EXTREMAL ELASTICITY OF QUADRATIC ORDERS

KAI (STEVE) FAN AND PAUL POLLACK

Abstract. We study how large and small elasticity can be for orders belonging to a fixed quadratic field, in terms of the corresponding conductors. For example, we show that if K is an imaginary quadratic field, then the order of conductor f in K has elasticity exceeding $(\log f)^{c_1 \log\log\log f}$ for all f that are sufficiently large. On the other hand, this elasticity is smaller than $(\log f)^{c_2 \log\log\log f}$ for infinitely many f. Here c_1, c_2 are universal positive constants. The proofs borrow methods from analytic number theory previously employed to study statistics of the multiplicative groups $(\mathbb{Z}/m\mathbb{Z})^\times$.

1. Introduction

Let R be an atomic domain, i.e., an integral domain in which every nonzero nonunit factors as a product of irreducibles. The elasticity of R, denoted $\rho(R)$, is the supremum of all ratios r/s, where r and s are positive integers for which there exists an equation

$$\pi_1 \cdots \pi_r = \rho_1 \cdots \rho_s$$

with each π_i and ρ_j irreducible in R. So for instance, every unique factorization domain (not a field) has elasticity 1. Conversely, if R is an atomic domain with elasticity 1, then R might be thought of as 'halfway' to unique factorization: any two factorizations of the same nonzero nonunit involve the same number of irreducibles, although the irreducibles themselves need not be pairwise associate. A domain of elasticity 1 is called a half-factorial domain (or HFD).

The study of half-factorial domains was initiated in a 1960 paper of Carlitz [Car60], where it is shown that the ring of integers $\mathcal{O}_K$ of the number field K is a half-factorial domain precisely when the corresponding class number $h_K = 1$ or 2. The general notion of elasticity was introduced by Valenza in a 1990 paper[1] [Val90] and further studied by Narkiewicz [Nar95] and Steffan [Ste86]. Collecting the results of these three papers, one has a complete determination of the elasticity of the ring of integers of an arbitrary number field.

For a finite abelian group G, we write $\operatorname{Dav} G$ for the Davenport constant of G, meaning the least positive integer D with the following property: Any sequence $g_1, \dots, g_D$ of elements of G possesses a nonempty subsequence multiplying to the identity.

Theorem A (Narkiewicz–Steffan–Valenza)**.** *Let R be a Dedekind domain with finite class group. Suppose that every ideal class of R is represented by at least one maximal ideal of R. Then*

$$\rho(R) = \max\left\{1, \frac{1}{2}\operatorname{Dav}\operatorname{Cl}(R)\right\},$$

where $\operatorname{Cl}(R)$ is the class group of R.

2020 *Mathematics Subject Classification.* Primary 11R27; Secondary 11N37, 11R11, 11R65, 13A05.

[1] received by the journal in 1980 !

Results of class field theory guarantee that the hypotheses of Theorem A are satisfied for any ring of S-integers in any global field. Thus, Theorem A gives a complete description of elasticities for the rings most prominent in number theory.

Of course, there are many other important rings in algebra and number theory, and there is a rich literature investigating elasticity and half-factoriality more generally. See [And97] and [CC00] for surveys. In this paper, which is a companion piece to our recent article [FP], we will be examining elasticity in orders of quadratic fields.

Let K be a quadratic field (a field extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] = 2$). An order in K is a subring of $\mathcal{O}_K$ strictly larger than $\mathbb{Z}$. The orders in K are in one-to-one correspondence with the natural numbers (positive integers) f. Each order $\mathcal{O}$ in K has the form

$$\mathcal{O}_f := \{\alpha \in \mathcal{O}_K : \alpha \equiv a \bmod f\mathcal{O}_K \text{ for some rational integer } a\}$$

for a unique $f \in \mathbb{N}$; conversely, $\mathcal{O}_f$ as defined above is always an order in K. It sometimes helpful to have a more explicit description of $\mathcal{O}_f$: It is well-known that for each quadratic field K, there is a unique squarefree integer D with $K = \mathbb{Q}(\sqrt{D})$. If we set

$$\tau_D = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \pmod 4, \\ \frac{1}{2}(1 + \sqrt{D}) & \text{if } D \equiv 1 \pmod 4, \end{cases} \tag{1}$$

then $\mathcal{O}_f = \mathbb{Z} + f\tau_D\mathbb{Z}$. We refer to $\mathcal{O}_f$ as the order of conductor f in K. Note that if $f \mid f'$, then $\mathcal{O}_{f'} \subseteq \mathcal{O}_f$, and that when $f = 1$, we have $\mathcal{O}_1 = \mathcal{O}_K$; we will refer to $\mathcal{O}_K$ as the maximal order in K. For more on the basic theory of quadratic orders, see the lovely book of Cox [Cox22] (p. 105 and following).

It was noted by Zaks [Zak76, Zak80] that $\mathbb{Z}[\sqrt{-3}]$, the order of conductor 2 in $K = \mathbb{Q}(\sqrt{-3})$, is a half-factorial domain. However, half-factorial quadratic orders were not systematically studied until the later work of Coykendall [Coy01] and Halter-Koch [HK83]. (This latter paper of Halter-Koch is not easy to come by; a more readily-available source for this material is [GHK06]; see p. 226 and following.) These papers contain a complete algebraic characterization of half-factorial quadratic orders.

The characterization in the imaginary case is surprisingly simple: $\mathbb{Z}[\sqrt{-3}]$ is the unique nonmaximal half-factorial quadratic order [Coy01, Theorem 2.3]. (Recall that maximal orders fall under the purview of Carlitz's 1960 theorem, so we may always restrict to the nonmaximal case.) The real case is substantially more complicated. Here there are various ways to state the characterization, some more explicit than others; the version we quote below is based on Coykendall's paper [Coy01] and a subsequent manuscript of Coykendall–Malcolmson–Okoh [CMO17].

Theorem B. *Let $\mathcal{O}$ be the order of conductor f in the real quadratic field K. In order for $\mathcal{O}$ to be half-factorial, it is necessary that*

(i) *$\mathcal{O}_K$ be half-factorial (equivalently, $h_K = 1$ or $h_K = 2$),* and

(ii) *$f = p$ or $f = 2p$, where p is a prime inert in K; if $f = 2p$, we require $p > 2$ and both 2 and p to be inert in K.*

Conversely, suppose $\mathcal{O}_K$ is half-factorial and $f = p$ is a prime inert in K. Let ϵ be the fundamental unit of K.[2] *Then*

$$\mathcal{O} \text{ is half-factorial} \iff \epsilon \text{ generates } (\mathcal{O}_K/f\mathcal{O}_K)^\times/\langle \text{images of integers prime to } f\rangle.$$

Finally, if $f = 2p$, where 2 and p are distinct primes inert in K, then

$$\mathcal{O} \text{ is half-factorial} \iff 3 \nmid p+1, \text{ and both } \mathcal{O}_2, \mathcal{O}_p \text{ are half-factorial.}$$

From the algebraic standpoint, there is no room for improvement in Theorem B; the stated conditions are both necessary and sufficient. But the statistical question of how often half-factorial orders appear "in the wild" is far from settled. For this, one must study how often the conditions of Theorem B are satisfied; this is an analytic problem rather than a purely algebraic one. In [Coy01], Coykendall posed two conjectures in this direction:

(A) Varying both the quadratic field K and the natural number f, one encounters infinitely many half-factorial quadratic orders $\mathcal{O}_f$.

(B) Fix the field $K = \mathbb{Q}(\sqrt{2})$. Then $\mathcal{O}_f$ is a half-factorial domain for infinitely many $f \in \mathbb{N}$.

Coykendall's conjectures were recently studied by the second author (P.P.) in [Pol24]. The weaker Conjecture A is proved in full, while the stronger Conjecture B is demonstrated under the assumption of the Generalized Riemann Hypothesis (GRH).[3] The methods of [Pol24] were extended in [Pol25] to obtain various related results. Here is a sample.

Theorem C. *Let $\mathcal{E} = \{1, \frac{3}{2}, 2, \frac{5}{2}, 3, \frac{7}{2}, \dots\} \cup \{\infty\}$.*

(i) *If K is any quadratic order, then $\rho(\mathcal{O}) \in \mathcal{E}$.*

(ii) *Under GRH, each element of $\mathcal{E}$ is the elasticity of infinitely many many distinct orders in $\mathbb{Q}(\sqrt{2})$.*

In both [Pol24, Pol25], the goal is to realize a prescribed elasticity, and the conductors f are constructed accordingly. It is natural to ask what elasticities one sees if instead of constructing f towards a predetermined end, one samples f "at random" and records the results. This question was recently considered by the present authors in [FP].

