbb{Q}(\sqrt{-23})$, $\alpha = \frac{1+\sqrt{-23}}{2}$ *and* $\mathfrak{m} = (3)$. *In this case,* $\mathrm{Cl}(K) \cong \mathbb{Z}/3\mathbb{Z}$ *(so that* $h = 3$*),* $(\alpha) = \mathfrak{p}_1\mathfrak{q}_1$, *and* $(\mathfrak{m}) = \mathfrak{p}_1\mathfrak{p}_2$, *where* $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{q}_1$ *are distinct prime ideals of order* 3 *in* $\mathrm{Cl}(K)$ *of respective norms* 3, 3, *and* 2. *Hence,* $\mathfrak{g} = (\alpha, \mathfrak{m}) = \mathfrak{p}_1$. *We choose the numbering of the ideal classes* C_1, C_2, C_3 *so that* $C_1 = [\mathfrak{p}_1]$. *Then* $\mathfrak{g}$ *has type* $\tau' = (1, 0, 0)$. *There is a unique irreducible type* τ *relative to* τ', *namely* $\tau = (3, 0, 0)$. *Thus,* $\tau - \tau' = (2, 0, 0)$ *and* $L = 2$. *We have* $N(\mathfrak{g}) = N(\mathfrak{p}_1) = 3$ *and*

$$\Phi(\mathfrak{m}\mathfrak{g}^{-1}) = \Phi(\mathfrak{p}_2) = \frac{h_{K,\mathfrak{p}_2}}{h_K}.$$

Using the well-known formula for the strict ray class number appearing, for example, as Proposition 2.1 on [1, p. 50], we find that $h_{K,\mathfrak{p}_2}/h_K = 1$. *Plugging all of this into Theorem 5.1, we conclude that as* $x \to \infty$,

$$\Pi(x; (3), \frac{1}{2}(1 + \sqrt{-23})) \sim \frac{1}{27}\frac{x}{\log x}\log\log x.$$

References

[1] N. Childress. *Class field theory*. Universitext (Springer, New York, 2009).

[2] A. Geroldinger and F. Halter-Koch. *Non-unique factorizations: Algebraic, combinatorial and analytic theory*, *Pure and Applied Mathematics (Boca Raton)*, Volume 278 (Chapman & Hall/CRC, Boca Raton, FL, 2006).

[3] A. Geroldinger and I.Z. Ruzsa. *Combinatorial number theory and additive group theory*. Advanced Courses in Mathematics. CRM Barcelona (Birkhäuser Verlag, Basel, 2009).

[4] G.H. Hardy and S. Ramanujan. 'The normal number of prime factors of a number n'. *Quart. J. Math.* **48** (1917), 76–92.

[5] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers* (Oxford University Press, Oxford, 2000), 5th edn.

[6] E. Landau. 'Über Ideale und Primideale in Idealklassen'. *Math. Z.* **2** (1-2) (1918), 52–154.

[7] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics (Springer-Verlag, Berlin, 2004), 3rd edn.

[8] P. Pollack. ‘An elemental Erdős-Kac theorem for algebraic number fields’. *Proc. Amer. Math. Soc.* To appear.

[9] P. Rémond. ‘Étude asymptotique de certaines partitions dans certains semi-groupes’. *Ann. Sci. École Norm. Sup. (3)* **83** (1966), 343–410.

Paul Pollack, Department of Mathematics, Boyd Graduate Studies Research Center,
University of Georgia, Athens, GA 30602, United States
e-mail: pollack@math.uga.edu

Lee Troupe, Department of Mathematics, University of British Columbia, Vancouver,
British Columbia V6T 1Z2, Canada
e-mail: ltroupe@math.ubc.ca