MAXIMALLY ELASTIC QUADRATIC FIELDS

PAUL POLLACK

Abstract. Recall that for a domain R where every nonzero nonunit factors into irreducibles, the elasticity of R is defined as

$$\sup\left\{\frac{s}{r} : \pi_1 \cdots \pi_r = \rho_1 \cdots \rho_s, \text{ with all } \pi_i, \rho_j \text{ irreducible}\right\}.$$

We call a quadratic field K maximally elastic if the ring of integers of K is a UFD and each element of $\{1, \frac{3}{2}, 2, \frac{5}{2}, 3, \dots\} \cup \{\infty\}$ appears as an elasticity of infinitely many orders inside K. This corresponds to the orders in K exhibiting, to the extent possible for a quadratic field, maximal variation in terms of the failure of unique factorization. Assuming the Generalized Riemann Hypothesis, we prove that $K = \mathbb{Q}(\sqrt{2})$ is universally elastic, and we provide evidence for a conjectured characterization of maximally elastic quadratic fields.

1. Introduction

Let R be an atomic domain, meaning an integral domain where every nonzero nonunit factors into irreducibles. The elasticity $\rho(R)$ is defined as the supremum of all ratios s/r, where r and s range over those pairs of positive integers for which

$$\pi_1 \cdots \pi_r = \rho_1 \cdots \rho_s \quad \text{for some irreducibles } \pi_i, \rho_j \text{ of } R.$$

This concept was introduced by Valenza [Val90] in the context of rings of integers of number fields. Later this same notion was considered for arbitrary Dedekind domains with finite class group by Steffan [Ste86] (who however did not use the term 'elasticity').[1] In the general form appearing here, the definition is due to Anderson–Anderson [AA92].

As a simple illustration, $\rho(R) = 1$ precisely when two factorizations into irreducibles of the same nonzero nonunit element always have the same length. In this case, the domain R is called a half-factorization domain (or HFD). Actually, the study of HFDs predates the notion of elasticity; Carlitz showed in 1960 that the ring of integers $\mathbb{Z}_K$ of a number field K is half-factorial exactly when K has class number 1 or 2 [Car60].

For number fields K the elasticity of $\mathbb{Z}_K$ is completely determined, as a function of the class group of K, in work of Valenza (op. cit.), Steffan (op. cit.), and Narkiewicz [Nar95]: It is 1 if K is a UFD and otherwise is half the Davenport constant of the class group of K. (While the Davenport constant lurks in the background of our work below, it will not be used explicitly, and so we refer the reader to the cited papers for the definition.) Less is known about elasticities of nonmaximal orders, although several quite general theorems of Halter-Koch [HK95] can be applied here. For example, suppose $\mathcal{O}$ is an order in the number field K. Then $\rho(\mathcal{O}) < \infty$ if and only if, for every prime ideal P of $\mathcal{O}$, there is precisely one prime ideal of $\mathbb{Z}_K$ lying above P; this is [HK95, Corollary 4]. Halter-Koch's work also provides useful upper and lower bounds on $\rho(\mathcal{O})$, although it is still a non-routine matter in most instances to compute the exact value.

2020 *Mathematics Subject Classification.* Primary 13F15; Secondary 11R11, 11R54.

[1] The publication dates are misleading here; Valenza's manuscript was submitted already in 1980.

Perhaps unsurprisingly, the orders for which the most is known are those belonging to quadratic number fields. In [PL01], M. Picavet-L'Hermitte calculates $\rho(\mathcal{O})$ whenever $\mathcal{O}$ is a quadratic order of class number 1. (The definition of the class group of an order is recalled in §2 below.) Necessary and sufficient conditions for a quadratic order $\mathcal{O}$ to be half-factorial have been given by Halter-Koch [HK83] and Coykendall [Coy01]. In [Coy01] (and [CC00]) one also finds the remarkable result that $\mathbb{Z}[\sqrt{-3}]$ is the unique nonmaximal imaginary quadratic half-factorial order.

Coykendall conjectured (op. cit.) that $\mathbb{Z}[\sqrt{2}]$ contains infinitely many orders that are HFDs. This conjecture was resolved by the author in [Pol24] under the assumption of the Generalized Riemann Hypothesis (GRH).[2] In this paper we prove, again conditionally on GRH, that $\mathbb{Z}[\sqrt{2}]$ enjoys a much stronger property.