It requires some care to settle on the right notion of "at random." Let K be a quadratic field, and let $\mathcal{O}$ be the order of conductor f in K. It follows from a general theorem of Halter-Koch (see [HK95, Corollary 4]) that $\rho(\mathcal{O}) = \infty$ if and only if f is divisible by a prime p that splits (completely) in K. For a given K, the Chebotarev density theorem guarantees that asymptotically half of all primes p split in K. It follows that asymptotically 100% of natural numbers f have at least one split prime factor, and so $\rho(\mathcal{O}_f) = \infty$ asymptotically 100% of the time. Thus, if we fix a quadratic field K, the natural problem is to study the distribution of $\rho(\mathcal{O}_f)$ with f sampled uniformly from (only) split-free integers, meaning integers possessing no split prime factors. This is precisely what we do in [FP].

[2]While not important here, we mention for later: We always view quadratic fields as embedded in $\mathbb{C}$. If $K = \mathbb{Q}(\sqrt{D})$ is real-quadratic, we assume $\sqrt{D} > 0$, and that the fundamental unit ϵ is normalized to satisfy $\epsilon > 1$.

[3]Throughout, by GRH we mean the assertion that all nontrivial zeros of all number field zeta functions lie on the line $\Re(s) = \frac{1}{2}$.

Theorem D. *Let K be a fixed imaginary quadratic field. Let Δ_K denote the discriminant of K. For almost all split-free numbers f,*

$$\rho(\mathcal{O}_f) = f/(\log f)^{\frac{1}{2}\log_3 f + \frac{1}{2}C_K + O((\log_4 f)^3/\log_3 f)},$$

where $\log_k$ denotes the kth iterate of the natural logarithm, and

$$C_K := \sum_{p>2} \frac{\log p}{(p-1)^2} - 1 - \frac{\operatorname{sgn}(\Delta_K) 1_{\mathcal{D}}(\Delta_K) |\Delta_K| \log \operatorname{Rad}(|\Delta_K|)}{\varphi(|\Delta_K|)^2}.$$

Here $\operatorname{Rad}(|\Delta_K|)$ is the product of the distinct primes dividing Δ_K, and $1_{\mathcal{D}}$ is the characteristic function of the set of prime discriminants

$$\mathcal{D} := \{-4, \pm 8\} \cup \left\{(-1)^{\frac{p-1}{2}} p \colon p > 2 \text{ is prime}\right\}.$$

Theorem E (conditional on GRH)**.** *Let K be a fixed real quadratic field. For almost all split-free numbers f,*

$$\rho(\mathcal{O}_f) = (\log f)^{\frac{1}{2} + O(1/\log_4 f)}.$$

In these theorems, almost all means that the proportion of split-free numbers up to x for which the estimate fails tends to 0, as $x \to \infty$. We remind the reader that $A = O(B)$ means $|A| \le C|B|$ for some implied constant C. In these results, as well as all the theorems appearing below, implied constants may depend on the field K.

In this paper, we continue our investigations into the distribution of elasticities of orders belonging to a fixed quadratic field. However, instead of looking for the typical size of $\rho(\mathcal{O}_f)$, we inquire into the extremal behavior. How large and how small can $\rho(\mathcal{O}_f)$ get, in terms of f?

The following are our principal results. Below, $A \ll B$ is synonymous with $A = O(B)$. That is, $|A| \le C|B|$, for a constant C that may depend on K. The notation "$A \gg B$" indicates that $B \ll A$.

Theorem 1.1 (Maximal order, imaginary case)**.** *Let K be a fixed imaginary quadratic field. Then $\rho(\mathcal{O}_f) \ll f$ for all split-free numbers f. Conversely, if p is a prime inert or ramified in K, then $\rho(\mathcal{O}_p) \gg p$.*

Theorem 1.2 (Minimal order, imaginary case)**.** *There are universal positive constants c_1, c_2, and f_0 for which the following holds: Let K be a fixed imaginary quadratic field. For all split-free numbers $f > f_0$, we have*

$$\rho(\mathcal{O}_f) > (\log f)^{c_1 \log\log\log f}. \tag{2}$$

On the other hand, there is a sequence of split-free numbers f tending to infinity along which

$$\rho(\mathcal{O}_f) < (\log f)^{c_2 \log\log\log f}. \tag{3}$$

Theorem 1.3 (Maximal order, real case)**.** *Let K be a real quadratic field. Then*

$$\rho(\mathcal{O}_f) \ll f/\log f$$

for all split-free $f > 1$. In the opposite direction, GRH implies that for every $\epsilon > 0$, there are infinitely many primes p, inert in K, with

$$\rho(\mathcal{O}_p) > p^{\frac{1}{4} - \epsilon}. \tag{4}$$

Theorem 1.4 (Minimal order, real case)**.** *Assume GRH. For every real quadratic field K, there is a constant C_K with the property that $\rho(\mathcal{O}_f) < C_K$ for infinitely many split-free numbers f.*

The reader will have noticed the large gap between the (rigorous) upper bound in Theorem 1.3 and the (GRH-conditional) lower bound. As we indicate in a remark following the proof, we believe the upper bound is sharp; in fact, we conjecture that there are infinitely many primes p, inert in K, with $\rho(\mathcal{O}_p) \gg p/\log p$.

2. The class group, its principal part, and the pre-class group

In this section we set up machinery from [FP] that will play an important role in our proofs.

Let K be a quadratic field. For each natural number f, we let $I_K(f)$ denote the group of fractional ideals of K generated by the nonzero ideals of $\mathcal{O}_K$ comaximal with $f\mathcal{O}_K$. We write $P_{K,\mathbb{Z}}(f)$ for the subgroup of $I_K(f)$ generated by principal ideals $\alpha\mathbb{Z}_K$, where $\alpha \in \mathcal{O}_K$ satisfies $\alpha \equiv a \pmod{f\mathcal{O}_K}$ for an integer a coprime to f. The class group $\mathrm{Cl}(\mathcal{O}_f)$ is defined as the quotient $I_K(f)/P_{K,\mathbb{Z}}(f)$. Note that when $f = 1$, our definition recovers the usual definition of the class group of $\mathcal{O}_K = \mathcal{O}_1$.

The next result, which appears as [FP, Lemma 2.1], is a variant of Theorem A for quadratic orders.

Proposition 2.1. *Let K be a quadratic field. For each split-free $f \in \mathbb{N}$,*

$$\frac{1}{2}\operatorname{Dav}\mathrm{Cl}(\mathcal{O}_f) \le \rho(\mathcal{O}_f) \le \max\left\{1, \frac{1}{2}\operatorname{Dav}\mathrm{Cl}(\mathcal{O}_f) + \frac{3}{2}\Omega(f)\right\}.$$

(Here $\Omega(\cdot)$ counts the total number of prime factors, with multiplicity; e.g., $\Omega(-12) = \Omega(30) = 3$.) Proposition 2.1 is not as precise as Theorem A; except in the case $f = 1$, it does not determine the exact value of $\rho(\mathcal{O}_f)$. Nevertheless, it will suffice to obtain our statistical results.

In order to access $\operatorname{Dav}\mathrm{Cl}(\mathcal{O}_f)$, we find it helpful to "pull apart" the class group. We define the principal part of the class group, denoted $\mathrm{PrinCl}(\mathcal{O}_f)$, by

$$\mathrm{PrinCl}(\mathcal{O}_f) := (\mathcal{O}_K/f\mathcal{O}_K)^\times/\langle\text{images of integers prime to } f, \text{ units of } \mathcal{O}_K\rangle.$$

Write P_K for $P_{K,\mathbb{Z}}(1)$ (the group of principal fractional ideals). The exact sequence

$$(\mathbb{Z}/f\mathbb{Z})^\times \times \mathcal{O}_K^\times \xrightarrow{\mu} (\mathcal{O}_K/f\mathcal{O}_K)^\times \xrightarrow{\iota} (I_K(f)\cap P_K)/P_{K,\mathbb{Z}}(f) \longrightarrow 1$$

allows us to identify $\mathrm{PrinCl}(\mathcal{O}_f)$ with the subgroup $(I_K(f)\cap P_K)/P_{K,\mathbb{Z}}(f)$ of $\mathrm{Cl}(\mathcal{O}_f)$; here μ and ι are the maps defined by

$$\mu((a \bmod f, \eta)) := a\eta \bmod f\mathcal{O}_K \quad \text{and} \quad \iota(\alpha \bmod f\mathcal{O}_K) = [\alpha\mathcal{O}_K].$$

This identification explains the term "principal part of the class group."