It will be shown below (see Lemma 2.2) that the elasticity of any quadratic order $\mathcal{O}$ belongs to the set

$$\mathscr{E} := \{1, \frac{3}{2}, 2, \frac{5}{2}, 3, \dots\} \cup \{\infty\}.$$

We call a quadratic field K maximally elastic if (a) the maximal order of K is a UFD, and (b) each element of $\mathscr{E}$ occurs as the elasticity of infinitely many orders in $\mathcal{O}$. This definition expresses the requirement that K exhibit the maximal possible variation in the factorization behavior of its orders. (Note that it would not be sensible to strengthen (a) to require infinitely many orders to be UFDs. UFDs are integrally closed and so only the maximal order has a shot at possessing unique factorization.)

Theorem 1.1 (conditional on GRH)**.** $\mathbb{Q}(\sqrt{2})$ *is maximally elastic.*

It is natural to wonder how unique $\mathbb{Q}(\sqrt{2})$ is in this regard. As explained in [Pol24], results of Halter-Koch (op. cit.), Coykendall (op. cit.), and Alan [Ala16] imply that for a quadratic field K to contain infinitely many half-factorial orders, it is necessary that K be real, have class number 1 or 2, and that the fundamental unit of K have norm -1. Thus, the following conjecture is the most optimistic one could hope for.

Conjecture 1.2. *Let K be a real quadratic field with class number 1 and fundamental unit of norm -1. Then K is maximally elastic.*

In §4 we provide what we view as strong evidence for Conjecture 1.2. Namely, we show that Conjecture 1.2 follows from the GRH and a plausible-seeming hypothesis (Conjecture 4.1) on the distribution of certain special primes associated to K.

Without assuming any unproved hypothesis, it was proved in [Pol24] that *some* real quadratic field K possesses infinitely many HFD orders. It seems to be a difficult problem to prove unconditionally the existence of a maximally elastic quadratic field. We hope the interested reader will take up this challenge.

2. Algebraic groundwork for the proof of Theorem 1.1

Lemma 2.1. *Let $\mathcal{O}$ be an order in a quadratic field K. If π is an element of $\mathcal{O}$ for which $|N\pi|$ is prime, then π is prime in $\mathcal{O}$.*

[2] For us GRH refers to the claim that all nontrivial zeros of all Dedekind zeta functions lie on $\Re(s) = \frac{1}{2}$.

Proof. For any quadratic order $\mathcal{O}$ and any nonzero $\alpha \in \mathcal{O}$, it is well-known that $|\mathcal{O}/\alpha\mathcal{O}| = |N\alpha|$. (See for instance Exercise 7.14 on p. 120 of [Cox22], whose solution appears on p. 382 of the same reference.) So in our setup, $\mathcal{O}/\pi\mathcal{O} \cong \mathbb{F}_p$ for the prime number $p = |N\pi|$. Hence, $\pi\mathcal{O}$ is a prime ideal of $\mathcal{O}$ and π is a prime element of $\mathcal{O}$. □

When m is a nonzero integer, we write $\Omega(m)$ for the number of rational primes dividing m, counted with multiplicity. For example, $\Omega(15) = \Omega(-9) = 2$.

Lemma 2.2. *Let $\mathcal{O}$ be an order in a quadratic field K. Then*

$$\rho(\mathcal{O}) = \frac{1}{2}\sup\{\Omega(N\pi) : \text{ irreducible } \pi \in \mathcal{O}\}. \tag{1}$$

Proof. Here and below we use a tilde to denote conjugation in K. If π is irreducible and $\Omega(N\pi) = r$, we may write $\pi\tilde{\pi} = \pm p_1 \cdots p_r$ with all the p_i rational primes. After decomposing the p_i into irreducibles of $\mathcal{O}$, we are left with a product of two irreducibles equal to a product of at least r irreducibles. Hence, $\rho(\mathcal{O}) \geq \frac{1}{2}r = \frac{1}{2}\Omega(N\pi)$. This proves the lower bound implicit in (1) and so establishes (1) whenever the right-hand side there is infinite.

Now suppose the right-hand side of (1) is finite, say equal to R. Clearly $R \geq 1$, since each rational prime p inert in K is irreducible in $\mathcal{O}$, and $\frac{1}{2}\Omega(Np) = 1$ for these p.