With the obvious maps, there is a short exact sequence

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (I_K(f)\cap P_K)/P_{K,\mathbb{Z}}(f) & \longrightarrow & I_K(f)/P_{K,\mathbb{Z}}(f) & \longrightarrow & I_K/P_K & \longrightarrow & 1. \\ & & \| \wr & & \| & & \| & & \\ & & \mathrm{PrinCl}(\mathcal{O}_f) & & \mathrm{Cl}(\mathcal{O}_f) & & \mathrm{Cl}(\mathcal{O}_K) & & \end{array}$$

(Exactness at the last position is not obvious; for this one uses that each ideal class in $\mathcal{O}_K$ has a representative comaximal with $f\mathcal{O}_K$.) Thus, we may view $\mathrm{PrinCl}(\mathcal{O}_f)$ as a subgroup of $\mathrm{Cl}(\mathcal{O}_f)$ for which

$$[\mathrm{Cl}(\mathcal{O}_f) : \mathrm{PrinCl}(\mathcal{O}_f)] = \#\mathrm{Cl}(\mathcal{O}_K) = h_K. \tag{5}$$

To apply Proposition 2.1 requires knowledge of $\operatorname{Dav}\operatorname{Cl}(\mathcal{O}_f)$. Equation (5) is helpful here; it implies that

$$\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) \le \operatorname{Dav}\operatorname{Cl}(\mathcal{O}_f) \le h_K \operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f). \tag{6}$$

(See [FP, Lemma 2.4].) In our results, an ambiguity up to a factor depending on K is acceptable, and (6) allows us to always work with $\operatorname{PrinCl}(\mathcal{O}_f)$ rather than $\operatorname{Cl}(\mathcal{O}_f)$.

We will understand $\operatorname{PrinCl}(\mathcal{O}_f)$ by viewing it as arising from a two-stage construction. First, we quotient $(\mathcal{O}_K/f\mathcal{O}_K)^\times$ (only) by the image of the integers prime to f; we call this is the pre-class group. That is,

$$\operatorname{PreCl}(\mathcal{O}_f) := (\mathcal{O}_K/f\mathcal{O}_K)^\times/\langle \text{images of integers prime to } f\rangle.$$

(The observant reader will have noticed that this group appeared already in Theorem B.) Second, we take the quotient of $\operatorname{PreCl}(\mathcal{O}_f)$ by the image $\mathcal{U}_f$ of $\mathcal{O}_K^\times$ in $\operatorname{PreCl}(\mathcal{O}_f)$; then $\operatorname{PreCl}(\mathcal{O}_f)/\mathcal{U}_f \cong \operatorname{PrinCl}(\mathcal{O}_f)$.

It is productive to view these pre-class groups $\operatorname{PreCl}(\mathcal{O}_f)$ as close cousins of the unit groups $(\mathbb{Z}/m\mathbb{Z})^\times$; this principle is exploited heavily in [FP] (and implicitly in [Pol24, Pol25]). Let $\psi(f) := \#\operatorname{PreCl}(\mathcal{O}_f)$. By the Chinese remainder theorem,

$$\operatorname{PreCl}(\mathcal{O}_f) \cong \prod_{p^k \| f} \operatorname{PreCl}(\mathcal{O}_{p^k}). \tag{7}$$

Thus, ψ is a multiplicative function of f. Furthermore, since the $\varphi(p^k)$ integers in $[1, p^k]$ that are prime to p^k have distinct images in $\mathcal{O}_K/p^k\mathcal{O}_K$,

$$\psi(p^k) = \frac{1}{\varphi(p^k)}(\#\mathcal{O}_K/p^k\mathcal{O}_K)^\times = \frac{1}{p^{k-1}(p-1)}(\#\mathcal{O}_K/p^k\mathcal{O}_K)^\times.$$

Now $\#(\mathcal{O}_K/p^k\mathcal{O}_K)^\times = N(p^k\mathcal{O}_K)\prod_{P|p}\left(1-\frac{1}{N(P)}\right) = p^{2k}\prod_{P|p}\left(1-\frac{1}{N(P)}\right)$. Plugging the result of this formula into the last display, considering separately the cases when p is ramified, split, or inert, we find after a short calculation that

$$\psi(p^k) = p^k - \left(\frac{\Delta_K}{p}\right)p^{k-1} = p^k\left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right),$$

where $\left(\frac{\cdot}{\cdot}\right)$ is the Kronecker symbol. Hence,

$$\psi(f) = f\prod_{p|f}\left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right),$$

in close analogy with the familiar formula $\varphi(f) = f\prod_{p|f}(1-\frac{1}{p})$ for Euler's φ-function.

The groups $\operatorname{PreCl}(\mathcal{O}_f)$ mirror $(\mathbb{Z}/m\mathbb{Z})^\times$ not only in their size but also in their structure. For instance, we have the following result.

Lemma 2.2. *Let K be a quadratic field, and let p be a rational prime with $p > 3$. Then $\operatorname{Cl}(\mathcal{O}_{p^k})$ is cyclic for each natural number k.*

Lemma 2.2 is an analogue of Gauss's classical theorem that $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic for each prime power p^k with $p > 2$.

Proof of Lemma 2.2. In the case where the prime $p > 3$ is ramified or inert in K, this result appears as Lemma 2.5 of [FP], where it is deduced from related structure theorems of Halter-Koch [HK72]. Suppose now that p is split, say $p\mathcal{O}_K = P_1P_2$ with the P_i distinct maximal ideals of $\mathcal{O}_K$. Then $\mathcal{O}_K/p^k\mathcal{O}_K \cong \mathcal{O}_K/P_1^k \times \mathcal{O}_K/P_2^k$, and each $\mathcal{O}_K/P_i^k \cong \mathbb{Z}/p^k\mathbb{Z}$. Furthermore,

$$\begin{aligned}\mathrm{PreCl}(\mathcal{O}_{p^k}) &= (\mathcal{O}_K/p^k\mathcal{O}_K)^\times/\langle\text{images of integers prime to } p^k\rangle \\ &\cong \frac{(\mathbb{Z}/p^k\mathbb{Z})^\times \times (\mathbb{Z}/p^k\mathbb{Z})^\times}{(\mathbb{Z}/p^k\mathbb{Z})^\times} \\ &\cong (\mathbb{Z}/p^k\mathbb{Z})^\times;\end{aligned}$$

here the $(\mathbb{Z}/p^k\mathbb{Z})^\times$ in the "denominator" of the second line is viewed as a subgroup of the "numerator" via the diagonal embedding. By the theorem of Gauss quoted above, $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic, and hence $\mathrm{PreCl}(\mathcal{O}_{p^k})$ is as well. □

It is clear from the isomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \cong \prod_{p^k \| m}(\mathbb{Z}/p^k\mathbb{Z})^\times$ that the exponent $\mathrm{Exp}\,(\mathbb{Z}/m\mathbb{Z})^\times$ is a divisor of $\mathrm{lcm}\{\varphi(p^k) : p^k \parallel m\}$, and Gauss showed in his *Disquisitiones* that the corresponding quotient is always 1 or 2. Our proof of Theorem 1.2 requires the following variant for pre-class groups. Put

$$L(f) := \mathrm{lcm}\{\psi(p^k) : p^k \parallel f\}. \tag{8}$$

Proposition 2.3. *For all natural numbers f,*

$$\mathrm{Exp}\,\mathrm{PreCl}(\mathcal{O}_f) \mid L(f) \mid 12\,\mathrm{Exp}\,\mathrm{PreCl}(\mathcal{O}_f).$$

It follows from Proposition 2.3 that $L(f)/\,\mathrm{Exp}\,\mathrm{PreCl}(\mathcal{O}_f) \in \{1, 2, 3, 4, 6, 12\}$.

Proof. The first divisibility is clear from the isomorphism (7), keeping in mind that $\#\mathrm{PreCl}(\mathcal{O}_{p^k}) = \psi(p^k)$. To prove the second, it suffices to show that

$$\psi(p^k) \mid 12\,\mathrm{Exp}\,\mathrm{PreCl}(\mathcal{O}_{p^k}) \quad \text{for each prime power } p^k,$$

for then

$$\begin{aligned}L(f) \mid \mathrm{lcm}\{12\,\mathrm{Exp}\,\mathrm{PreCl}(\mathcal{O}_{p^k}) : p^k \parallel f\} &= 12\,\mathrm{lcm}\{\mathrm{Exp}\,\mathrm{PreCl}(\mathcal{O}_{p^k}) : p^k \parallel f\} \\ &= 12\,\mathrm{Exp}\,\mathrm{PreCl}(\mathcal{O}_f),\end{aligned}$$

as desired.