Take any two factorizations of the same nonzero nonunit element into irreducibles, say

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

arranged so that $r \leq s$. If any ρ_j is prime in $\mathcal{O}$, it must divide some π_i; canceling, we arrive at two factorizations with $r-1$ and $s-1$ irreducibles, respectively. If any of the irreducibles on the new right-hand side is prime, we can cancel again. Continuing, we are led to a product of $r-k$ irreducibles equal to one of $s-k$ irreducibles (for some $k \geq 0$), say

$$\pi'_1 \cdots \pi'_{r-k} = \rho'_1 \cdots \rho'_{s-k},$$

where none of the ρ'_j are prime in $\mathcal{O}$. If $r-k = 0$, then $s-k = 0$, so $s = k = r$ and $s/r = 1 \leq R$. Otherwise, $0 < r-k \leq s-k$, and $\frac{s}{r} \leq \frac{s-k}{r-k}$. By Lemma 2.1, the norm of each ρ'_j has at least two prime factors, and so

$$2R(r-k) \geq \Omega(N(\pi'_1 \cdots \pi'_{r-k})) = \Omega(N(\rho'_1 \cdots \rho'_{s-k})) \geq 2(s-k).$$

Hence, $\frac{s}{r} \leq \frac{s-k}{r-k} \leq R$, which completes the proof of the upper bound in (1). □

Remarks. In the terminology of [AA92], the mapping $\alpha \mapsto \Omega(N\alpha)$ is a length function on $\mathcal{O}$. Our proof of the upper bound half of (1) follows the argument for Theorem 2.1 in [AA92].

Recall that the orders in a quadratic field K are naturally parametrized by positive integers f: If $\mathcal{O}$ is an order in K, then its index (as an additive subgroup) $f := [\mathbb{Z}_K : \mathcal{O}]$ is finite, and

$$\mathcal{O} = \{\alpha \in \mathbb{Z}_K : \alpha \equiv a \pmod{f\mathbb{Z}_K} \text{ for some } a \in \mathbb{Z}\}.$$

Conversely, given $f \in \mathbb{Z}_{>0}$ this last display defines an order in $\mathbb{Z}_K$ with index f. See for instance [Cox22, p. 105]. We refer to f as the conductor of $\mathcal{O}$. In the sequel, the order of conductor f will be denoted $\mathcal{O}_f$. The ambient field K will always be clear from context.

Let $\mathcal{O}$ be an order of conductor f in a quadratic field K. With I_K the group of fractional ideals of K, we let $I_K(f)$ denote the subgroup of I_K generated by those nonzero ideals of $\mathbb{Z}_K$ comaximal with $f\mathbb{Z}_K$. (So $I_K(1) = I_K$.) Write $P_{K,\mathbb{Z}}(f)$ for the subgroup of $I_K(f)$ generated by the ideals $\alpha\mathbb{Z}_K$, where $\alpha \equiv a \pmod{f\mathbb{Z}_K}$ for some rational integer a coprime to f. The (ring) class group $\mathrm{Cl}(\mathcal{O})$ of $\mathcal{O}$ is defined as the quotient $I_K(f)/P_{K,\mathbb{Z}}(f)$. The class number of $\mathcal{O}$ is $h(\mathcal{O}) := \#\mathrm{Cl}(\mathcal{O})$. We write $h(K)$ for the class number of K, corresponding in this picture to $\mathcal{O} = \mathbb{Z}_K$.

For real quadratic K, the numbers $h(\mathcal{O})$ and $h(K)$ are related by the following relative class number formula. See Theorem 2 on p. 217 in [Coh80] or Theorem 3.8.7 on p. 277 of [HK20].

Relative class number formula. *Let K be a real quadratic field with discriminant Δ and fundamental unit ε_0. Let $\mathcal{O}$ be the order of conductor f inside K. Then*

$$h(\mathcal{O}) = h(K)\psi_\Delta(f)/u,$$

where

$$\psi_\Delta(f) := f\prod_{p\mid f}\left(1 - \left(\frac{\Delta}{p}\right)p^{-1}\right),$$

and u (the unit index of $\mathcal{O}$) is the least positive integer with $\varepsilon_0^u \in \mathcal{O}$.

The next lemma is due essentially to Weber [Web82] (see also Corollary 2.11.16 on p. 159 of [GHK06]). Recall that if P is a nonzero prime ideal of $\mathbb{Z}_K$, the (absolute) degree of P is the dimension of $\mathbb{Z}_K/P$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$, where $p\mathbb{Z} = P \cap \mathbb{Z}$.

Lemma 2.3. *Let $\mathcal{O}$ be an order in a quadratic field K. Every class in $\mathrm{Cl}(\mathcal{O})$ is represented by infinitely many degree one prime ideals of $\mathbb{Z}_K$.*

Proof. We sketch a proof for completeness. Let f be the conductor of $\mathcal{O}$. The group $\mathrm{Cl}(\mathcal{O}) = I_K(f)/P_{K,\mathbb{Z}}(f)$ is a generalized ideal class group of K for the modulus $f\mathbb{Z}_K$. By the existence theorem of global class field theory, there is an abelian extension L/K for which the Artin map sets up an isomorphism $\mathrm{Cl}(\mathcal{O}) \cong \mathrm{Gal}(L/K)$. (See [Cox22, Chapter 8] for a lucid discussion of the main statements of global class field theory.) Applying the Chebotarev density theorem to L/K, the set of prime ideals of $\mathbb{Z}_K$ (comaximal with $f\mathbb{Z}_K$) that represent a given class in $\mathrm{Cl}(\mathcal{O})$ has Dirichlet density $1/h(\mathcal{O})$. As the prime ideals of degree larger than 1 make up a set of density zero, the lemma follows. □

Lemma 2.4. *Let K be a quadratic field of class number 1. Let $\mathcal{O}$ be the order of conductor p^k inside K, where p is an odd prime inert in K and $k \in \mathbb{Z}_{>0}$. Then $\mathrm{Cl}(\mathcal{O})$ is cyclic.*

Proof. Write $K = \mathbb{Q}(\sqrt{D})$ with D squarefree. Choose $w \in \mathbb{Z}_K$ whose mod $p\mathbb{Z}_K$ reduction generates the multiplicative group of the finite field $\mathbb{Z}_K/p\mathbb{Z}_K$. Then as shown by Halter-Koch [HK72], the group $G := (\mathbb{Z}_K/p^k\mathbb{Z}_K)^\times$ has as a basis the mod $p^k\mathbb{Z}_K$ images of $g_1 := w^{p^{2k-2}}$, $g_2 := 1 + p\sqrt{D}$, and $g_3 := 1 + p$; furthermore, these elements have respective orders $p^2 - 1$, p^{k-1}, and p^{k-1} in G.

Hence, if H is any subgroup of G containing $g_3 \bmod p^k\mathbb{Z}_K$, then G/H is generated by the mod $p^k\mathbb{Z}_K$ reductions of g_1 and g_2. Since g_1 and g_2 have coprime orders in G/H, it follows that G/H is cyclic with generator g_1g_2.

To deduce the lemma, we use (for the first time in this proof) that $\mathbb{Z}_K$ is a PID. There is a surjective homomorphism $G \to \mathrm{Cl}(\mathcal{O})$ mapping $\alpha \bmod p^k\mathbb{Z}_K$ to the class of the ideal $\alpha\mathbb{Z}_K$. Since $g_3\mathbb{Z}_K \in P_{K,\mathbb{Z}}(p^k)$, the corresponding kernel H contains $g_3 \bmod p^k$, and $\mathrm{Cl}(\mathcal{O}) \cong G/H$. □

The next two lemmas are our workhorse results; they compute the elasticities of the orders we will use to prove Theorem 1.1.

The following basic observation will be used repeatedly in subsequent arguments. Let K be a quadratic field and let $f \in \mathbb{Z}_{>0}$. Suppose $\alpha, \beta \in \mathcal{O}_f$ and that β divides α in $\mathbb{Z}_K$. Suppose further that $\beta \equiv b \pmod{f\mathbb{Z}_K}$, where b is a rational integer with $\gcd(b, f) = 1$. Then β divides α in $\mathcal{O}_f$. For the proof, write $\alpha = \beta\gamma$ and reduce mod $f\mathbb{Z}_K$. If $\alpha \equiv a \pmod{f\mathbb{Z}_K}$ with $a \in \mathbb{Z}$, then $\gamma \equiv ab^{-1} \pmod{f}$, where b^{-1} denotes a (rational integer) inverse of b mod $f\mathbb{Z}_K$. Thus, $\gamma \in \mathcal{O}_f$.

Lemma 2.5. *Let K be a real quadratic field of class number 1. Let $\mathcal{O}$ be the order of conductor p^k in K, where p is an odd prime inert in K and $k \in \mathbb{Z}_{>0}$. Let h be the class number of $\mathcal{O}$. Then*

$$\rho(\mathcal{O}) = k + \frac{1}{2}(h-1).$$

In the following arguments, ε_0 always denotes the fundamental unit of K.

Proof. Using Lemma 2.3, let P be a degree one prime ideal of $\mathbb{Z}_K$ that is comaximal with $p\mathbb{Z}_K$ and generates $\mathrm{Cl}(\mathcal{O})$. Write $P = \pi\mathbb{Z}_K$, with $\pi \in \mathbb{Z}_K$.

To bound $\rho(\mathcal{O})$ from below, we will show that at least one of $\alpha := p^k\pi^{h-1}$ and $\alpha' := p^k\pi^{h-1}\varepsilon_0$ must be irreducible in $\mathcal{O}$. The lower bound half of the lemma then follows from Lemma 2.2, since $\frac{1}{2}\Omega(N\alpha) = \frac{1}{2}\Omega(N\alpha') = k + \frac{1}{2}(h-1)$.