When $p > 3$, we have $\psi(p^k) = \mathrm{Exp}\,\mathrm{PreCl}(\mathcal{O}_{p^k})$ (Lemma 2.2). So we may assume $p = 2$ or $p = 3$.

Suppose first that $p = 2$. Since $\psi(2^k) = (2 - \left(\frac{\Delta_K}{2}\right))2^{k-1} \mid 12$ when $k \in \{1, 2\}$, we may assume that $k \geq 3$. Let $\alpha = 1 + 2\sqrt{D}$, where D is the squarefree integer with $K = \mathbb{Q}(\sqrt{D})$. A straightforward induction shows that, for each integer $j \geq 0$,

$$\alpha^{2^j} = u_j + v_j\sqrt{D}$$

for integers u_j, v_j with u_j odd and $2^{j+1} \parallel v_j$. In particular, $\alpha^{2^{k-1}} \in \mathbb{Z}[2^k\sqrt{D}] \subseteq \mathcal{O}_{2^k}$. Since $\alpha\mathcal{O}_K$ and $2\mathcal{O}_K$ are comaximal, we conclude that α represents an element of $\mathrm{PreCl}(\mathcal{O}_{2^k})$ of order e (say) with

$$e \mid 2^{k-1}.$$

On the other hand,

$$2\alpha^{2^{k-3}} = 2u_{k-3} + 2v_{k-3}\sqrt{D} \notin \mathbb{Z}[2^k\sqrt{D}].$$

As $2\mathcal{O}_{2^k} \subseteq \mathbb{Z}[2^k\sqrt{D}]$, it must be that $\alpha^{2^{k-3}} \notin \mathcal{O}_{2^k}$. Thus,

$$e \nmid 2^{k-3}.$$

Combining the last two displays, we find that $e = 2^{k-2}$ or $e = 2^{k-1}$. Hence,

$$\psi(2^k) = (2 - \left(\tfrac{\Delta_K}{2}\right))2^{k-1} \mid 12 \cdot 2^{k-2} \mid 12e \mid 12 \operatorname{Exp} \operatorname{PreCl}(\mathcal{O}_{2^k}).$$

The proof when $p = 3$ is similar, and we condense the details. Since $\psi(3^k) = (3 - \left(\tfrac{\Delta_K}{3}\right))3^{k-1} \mid 12$ when $k = 1$, we can assume that $k \geq 2$. In this case, one takes $\alpha' = 1 + 3\sqrt{D}$ and shows by induction that for each integer $j \geq 0$,

$$\alpha'^{3^j} = u'_j + v'_j\sqrt{D}$$

with integers u'_j, v'_j for which $3 \nmid u'_j$, $3^{j+1} \parallel v'_j$. Then $\alpha'^{3^{k-1}} \in \mathcal{O}_{3^k}$ while $\alpha'^{3^{k-2}} \notin \mathcal{O}_{3^k}$. It follows that α' represents an element in $\operatorname{PreCl}(\mathcal{O}_{3^k})$ of exact order 3^{k-1}. Hence,

$$\psi(3^k) = (3 - \left(\tfrac{\Delta_K}{3}\right))3^{k-1} \mid 12 \cdot 3^{k-1} \mid 12 \operatorname{Exp} \operatorname{PreCl}(\mathcal{O}_{3^k}),$$

as desired. □

We saw above that $\operatorname{PrinCl}(\mathcal{O}_f) \cong \operatorname{PreCl}(\mathcal{O}_f)/\mathcal{U}_f$, where $\mathcal{U}_f$ is the image of $\mathcal{O}_K^\times$ inside $\operatorname{PreCl}(\mathcal{O}_f)$. Hence, setting

$$\ell(f) := \#\mathcal{U}_f,$$

we have that

$$\#\operatorname{PrinCl}(\mathcal{O}_f) = \frac{\psi(f)}{\ell(f)}.$$

We finish this section by recording two observations about $\mathcal{U}_f$ that will be relevant in the sequel:

(i) When K is imaginary quadratic, $\ell(f) \leq \#\mathcal{O}_K^\times \leq 6$. Moreover, $\mathcal{U}_f$ is cyclic, generated by (the image of) a primitive $\#\mathcal{O}_K^\times$-th root of unity.

(ii) When K is real, $\mathcal{O}_K^\times$ is generated by ± 1 and the fundamental ϵ. Since -1 projects to the identity in $\operatorname{PreCl}(\mathcal{O}_f)$, it follows that $\mathcal{U}_f$ is cyclic in this case as well, generated by the image of ϵ in $\operatorname{PreCl}(\mathcal{O}_f)$. Furthermore,

$$\ell(f) \text{ is the least integer } \ell \text{ with } \epsilon^\ell \in \mathcal{O}_f.$$

3. Maximal order in the imaginary case: Proof of Theorem 1.1

3.1. **Upper bound.** We start by showing that $\rho(\mathcal{O}_f) \ll f$ for each split-free f. We may (and will) assume that $f > 1$. By Proposition 2.1, for each split-free number $f > 1$,

$$\rho(\mathcal{O}_f) \leq \frac{1}{2} \operatorname{Dav} \operatorname{Cl}(\mathcal{O}_f) + \frac{3}{2}\Omega(f).$$

Clearly,

$$2^{\Omega(f)} = \prod_{p^k \parallel f} 2^k \leq \prod_{p^k \parallel f} p^k = f, \quad \text{so that} \quad \Omega(f) \ll \log f,$$

and $\log f \ll f$. Furthermore, we have from (6) that

$$\operatorname{Dav} \operatorname{Cl}(\mathcal{O}_f) \leq h_K \operatorname{Dav} \operatorname{PrinCl}(\mathcal{O}_f).$$

It therefore suffices to show that $\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) \ll f$. This is an immediate consequence of the following result, which will also be needed later for real K.

Proposition 3.1. *Let K be any quadratic field. For every natural number f,*

$$\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) \ll \frac{f}{\ell(f)}. \tag{9}$$

The main ingredient in the proof of Proposition 3.1 is an elegant result of Van Emde Boas and Kruyswijk [vEBK67] which bounds from above the Davenport constant of a finite abelian group G in terms of $\operatorname{Exp} G$.

Proposition 3.2. *Let G be a finite abelian group, and put*

$$r(G) = \frac{\#G}{\operatorname{Exp} G}.$$

Then

$$\operatorname{Dav} G \leq \#G \left(\frac{1 + \log r(G)}{r(G)} \right).$$

The function $t \mapsto \frac{1+\log t}{t}$ is decreasing on the domain $t \geq 1$, with maximum value 1. Thus, $D(G) \leq \#G$ always, with strict inequality whenever $r(G) > 1$ (that is, whenever G is not cyclic).

In order for Proposition 3.2 to be of use in the proof of (9), we need a handle on $r(\operatorname{PrinCl}(\mathcal{O}_f))$. This will be given to us by the next lemma. Below, we write $\operatorname{rk}_2 G$ for the 2-rank of G.

Lemma 3.3. *For every finite abelian group G,*

$$\exp G \mid 2^{1-\operatorname{rk}_2 G} \#G.$$

Hence,

$$r(G) \geq 2^{\operatorname{rk}_2 G - 1}.$$

Proof. The second claim is immediate from the first, so we focus on that.

If $\operatorname{rk}_2 G \leq 1$, the asserted divisibility is trivial, so we assume $\operatorname{rk}_2 G > 1$. We may also assume $G = A \oplus \mathbb{Z}/2^{r_1}\mathbb{Z} \oplus \mathbb{Z}/2^{r_2}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/2^{r_l}\mathbb{Z}$, where $l = \operatorname{rk}_2 G$, the r_i satisfy $1 \leq r_1 \leq r_2 \leq \cdots \leq r_l$, and A has odd order. Then

$$\operatorname{Exp} G \mid 2^{r_l} \#A = 2^{1-l} \cdot 2^{(l-1)+r_l} \#A \mid 2^{1-l} \cdot 2^{r_1+r_2+\cdots+r_{l-1}+r_\ell} \#A = 2^{1-l} \#G. \qquad \square$$

Proof of Proposition 3.1. Let w denote the number of (distinct) odd primes p dividing f which are inert in K. We will bound $\operatorname{rk}_2 \operatorname{PrinCl}(\mathcal{O}_f)$ below in terms of w and then apply Lemma 3.3.