Suppose $\alpha = \beta\gamma$, where β and γ are nonunits of $\mathcal{O}$. After changing the signs of β and γ if necessary, we can write

$$\beta = p^a\pi^b\varepsilon_0^c, \quad \gamma = p^{a'}\pi^{b'}\varepsilon_0^{c'},$$

where a, b, c and a', b', c' are nonnegative integers with $a + a' = k$, $b + b' = h - 1$, and $c + c' = 0$. If $a = 0$, then $\pi^b\varepsilon_0^c \in \mathcal{O}$, implying that P^b represents the identity of $\mathrm{Cl}(\mathcal{O})$. Since $0 \le b < h$ while P has order h in $\mathrm{Cl}(\mathcal{O})$, this forces $b = 0$, contradicting that β is a not a unit. Thus $a \neq 0$. Similarly, $a' \neq 0$. Since a and a' are positive integers summing to k, both $a, a' < k$. It follows that $\pi^b\varepsilon_0^c$ and $\pi^{b'}\varepsilon_0^{c'}$ belong to $\mathcal{O}_p$. Hence,

$$\pi^{h-1} = (\pi^b\varepsilon_0^c)(\pi^{b'}\varepsilon_0^{c'}) \in \mathcal{O}_p. \tag{2}$$

An entirely analogous argument shows that if α' is not irreducible in $\mathcal{O}$, then

$$\pi^{h-1}\varepsilon_0 \in \mathcal{O}_p.$$

So if neither α nor α' is irreducible, then π^{h-1} and $\pi^{h-1}\varepsilon_0$ both belong to $\mathcal{O}_p$. Let u, u' be rational integers with $\pi^{h-1} \equiv u \pmod{p\mathbb{Z}_K}$, $\pi^{h-1}\varepsilon_0 \equiv u' \pmod{p\mathbb{Z}_K}$. Since $\pi\mathbb{Z}_K$ and $p\mathbb{Z}_K$ are comaximal, both u and u' are coprime to p. Then $\varepsilon_0 \equiv u'u^{-1} \pmod{p\mathbb{Z}_K}$, where u^{-1} is a rational integer that inverts u mod $p\mathbb{Z}_K$. Hence $\varepsilon_0 \in \mathcal{O}_p$.

We can obtain a contradiction as follows. Since P generates $\mathrm{Cl}(\mathcal{O})$, it also generates $\mathrm{Cl}(\mathcal{O}_p)$. (We use here that $I_K(p) = I_K(p^k)$ while $P_{K,\mathbb{Z}}(p^k) \subseteq P_{K,\mathbb{Z}}(p)$, so that $\mathrm{Cl}(\mathcal{O}_p)$ can be viewed as a quotient of $\mathrm{Cl}(\mathcal{O}) = \mathrm{Cl}(\mathcal{O}_{p^k})$.) By (2), P^{h-1} is the identity of $\mathrm{Cl}(\mathcal{O}_p)$, and therefore

$$h(\mathcal{O}_p) \mid h - 1 = h(\mathcal{O}) - 1.$$

On the other hand, $h(\mathcal{O}_p) \mid h(\mathcal{O})$. Hence, $h(\mathcal{O}_p) = 1$. But $\varepsilon_0 \in \mathcal{O}_p$, so that the relative class number formula makes the contrasting assertion that $h(\mathcal{O}_p) = p + 1$.

To argue for the upper bound on $\rho(\mathcal{O})$, we let α be an arbitrary irreducible of $\mathcal{O}$ and we factor α over $\mathbb{Z}_K$, say $\alpha = p^e \pi_1 \cdots \pi_r \varepsilon$, where $e \geq 0$, the π_i are primes of $\mathbb{Z}_K$ generating ideals comaximal with $p\mathbb{Z}_K$, and ε is a unit. (We include ε in our potential factorization to handle the case when $r = 0$; otherwise, it can be absorbed into one of the π_i.)

If any of the π_i lie above a prime q that is inert in $\mathbb{Z}_K$, then q divides α in $\mathbb{Z}_K$, and q is an element of $\mathcal{O}$ for which $q\mathbb{Z}_K$ and $p\mathbb{Z}_K$ are comaximal. So we are set up to apply our 'basic observation' and conclude that q divides α in $\mathcal{O}$. Since q is not a unit, it must be that α is an associate of q. Then $\frac{1}{2}\Omega(N\alpha) = 1 \leq k + \frac{1}{2}(h-1)$. So for the sake of proving our upper bound, we can suppose each of the π_i lie above rational primes that are split or ramified in K. In particular, each $N\pi_i$ is itself a rational prime (up to sign).