If $p^k \parallel f$ with p odd and inert in K, then $\#\operatorname{PreCl}(\mathcal{O}_{p^k}) = \psi(p^k) = p^k + p^{k-1}$ is even. Hence, $\operatorname{rk}_2 \operatorname{PreCl}(\mathcal{O}_{p^k}) \geq 1$, and

$$\operatorname{rk}_2 \operatorname{PreCl}(\mathcal{O}_f) = \sum_{p^k \parallel f} \operatorname{rk}_2 \operatorname{PreCl}(\mathcal{O}_{p^k}) \geq w.$$

As $\mathcal{U}_f$ is cyclic, $\operatorname{rk}_2 \mathcal{U}_f \leq 1$, and

$$\operatorname{rk}_2 \operatorname{PrinCl}(\mathcal{O}_f) = \operatorname{rk}_2 \frac{\operatorname{PreCl}(\mathcal{O}_f)}{\mathcal{U}_f} \geq \operatorname{rk}_2 \operatorname{PreCl}(\mathcal{O}_f) - \operatorname{rk}_2 \mathcal{U}_f \geq w - 1.$$

Thus, by Lemma 3.3,

$$r := r(\mathrm{PrinCl}(\mathcal{O}_f)) \geq 2^{w-2}.$$

Suppose that $w \geq 2$. Then $r \geq 2^{w-2} \geq 1$, and Proposition 3.2 yields

$$\mathrm{Dav}\,\mathrm{PrinCl}(\mathcal{O}_f) \leq \frac{\psi(f)}{\ell(f)} \frac{1+\log r}{r} \leq \frac{\psi(f)}{\ell(f)} \frac{1+\log 2^{w-2}}{2^{w-2}} < \frac{4w}{2^w} \cdot \frac{\psi(f)}{\ell(f)}.$$

As f is split-free, we have $\omega(f) \leq w + 1 + \omega(\Delta_K)$. (Per the usual convention in analytic number theory, we write $\omega(\cdot)$ for the count of distinct prime factors.) Therefore,

$$\psi(f) \leq f \prod_{p \mid f} \left(1 + \frac{1}{p}\right) \leq (3/2)^{\omega(f)} f \leq (3/2)^{w+1+\omega(\Delta_K)} f.$$

and

$$\mathrm{Dav}\,\mathrm{PrinCl}(\mathcal{O}_f) < \frac{4w}{2^w} \frac{\psi(f)}{\ell(f)} \leq (3/2)^{1+\omega(\Delta_K)} (4w(3/4)^w) \frac{f}{\ell(f)}.$$

In this last expression, the coefficient of $f/\ell(f)$ is bounded by a constant depending only K, establishing (9) when $w \geq 2$.

If $w \leq 1$, the argument is easier. In this case, $\omega(f) \leq 2 + \omega(\Delta_K)$, and

$$\begin{aligned} \mathrm{Dav}\,\mathrm{PrinCl}(\mathcal{O}_f) \leq \#\mathrm{PrinCl}(\mathcal{O}_f) &= \frac{\psi(f)}{\ell(f)} \\ &= \frac{f}{\ell(f)} \prod_{p \mid f} \left(1 - \frac{1}{p}\left(\frac{\Delta_K}{p}\right)\right) \leq (3/2)^{\omega(f)} \frac{f}{\ell(f)} \ll \frac{f}{\ell(f)}, \end{aligned}$$

as desired. □

3.2. **Lower bound.** We turn now to the (much simpler) proof that $\rho(\mathcal{O}_p) \gg p$ for all p that do not split completely in K. If $p = 2$ or $p = 3$, then $\rho(\mathcal{O}_p) \geq 1 \geq \frac{1}{3}p$, so we suppose that $p > 3$. By Proposition 2.1 and (6),

$$\rho(\mathcal{O}_p) \geq \frac{1}{2} \mathrm{Dav}\,\mathrm{PrinCl}(\mathcal{O}_p).$$

The group $\mathrm{PrinCl}(\mathcal{O}_p)$ is cyclic, as a quotient of the cyclic group $\mathrm{PreCl}(\mathcal{O}_p)$ (see Lemma 2.2). Whenever G is cyclic, $\mathrm{Dav}\, G = \#G$ (see, e.g., Lemma 1.4.9 on p. 27 of [GHK06].) Thus, $\mathrm{Dav}\,\mathrm{PrinCl}(\mathcal{O}_p) = \#\mathrm{PrinCl}(\mathcal{O}_p) = \psi(p)/\ell(p)$, and we conclude that

$$\rho(\mathcal{O}_p) \geq \frac{\psi(p)}{2\ell(p)}. \tag{10}$$

Up to this point all of our reasoning has been valid whether K is real or imaginary. But if we assume K is imaginary, then $\ell(p) \leq \#\mathcal{O}_K^\times \leq 6$, leading to the conclusion that

$$\rho(\mathcal{O}_p) \geq \frac{\psi(p)}{12} = \frac{p - \left(\frac{\Delta_K}{p}\right)}{12} \geq \frac{p}{12}$$

for all non-split $p > 3$. This establishes the lower bound claimed in Theorem 1.1. In fact, we have shown that the implied constant there can be taken as $\frac{1}{12}$, independently of K.

4. Minimal order in the imaginary case: Proof of Theorem 1.2

Our proof of Theorem 1.2 is based on arguments of Erdős, Pomerance, and Schmutz [EPS91] used to estimate the minimal order of Carmichael's lambda function $\lambda(m) := \#\operatorname{Exp}(\mathbb{Z}/m\mathbb{Z})^\times$. According to the first half of Theorem 1 of [EPS91], we have

$$\lambda(m) > (\log m)^{(\frac{1}{\log 2}+o(1))\log\log\log m}$$

whenever $m \to \infty$. (As usual in analytic number theory, $o(1)$ denotes a quantity tending to 0.) The second half of that theorem asserts the existence of a strictly increasing sequence of natural numbers $\{m_i\}_{i\geq 1}$ such that

$$\lambda(m_i) < (\log m_i)^{c_0 \log\log\log m_i}$$

for all $i \geq 1$.

We need an $L(f)$-analogue of the quoted results, where $L(f)$ is the function defined in (8).

Proposition 4.1. *Let K be a quadratic field. For any sequence of natural numbers $f \to \infty$,*

$$L(f) > (\log f)^{(\frac{1}{\log 2}+o(1))\log\log\log f},$$

uniformly in K. On the other hand, for some universal constant $c_0 > 0$, and each fixed choice of K, there is a strictly increasing sequence $\{f_i\}_{i\geq 1}$ of positive integers, each of which is a product of distinct primes inert in K, such that

$$L(f_i) < (\log f_i)^{c_0 \log\log\log f_i}$$

for all $i \geq 1$.

Taking Proposition 4.1 as shown, we can quickly conclude the proof of Theorem 1.2. We start with the lower bound (2). From Proposition 2.1 and (6), $\rho(\mathcal{O}_f) \geq \frac{1}{2}\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f)$. As $\operatorname{PrinCl}(\mathcal{O}_f)$ is the quotient of $\operatorname{PreCl}(\mathcal{O}_f)$ by the subgroup $\mathcal{U}_f$ of order $\#\mathcal{U}_f \leq \#\mathcal{O}_K^\times \leq 6$, we have $\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) \geq \frac{1}{6}\operatorname{Dav}\operatorname{PreCl}(\mathcal{O}_f)$ (see [FP, Lemma 2.4]). Therefore,

$$\rho(\mathcal{O}_f) \geq \frac{1}{12}\operatorname{Dav}\operatorname{PreCl}(\mathcal{O}_f) \geq \frac{1}{12}\operatorname{Exp}\operatorname{PreCl}(\mathcal{O}_f) \geq \frac{1}{12^2}L(f),$$

invoking Proposition 2.3 at the last step. The lower bound of Proposition 4.1 thus implies that (2) holds for any constant $c_1 < 1/\log 2$.

The upper bound (3) is slightly more intricate. From Proposition 2.1, (6), and the bound $\Omega(f) \ll \log f$, we have

$$\rho(\mathcal{O}_f) \ll \operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) + \log f \tag{11}$$

for all split-free f. Applying the Van Emde Boas–Kruyswijk exponent bound (Proposition 3.2),

$$\begin{aligned}\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) &\leq \operatorname{Exp}\operatorname{PrinCl}(\mathcal{O}_f)\left(1+\log\frac{\#\operatorname{PrinCl}(\mathcal{O}_f)}{\operatorname{Exp}\operatorname{PrinCl}(\mathcal{O}_f)}\right)\\ &\leq \operatorname{Exp}\operatorname{PrinCl}(\mathcal{O}_f)(1+\log\psi(f)).\end{aligned}$$

Now $\psi(f) \leq (3/2)^{\omega(f)}f$, so that

$$\log\psi(f) \leq \omega(f)\log\frac{3}{2} + \log f \leq \Omega(f)\log\frac{3}{2} + \log f \ll \log f.$$

We conclude that for all split-free f,

$$\begin{aligned} \operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) &\ll \operatorname{Exp}\operatorname{PrinCl}(\mathcal{O}_f)(1+\log f) \\ &\le L(f)(1+\log f). \end{aligned} \tag{12}$$

The upper bound half of Theorem 1.2 now follows from (11), (12), and the upper bound result of Proposition 4.1. Indeed, fixing any $c_2 > c_0$, we find that (3) holds for all large enough f (large enough in terms of K) from the sequence $\{f_i\}$.

The remainder of this section is devoted to the proof of Proposition 4.1. We make little claim to originality here; our arguments are straightforward adaptations of those in [EPS91].

4.1. **The lower bound in Proposition 4.1.** We start by observing that $L(f) \to \infty$ whenever $f \to \infty$. Indeed, if $L(f) \le B$ for some constant $B > 0$, then $p^k \le 2B$ for all $p^k \parallel f$, since $L(p^k) \ge \varphi(p^k) \ge p^k/2$ for all prime powers p^k. Consequently, there are only finitely many f for which $L(f) \le B$.

Next, a case-by-case analysis shows that L is at most 4-to-1 on prime powers. To see this, we show that every $m \in \mathbb{N}$ is the L-image of at most 4 prime powers. Since the restriction of L to powers of ramified primes is the identity function, the L-preimage of m contains at most one power of a ramified prime. Let p be the least prime for which there exists some $k \in \mathbb{N}$ with $L(p^k) = m$.

Case I. p is ramified in K.

Let $L(q^l) = m$ for some $q^l \ne p^k$, where $q > p$ is unramified in K. Suppose first that q splits in K. For this case, we have $p^k = q^{l-1}(q-1)$, which implies that $l = 1$ and thus $q = p^k + 1$. Suppose now that q is inert in K. Then $p^k = q^{l-1}(q+1)$. So $l = 1$ and $q = p^k - 1$. We conclude that m is the L-image of at most 3 prime powers.

Case II. p splits in K.

Again, let $L(q^l) = m$ for some $q^l \ne p^k$ with $q \ge p$. Suppose first that q is ramified in K. Then $q > p$, which leads to $p^{k-1}(p-1) \ne q^l$, contradicting $L(p^k) = L(q^l)$. If q splits in K, then $p^{k-1}(p-1) = q^{l-1}(q-1)$. Since $q^l \ne p^k$, we have $q > p$. This implies that $l = 1$ and $q = p^{k-1}(p-1) + 1$. If q is inert in K, then $q > p$ and $p^{k-1}(p-1) = q^{l-1}(q+1)$. Once again, we must have $l = 1$, from which we deduce that $q = p^{k-1}(p-1) - 1$. So as in Case I, m is the L-image of at most 3 prime powers.

Case III. p is inert in K.

Suppose that $L(q^l) = m$ for some $q^l \ne p^k$ with $q \ge p$. If q is ramified in K, then $q > p$ and $p^{k-1}(p+1) = q^l$. In particular, we have $q \ge p+1$ and $q^l \mid (p+1)$. So we must have $l = 1$ and $q = p+1$. Next, if q splits in K, then $q > p$ and $p^{k-1}(p+1) = q^{l-1}(q-1)$. If $l > 1$, then the same argument shows that $l = 2$ and $q = p+1$. Of course, we get $q = p^{k-1}(p+1)+1$ when $l = 1$. Finally, if q is inert in K, then $p^{k-1}(p+1) = q^{l-1}(q+1)$. Since $q^l \ne p^k$, we have $q > p$. When $l > 1$, we get $l = 2$ and $q = p+1$ once again. When $l = 1$, it is obvious that $q = p^{k-1}(p+1) - 1$. In view of the fact that $q = p+1$ can occur for at most one of the three possible cases for q, we conclude that m is the L-image of at most 4 prime powers.

This concludes the proof that L is at most 4-to-1 on prime powers.

We can now complete the proof of the lower bound on $L(f)$. Let f be sufficiently large, and suppose that $L(f) = m$. Since $p^k \le 2\varphi(p^k) \le 2L(p^k)$ for all prime powers p^k, we have

$$f \le \prod_{\substack{p^k \mid f \\ L(p^k) \mid m}} p^k \le \prod_{d \mid m} \prod_{p^k \colon L(p^k) = d} p^k \le \prod_{d \mid m} (2m)^4 = (2m)^{4\tau(m)},$$

where $\tau(\cdot)$ is the divisor counting function. Using the inequality $\tau(m) \le 2^{(1+o(1))\log m/\log\log m}$ (see [HW08, Theorem 317, p. 345]), we deduce that

$$f \le \exp\left((4\log(2m))2^{(1+o(1))\log m/\log\log m}\right),$$

from which it follows that

$$L(f) = m \ge (\log f)^{(1/\log 2 + o(1))\log\log\log f}.$$

As the inequality "$f \le (2m)^{4\tau(m)}$" holds independently of K, the "$o(1)$" term appearing in these last two displays decays to 0 uniformly in K.

4.2. **The upper bound in Proposition 4.1.** We need two lemmas. The first of these appears as Proposition 8 in [EPS83]. For each real number $x > 0$ and each pair of integers a, k with $k \in \mathbb{N}$ and $\gcd(a, k) = 1$, put

$$\theta(x; k, a) = \sum_{\substack{p \le x \\ p \equiv a \,(\mathrm{mod}\, k)}} \log p.$$

Lemma 4.2. *Let $\epsilon > 0$. There are computable positive constants δ and x_0 such that*

$$\left|\theta(x; k, a) - \frac{x}{\varphi(k)}\right| < \epsilon \frac{x}{\varphi(k)}$$

for all $x \ge x_0$, all $k \in \mathbb{N} \cap [1, x^\delta]$ and all $a \in \mathbb{Z}$ with $\gcd(k, a) = 1$, except possibly for those k which are divisible by a certain integer $k_0 = k_0(x) > (\log x)^{3/2}$.

The next result is a variant of [EPS83, Proposition 10].

Lemma 4.3. *Let K be a quadratic field. For all x that are sufficiently large in terms of K, there is a natural number $M_x \le x^2$ for which*

$$\#\{p \text{ inert in } K \colon (p+1) \mid M_x\} > \exp\left(C \frac{\log x}{\log\log x}\right). \tag{13}$$

Here C is a positive, universal constant.

Proof. We let $\delta, x_0 > 0$ be the parameters of Lemma 4.2 corresponding to the choice $\epsilon = \frac{1}{2}$.

Without loss of generality, we may assume that x_0 is sufficiently large (in terms of K). For $x \ge x_0$, let $k_1 = k_1(x)$ denote the product of all the unramified primes $p \le \frac{1}{2}\delta \log x$. Then $k_1 < x^\delta/|\Delta_K|$. Let P be the largest prime factor of Δ_K, and let $p_0 \ge P + 1$ be an arbitrary common prime factor of k_0 and k_1, with the convention that $p_0 = 1$ when $\gcd(k_0, k_1)$ has no prime factors at least $P + 1$. Put $k = k_1/p_0$. If $p_0 > 1$, then it is obvious that $k_0 \nmid k\Delta_K$. On the other hand, if $p_0 = 1$ and $k_0 \mid k\Delta_K$, then all of the prime factors of k_0 would be at most P. Since $k_0 > (\log x)^{3/2}$, there would exist some $p \le P$ such that $p^4 \mid k_0$. But $\gcd(k, \Delta_K) = 1$, k is squarefree, and $\Delta_K = 2^r s$, where $r \in \{0, 2, 3\}$ and $s \in \mathbb{Z}$ is odd and squarefree, so that $p^4 \nmid k\Delta_K$, a contradiction. Therefore, we have $k_0 \nmid k\Delta_K$ in both cases.

For each $d \mid k$, we have from Lemma 4.2 that

$$\begin{aligned}\sum_{\substack{p\le x\\ p\equiv -1 \,(\mathrm{mod}\, d)\\ p \text{ inert in } K}} 1 &= \sum_{\substack{j\in(\mathbb{Z}/|\Delta_K|\mathbb{Z})^\times\\ (\Delta_K/j)=-1}} \sum_{\substack{p\le x\\ p\equiv a_j \,(\mathrm{mod}\, |\Delta_K| d)}} 1\\ &\ge \frac{1}{\log x} \sum_{\substack{j\in(\mathbb{Z}/|\Delta_K|\mathbb{Z})^\times\\ (\Delta_K/j)=-1}} \theta(x; |\Delta_K| d, a_j)\\ &> (1-\epsilon)\frac{x}{\varphi(|\Delta_K| d)\log x} \sum_{\substack{j\in(\mathbb{Z}/|\Delta_K|\mathbb{Z})^\times\\ (\Delta_K/j)=-1}} 1\\ &= (1-\epsilon)\frac{x}{\varphi(|\Delta_K|)\varphi(d)\log x}\cdot\frac{\varphi(|\Delta_K|)}{2}\\ &= \frac{x}{4\varphi(d)\log x},\end{aligned}$$

where $a_j \in (\mathbb{Z}/|\Delta_K| d\mathbb{Z})^\times$ satisfies $a_j \equiv -1 \,(\mathrm{mod}\, d)$ and $a_j \equiv j \,(\mathrm{mod}\, |\Delta_K|)$.