Suppose that $r \geq h$. In this case, some nonempty subsequence of $\pi_1\mathbb{Z}_K, \ldots, \pi_h\mathbb{Z}_K$ multiplies to the identity in $\mathrm{Cl}(\mathcal{O})$. (Here is the easy proof, well-known in the theory of Davenport constants: If none of the h ideals $\pi_1\mathbb{Z}_K, \pi_1\pi_2\mathbb{Z}_K, \ldots, \pi_1 \cdots \pi_h\mathbb{Z}_K$ represents the identity in $\mathrm{Cl}(\mathcal{O})$, the pigeonhole principle forces two of these to coincide in $\mathrm{Cl}(\mathcal{O})$, say $\pi_1 \cdots \pi_i\mathbb{Z}_K = \pi_1 \cdots \pi_j\mathbb{Z}_K$, with $i < j$. Then $\pi_{i+1} \cdots \pi_j\mathbb{Z}_K$ is trivial in $\mathrm{Cl}(\mathcal{O})$.) Thus, after possibly reordering the π_i, we can write

$$\pi_1 \cdots \pi_j\mathbb{Z}_K = \gamma\mathbb{Z}_K,$$

for some $j \in \{1, 2, \ldots, h\}$ and some $\gamma \in \mathcal{O}$. Observe that γ divides α in $\mathbb{Z}_K$ and that $\gamma\mathbb{Z}_K$ is comaximal with $p\mathbb{Z}_K$, so that γ divides α in $\mathcal{O}$. Since γ is not a unit in $\mathcal{O}$, it must be that α is a $\mathbb{Z}_K$-associate of $\pi_1 \cdots \pi_j$, forcing

$$\frac{1}{2}\Omega(N\alpha) = \frac{1}{2}j \leq \frac{1}{2}h < k + \frac{1}{2}(h-1).$$

So for the sake of proving our target upper bound, we can assume $r \leq h - 1$.

We can also assume that $e \leq k$: If $e > k$, then writing $\alpha = p \cdot (p^{e-1}\pi_1 \cdots \pi_r)$ yields a nontrivial factorization of α in $\mathcal{O}$. Since $e \leq k$ and $r \leq h - 1$,

$$\frac{1}{2}\Omega(N\alpha) = e + \frac{1}{2}r \leq k + \frac{1}{2}(h-1),$$

and the lemma is proved. □

Lemma 2.6. *Let K be a real quadratic field of class number 1. Let p be a prime inert in K with $h(\mathcal{O}_p) = 1$. Suppose that q is a prime distinct from p which is inert in K and that*

$$h(\mathcal{O}_q) = h(\mathcal{O}_{q^k}) = 2,$$

where $k \in \mathbb{Z}_{>0}$. Suppose also that $\gcd(q^{\frac{q+1}{2}}, p+1) = 1$. *Then $\rho(\mathcal{O}_{pq^k}) = k + \frac{1}{2}$.*

Proof. We write Δ for the discriminant of K and we let $\mathcal{O} = \mathcal{O}_{pq^k}$. We start by showing that $h(\mathcal{O}) = 2$. Since $\mathcal{O}_p$ has class number 1 while $\mathcal{O}_{q^k}$ has class number 2, the order $\mathcal{O}_p$ has unit index $\psi_\Delta(p) = p + 1$ while $\mathcal{O}_{q^k}$ has unit index $\frac{1}{2}\psi_\Delta(q^k) = \frac{1}{2}(q+1)q^{k-1}$. As $\gcd(\psi_\Delta(p), \frac{1}{2}\psi_\Delta(q^k)) = 1$, it follows that $\mathcal{O}$ has unit index $\frac{1}{2}\psi_\Delta(p)\psi_\Delta(q^k) = \frac{1}{2}\psi_\Delta(pq^k)$. Thus, $h(\mathcal{O}) = 2$.

Next, we exhibit an irreducible α in $\mathcal{O}$ with $\Omega(N\alpha) = 2k+1$; by Lemma 2.2, this will show that the elasticity is at least as large as claimed. Let P be a degree one prime ideal of $\mathbb{Z}_K$ comaximal with