We now use this estimate to lower bound the cardinality of the set A of pairs $(m,p) \in (\mathbb{N}\cap[1,x])^2$ satisfying the congruence $m(p+1) \equiv 0 \,(\mathrm{mod}\, k)$, where p is inert in K. To this end, we define

$$A_d := \{(m,p) \in A\colon d \mid (p+1) \text{ and } \gcd(m,k) = k/d\}$$

for each $d \mid k$. Then A is the disjoint union of A_d's over $d \mid (p+1)$. Note that the number of $m \le x$ with $\gcd(m,k) = k/d$ is at least $\varphi(d)\lfloor x/k\rfloor$. Hence, we obtain

$$\#A_d > \frac{x}{4\varphi(d)\log x}\cdot\varphi(d)\lfloor x/k\rfloor > \frac{x^2}{5k\log x}$$

and

$$\#A = \sum_{d\mid k} \#A_d > \frac{x^2}{5k\log x}\cdot\tau(k) = \frac{x^2}{5k\log x}\cdot 2^{\omega(k)} > \frac{x^2}{5k\log x}\cdot 2^{\frac{(\delta/4)\log x}{\log\log x}},$$

where we have used the prime number theorem to get

$$\omega(k) \ge \pi\left(\frac{\delta}{2}\log x\right) - \omega(\Delta_K) - 1 > \frac{(\delta/4)\log x}{\log\log x}$$

for sufficiently large x depending on Δ_K. Since $m(p+1) \in \{n \le x^2\colon k \mid n\}$ for every pair $(m,p) \in A$, some $n \le x^2$ with $k \mid n$ must admit at least

$$\frac{\#A}{x^2/k} > \frac{1}{5\log x}\cdot 2^{\frac{(\delta/4)\log x}{\log\log x}} > \exp\left(\frac{\delta}{6}\frac{\log x}{\log\log x}\right)$$

representations of the form $n = m(p+1)$ with $(m,p) \in A$. (We use here that $\frac{1}{4}\log 2 > \frac{1}{6}$.) The proof of (13) is completed by taking M_x to be this n. □

We are now in a position to establish the upper bound in Proposition 4.1. Let C be as in Lemma 4.3. Put $x_i = (\log i)^{(2/C)\log\log\log i}$ and

$$g_i = \prod_{\substack{p \text{ inert in } K\\ (p+1)\mid M_{x_i}}} p.$$

By (13), we have

$$g_i \geq \prod_{\substack{p \text{ inert in } K \\ (p+1)|M_{x_i}}} 2 > \exp\left((\log 2)\exp\left(C\frac{\log x_i}{\log\log x_i}\right)\right) > i$$

for sufficiently large i. Moreover, we have $L(g_i) \mid M_{x_i}$, which implies that

$$L(g_i) \leq M_{x_i} \leq x_i^2 = (\log i)^{(4/C)\log\log\log i} < (\log g_i)^{c_0 \log\log\log g_i}$$

for sufficiently large i, where $c_0 := 4/C$. The asserted upper bound follows by extracting a strictly monotonic subsequence $\{f_i\}_{i\geq 1}$ from $\{g_i\}_{i\geq 1}$.

5. Minimal order in the real case: Proof of Theorem 1.4

Let K be a real quadratic field. We remind the reader that ϵ denotes the fundamental unit of K, and we set

$$\delta = \begin{cases} 1 & \text{if } N_{K/\mathbb{Q}}(\epsilon) = 1, \\ 2 & \text{if } N_{K/\mathbb{Q}}(\epsilon) = -1. \end{cases}$$

If p is a prime inert in K, then its associated Frobenius element is conjugation on K (the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q})$). Hence,

$$\epsilon^{p+1} \equiv \epsilon^p \epsilon \equiv N_{K/\mathbb{Q}}(\epsilon) \pmod{p\mathcal{O}_K},$$

and

$$\epsilon^{\delta(p+1)} \equiv N_{K/\mathbb{Q}}(\epsilon)^\delta \equiv 1 \pmod{p\mathcal{O}_K}.$$

Thus, the order of ϵ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ is a divisor of $\delta(p+1)$. We will base our proof of Theorem 1.4 on the following result of Roskam [Ros00].

Proposition 5.1 (conditional on GRH)**.** *There are infinitely many primes p, inert in K, for which the order of ϵ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ is precisely $\delta(p+1)$.*

(In fact, Roskam shows that the order is $\delta(p+1)$ not only for infinitely many inert primes, but for a positive proportion of all inert primes. The weaker version here is sufficient for our purposes.) Theorem 1.4 is an immediate consequence of Proposition 5.1 in conjunction with the next assertion.

Proposition 5.2. *If p is a prime inert in K for which ϵ has order $\delta(p+1)$ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$, then*

$$\rho(\mathcal{O}_p) \leq h_K + \frac{3}{2}.$$

Proof. Let p be as in the proposition. Then $\epsilon^{\ell(p)} \equiv n \pmod{p\mathcal{O}_K}$ for some rational integer n prime to p. By Fermat's little theorem,

$$\epsilon^{(p-1)\ell(p)} \equiv 1 \pmod{p\mathcal{O}_K}.$$

We are assuming that ϵ has order $\delta(p+1)$ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$. Hence, the displayed congruence forces

$$p+1 \mid \delta(p+1) \mid (p-1)\ell(p).$$

Writing $(p-1)\ell(p) = (p+1)\ell(p) - 2\ell(p)$, we deduce that $p+1 \mid 2\ell(p)$. In particular,

$$\ell(p) \geq \frac{p+1}{2}.$$

By Proposition 2.1 and (6),

$$\rho(\mathcal{O}_p) \le \frac{1}{2}\operatorname{Dav}\operatorname{Cl}(\mathcal{O}_p) + \frac{3}{2} \le \frac{h_K}{2}\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_p) + \frac{3}{2} \le \frac{h_K}{2}\#\operatorname{PrinCl}(\mathcal{O}_p) + \frac{3}{2}.$$

The proof is completed by observing that $\#\operatorname{PrinCl}(\mathcal{O}_p) = \frac{\psi(p)}{\ell(p)} = \frac{p+1}{\ell(p)} \le 2$. □

6. Maximal order in the real case: Proof of Theorem 1.3

6.1. **Upper bound.** We start by showing that $\rho(\mathcal{O}_f) \ll f/\log f$ for each $f > 1$. By Proposition 2.1 and (6),

$$\rho(\mathcal{O}_f) \le \frac{h_K}{2}\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) + \frac{3}{2}\Omega(f).$$

As $\Omega(f) \ll \log f \ll \frac{f}{\log f}$, it suffices to demonstrate that $\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) \ll \frac{f}{\log f}$. According to (9), we have $\operatorname{Dav}\operatorname{PrinCl}(\mathcal{O}_f) \ll f/\ell(f)$, so we will be done if we prove that

$$\ell(f) \gg \log f.$$

For this we may assume f is sufficiently large (bounded f can be dealt with by adjusting the implied constant). Say $K = \mathbb{Q}(\sqrt{D})$ with D squarefree, and let τ_D be defined as in (1), so that $1, f\tau_D$ are a $\mathbb{Z}$-basis for $\mathcal{O}_f$. If we express $\epsilon^{\ell(f)} = U + V\tau_D$, then V is a positive integer multiple of f. Writing $\epsilon^{\ell(f)} = u + v\sqrt{D}$ (with $u, v \in \mathbb{Z}$), we find that $v \ge \frac{1}{2}V \ge \frac{1}{2}f$. Therefore, using a tilde for conjugation in K,

$$f \le 2v = \frac{\epsilon^{\ell(f)} - \tilde{\epsilon}^{\ell(f)}}{\sqrt{D}} < \frac{\epsilon^{\ell(f)} + 1}{\sqrt{D}}. \tag{14}$$

Hence (continuing to assume f is large),

$$\epsilon^{\ell(f)} > f\sqrt{D} - 1 > f,$$

and $\ell(f) > \frac{\log f}{\log \epsilon} \gg \log f$.