$pq\mathbb{Z}_K$ and representing the nontrivial ideal class of $\mathrm{Cl}(\mathcal{O}_q)$. Write $P = \pi\mathbb{Z}_K$. Since $\mathrm{Cl}(\mathcal{O}_p) = 1$, we have $\pi\varepsilon_0^a \in \mathcal{O}_p$ for some $a \in \mathbb{Z}$. We let

$$\alpha = q^k \pi \varepsilon_0^a.$$

Clearly, $\alpha \in \mathcal{O}$ and $\Omega(N\alpha) = 2k+1$, so we focus on proving that α is irreducible in $\mathcal{O}$. After reordering and possibly changing signs, any factorization of α over $\mathbb{Z}_K$ has the form

$$q^{k_1}\varepsilon_0^{a_1} \cdot q^{k_2}\pi\varepsilon_0^{a_2},$$

where $k_1 + k_2 = k$ and $a_1 + a_2 = a$. For the factorization to be nontrivial, we need that $k_1 > 0$, so that $k_2 = k - k_1 < k$. But then the second factor above cannot land in $\mathcal{O}$: $q^{k_2}\pi\varepsilon_0^{a_2} \in \mathcal{O}$ implies $\pi\varepsilon_0^{a_2} \in \mathcal{O}_{q^{k-k_2}p} \subseteq \mathcal{O}_q$, and this contradicts the choice of P.

To prove the elasticity is no larger than claimed, we let α be any irreducible of $\mathcal{O}$ and we show $\Omega(\alpha) \le 2k+1$. We can factor α over $\mathbb{Z}_K$ as

$$p^a q^b \pi_1 \cdots \pi_r \varepsilon,$$

where a and b are nonnegative integers, $\pi_1, \ldots, \pi_r$ (with $r \ge 0$) are primes of $\mathbb{Z}_K$ generating ideals comaximal with $pq\mathbb{Z}_K$, and ε is a unit of $\mathbb{Z}_K$.

As in the last proof we can assume each $N\pi_i$ is prime in $\mathbb{Z}$ (up to sign); otherwise, $\Omega(N\alpha) \le 2 < 2k+1$. Also, $a \le 1$ and $b \le k$; otherwise, we could have factored α over $\mathcal{O}$ as $p \cdot \frac{\alpha}{p}$ or $q \cdot \frac{\alpha}{q}$.

Suppose that $r > 1$. Then either $\pi_1\mathbb{Z}_K$, $\pi_2\mathbb{Z}_K$, or $\pi_1\pi_2\mathbb{Z}_K$ represents the identity of $\mathrm{Cl}(\mathcal{O})$ and so π_1, π_2, or $\pi_1\pi_2$ has a $\mathbb{Z}_K$-associate in $\mathcal{O}$. This associate is a $\mathbb{Z}_K$-divisor of α and so (by our basic observation) also an $\mathcal{O}$-divisor of α. Since α is irreducible over $\mathcal{O}$, this implies $\Omega(N\alpha) \le 2 < 2k+1$. Summarizing, we may assume $b \in \{0, 1, \ldots, k\}$ and that $a, r \in \{0, 1\}$.

So to have $\Omega(N\alpha) > 2k+1$, either $\alpha = pq^k\varepsilon$ or $\alpha = pq^k\pi_1\varepsilon$. Neither is possible. If $\alpha = pq^k\varepsilon$, then α admits the nontrivial $\mathcal{O}$-factorization $\alpha = p\varepsilon_0^{-a} \cdot q^k\varepsilon\varepsilon_0^a$, where $a \in \mathbb{Z}$ is chosen to ensure $\varepsilon_0^{-a} \in \mathcal{O}_{q^k}$ and $\varepsilon\varepsilon_0^a \in \mathcal{O}_p$. Here the conditions on a can be satisfied simultaneously as they amount to putting a in certain residue classes modulo $\frac{1}{2}(q+1)q^{k-1}$ and modulo $p+1$, and $\gcd(\frac{1}{2}(q+1)q^{k-1}, p+1) = 1$. Similarly, we can factor $pq^k\pi_1\varepsilon$ over $\mathcal{O}$ as $p\varepsilon_0^{-a} \cdot q^k\pi_1\varepsilon\varepsilon_0^a$ for a suitably chosen integer a. Here it is crucial there be *some* $\mathbb{Z}_K$-associate of $\pi_1\varepsilon$ belonging to $\mathcal{O}_p$, which is guaranteed by $h(\mathcal{O}_p) = 1$. □

The next two lemmas will be proved by analytic methods in §3.

Lemma 2.7 (assuming GRH)**.** *Let $K = \mathbb{Q}(\sqrt{2})$. For each positive integer h not divisible by 4, there are infinitely many primes p that are inert in K and have $h(\mathcal{O}_p) = h$.*

Lemma 2.8 (assuming GRH)**.** *Let $K = \mathbb{Q}(\sqrt{2})$. There are infinitely many primes p inert in K with $\gcd(p+1, 15) = 1$ and $h(\mathcal{O}_p) = 1$.*

We finish this section by showing how to complete the proof of Theorem 1.1 assuming Lemmas 2.7 and 2.8.