6.2. **Lower bound.** Now we turn to the lower bound (4). Let p be a prime inert in K with $p > 3$. According to (10),

$$\rho(\mathcal{O}_p) \ge \frac{1}{2}\frac{p+1}{\ell(p)},$$

and so it suffices to produce infinitely many inert p with

$$\frac{p+1}{\ell(p)} > 2p^{\frac{1}{4}-\epsilon}. \tag{15}$$

For this we borrow Lemma 6.4 from [FP].

Lemma 6.1 (conditional on GRH)**.** *Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field, where $D > 1$ is squarefree. Let $\eta = \epsilon$ or ϵ^2, according to whether $N_{K/\mathbb{Q}}(\epsilon) = 1$ or -1, respectively. Let q be an odd prime not dividing D, and let $y \ge 2$ be a real number. The count of primes $p \le y$ for which*

$$p \text{ is inert in } K, \quad p \equiv -1 \pmod{q}, \quad \text{and} \quad \eta^{(p+1)/q} \equiv 1 \pmod{p}, \tag{16}$$

is

$$\frac{1}{2q(q-1)}\int_2^y \frac{\mathrm{d}t}{\log t} + O(y^{1/2}\log(qy)),$$

where the implied constant depends at most on K.

Proof that (15) *holds for infinitely many inert p.* Fix $\epsilon \in (0, 1/2)$. For large y, we select an arbitrary prime q satisfying

$$y^{\frac{1}{4}-\frac{1}{2}\epsilon} < q \le y^{\frac{1}{4}-\frac{1}{4}\epsilon}.$$

By the prime number theorem, there will be many choices for q once y is large enough, and none of these will divide D. Using C for a constant depending at most on K, the count of $p \le y$ satisfying (16) is bounded below by

$$\begin{aligned}\frac{1}{2q(q-1)}\int_2^y \frac{\mathrm{d}t}{\log t} - Cy^{1/2}\log y &> \frac{1}{2q(q-1)\log y}\int_2^y \mathrm{d}t - Cy^{1/2}\log y \\ &> \frac{1}{3}\frac{y^{\frac{1}{2}+\frac{1}{2}\epsilon}}{\log y} - Cy^{1/2}\log y \\ &> y^{\frac{1}{2}+\frac{1}{4}\epsilon}.\end{aligned}$$

In particular, for all large y there is at least one such p. As $\eta^{(p+1)/q} \equiv 1 \pmod{p\mathcal{O}_K}$, and $\eta = \epsilon$ or ϵ^2, we must have $\epsilon^{(p+1)/q} \equiv \pm 1 \pmod{p\mathcal{O}_K}$. Hence, $\epsilon^{(p+1)/q} \in \mathcal{O}_p$ and $\ell(p) \mid \frac{p+1}{q}$. Therefore, $q \mid \frac{p+1}{\ell(p)}$, and

$$\frac{p+1}{\ell(p)} \ge q > y^{\frac{1}{4}-\frac{1}{2}\epsilon} > 2y^{\frac{1}{4}-\epsilon} \ge 2p^{\frac{1}{4}-\epsilon},$$

verifying (15).

To see that this argument produces infinitely many p, note that $p > q > y^{\frac{1}{4}-\frac{1}{2}\epsilon}$, while y can be taken arbitrarily large. □

Remark. Let K be a real quadratic field. For each $m = 0, 1, 2, \ldots$, write $2\epsilon^m = u_m + v_m\sqrt{D}$, where $u_m, v_m \in \mathbb{Q}$. Then $u_m, v_m \in \mathbb{N}$, and v_m grows exponentially with m; in fact, $v_m \sim \epsilon^m/\sqrt{D}$, as $m \to \infty$ (compare with (14)).

We conjecture the existence of a constant $\delta = \delta_K > 0$ for which the following holds:

(17) v_m has an inert prime factor $p > v_m^\delta$ for infinitely many $m \in \mathbb{N}$.

Suppose p, m are related as in (17), and that m is large. Then $p > 3$, and $p \mid v_m$ implies that $\epsilon^m \in \mathcal{O}_p$. It follows that

$$\ell(p) \le m \ll \log v_m \ll \log p,$$

and

$$\rho(\mathcal{O}_p) \ge \frac{1}{2}\frac{p+1}{\ell(p)} \gg \frac{p}{\log p}.$$

So if our conjecture (17) holds, then the upper bound of Theorem 1.3(a) is sharp.

To illustrate, let $K = \mathbb{Q}(\sqrt{2})$. In this case, $\epsilon = 1 + \sqrt{2}$, each v_m is even, and $\frac{1}{2}v_m$ is commonly termed the mth Pell number. It seems plausible to conjecture that there are infinitely many Pell numbers that are themselves prime; e.g., looking at indices $m < 1000$, one finds that $\frac{1}{2}v_m$ is prime for $m = 2$, 3, 5, 11, 13, 29, 41, 53, 59, 89, 97, 101, 167, 181, 191, 523, 929 (this is OEIS sequence A096650). Among these m, the prime $\frac{1}{2}v_m$ is inert in K roughly half the time, for $m = 3$, 5, 11, 13, 29, 53, 59, 101, 181, 523. We view this as compelling evidence that when $K = \mathbb{Q}(\sqrt{2})$, our hypothesis (17) holds for any $\delta \in (0, 1)$.

Acknowledgements

P.P. gratefully acknowledges the support of the National Science Foundation under award DMS-2001581.

References

[And97] D. F. Anderson, *Elasticity of factorizations in integral domains: a survey*, Factorization in integral domains (Iowa City, IA, 1996), Lecture Notes in Pure and Appl. Math., vol. 189, Dekker, New York, 1997, pp. 1–29.

[Car60] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. **11** (1960), 391–392.

[CC00] S. T. Chapman and J. Coykendall, *Half-factorial domains, a survey*, Non-Noetherian commutative ring theory, Math. Appl., vol. 520, Kluwer Acad. Publ., Dordrecht, 2000, pp. 97–115.

[CMO17] J. Coykendall, P. Malcolmson, and F. Okoh, *Inert primes and factorization in extensions of quadratic orders*, Houston J. Math. **43** (2017), 61–77.

[Cox22] D. A. Cox, *Primes of the form $x^2 + ny^2$—Fermat, class field theory, and complex multiplication*, third ed., AMS Chelsea Publishing, Providence, RI, 2022.

[Coy01] J. Coykendall, *Half-factorial domains in quadratic fields*, J. Algebra **235** (2001), 417–430.

[EPS83] P. Erdős, C. Pomerance, and E. Schmutz, *On distinguishing prime numbers from composite numbers*, Annals Math. **117** (1983), 173–206.

[EPS91] ———, *Carmichael's lambda function*, Acta Arith. **58** (1991), 363–385.

[FP] K. (S) Fan and P. Pollack, *The typical elasticity of a quadratic order*, submitted; `arXiv:2411.09063`.

[GHK06] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations*, Pure and Applied Mathematics (Boca Raton), vol. 278, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[HK72] F. Halter-Koch, *Einseinheitengruppen und prime Restklassengruppen in quadratischen Zahlkörpern*, J. Number Theory **4** (1972), 70–77.

[HK83] ———, *Factorization of algebraic integers*, Grazer Math. Berichte **191** (1983).

[HK95] ———, *Elasticity of factorizations in atomic monoids and integral domains*, J. Théor. Nombres Bordeaux **7** (1995), 367–385.

[HW08] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008.

[Nar95] W. Narkiewicz, *A note on elasticity of factorizations*, J. Number Theory **51** (1995), 46–47.

[Pol24] P. Pollack, *Half-factorial real quadratic orders*, Arch. Math. (Basel) **122** (2024), 491–500.

[Pol25] ———, *Maximally elastic quadratic fields*, J. Number Theory **267** (2025), 80–100.

[Ros00] H. Roskam, *A quadratic analogue of Artin's conjecture on primitive roots*, J. Number Theory **81** (2000), 93–109, erratum in **85** (2000), 108.

[Ste86] J.-L. Steffan, *Longueurs des décompositions en produits d'éléments irréductibles dans un anneau de Dedekind*, J. Algebra **102** (1986), 229–236.

[Val90] R. J. Valenza, *Elasticity of factorization in number fields*, J. Number Theory **36** (1990), 212–218.

[vEBK67] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite Abelian groups*, Math. Centrum Amsterdam Afd. Zuivere Wisk. (1967), 27 pp.

[Zak76] A. Zaks, *Half factorial domains*, Bull. Amer. Math. Soc. **82** (1976), 721–723, corrigendum in **82** (1976), 965.

[Zak80] ———, *Half-factorial-domains*, Israel J. Math. **37** (1980), 281–302.

Department of Mathematics, University of Georgia, Athens, GA 30602

Email address: `Steve.Fan@uga.edu`

Email address: `pollack@uga.edu`