Lemma 2.9. *Let K be a quadratic field, and let p be an odd prime. Suppose $\eta \in \mathbb{Z}_K$ is congruent, modulo $p\mathbb{Z}_K$, to a rational integer that is relatively prime to p. If $\eta \in \mathcal{O}_{p^i} \setminus \mathcal{O}_{p^{i+1}}$, then $\eta^p \in \mathcal{O}_{p^{i+1}} \setminus \mathcal{O}_{p^{i+2}}$.*

Proof. By hypothesis, $\eta \in \mathcal{O}_p$ and so $i \geq 1$. Write $\eta = u + p^i\nu$, where $u \in \mathbb{Z}$ and $\nu \in \mathbb{Z}_K$. Then $\gcd(u,p) = 1$ and $\nu \notin \mathcal{O}_p$. Taking pth powers, $\eta^p = u^p + u^{p-1}p^{i+1}\nu + p^{2i+1}\gamma$ for some $\gamma \in \mathbb{Z}_K$. (We use here that p is odd.) Thus, $\eta^p \equiv u^p \pmod{p^{i+1}\mathbb{Z}_K}$, so that $\eta^p \in \mathcal{O}_{p^{i+1}}$. If $\eta^p \in \mathcal{O}_{p^{i+2}}$, then $u^p + u^{p-1}p^{i+1}\nu$ is congruent, mod $p^{i+2}\mathbb{Z}_K$, to some rational integer v. Necessarily $v \equiv u^p \pmod{p^{i+1}\mathbb{Z}}$ and $u^{p-1}\nu \equiv \frac{v-u^p}{p^{i+1}} \pmod{p\mathbb{Z}_K}$. Selecting $u' \in \mathbb{Z}$ as a multiplicative inverse of u mod p, we deduce that $\nu \equiv u'^{p-1}\frac{v-u^p}{p^{i+1}} \pmod{p\mathbb{Z}_K}$. Here the right-hand side lies in $\mathbb{Z}$, and so $\nu \in \mathcal{O}_p$ after all, a contradiction. □

Proof of Theorem 1.1. From the result of Halter-Koch alluded to in the introduction [HK95, Corollary 4], the elasticity ∞ occurs for any order whose conductor is divisible by a prime split in K. To see this, note that if p is any prime dividing the conductor f of $\mathcal{O}$, then $P := p\mathbb{Z} + f\mathbb{Z}_K$ is a prime ideal of $\mathcal{O}$, and every prime of $\mathbb{Z}_K$ that lies above p also lies above P. So if p is split in K, then there are two distinct prime ideals of $\mathbb{Z}_K$ lying above P, yielding $\rho(\mathcal{O}) = \infty$. (It is also possible to prove $\rho(\mathcal{O}) = \infty$ in these cases using Lemma 2.2.)

Now we turn to the finite elasticities. By Lemmas 2.5 and 2.7, each elasticity from $\{1, \frac{3}{2}, 2, \frac{5}{2}, \dots\}$ is realized infinitely often, except possibly those of the form $2m + \frac{1}{2}$, with $m \in \mathbb{Z}_{>0}$. To fill in these gaps we use Lemma 2.6.

Let u_k denote the unit index of $\mathcal{O}_{5^k}$. Then $u_1 = 3$, since $\varepsilon_0 = 1+\sqrt{2} \notin \mathcal{O}_5$ while $\varepsilon_0^3 = 7+5\sqrt{2} \in \mathcal{O}_5$. Now suppose that $k \geq 2$. Starting from $\varepsilon_0^3 \equiv 2 \pmod{5\mathbb{Z}_K}$ and $\varepsilon_0^3 \in \mathcal{O}_5 \setminus \mathcal{O}_{5^2}$, repeated application of Lemma 2.9 yields $\varepsilon_0^{3\cdot 5^{j-1}} \in \mathcal{O}_{5^j} \setminus \mathcal{O}_{5^{j+1}}$, for each $j = 1, 2, 3, \dots$. It follows that u_k divides $3 \cdot 5^{k-1}$ but does not divide $3 \cdot 5^{k-2}$, and so $u_k = 5^{k-1}$ or $u_k = 3 \cdot 5^{k-1}$. But $u_1 = 3$ is a divisor of u_k for every k, and so we must have $u_k = 3 \cdot 5^{k-1}$. Applying the relative class number formula, $h(\mathcal{O}_{5^k}) = 2$ for every positive integer k. Taking p as in the conclusion of Lemma 2.8, and applying Lemma 2.6 with $q = 5$, we find $\rho(\mathcal{O}_{5^k p}) = k + \frac{1}{2}$. Varying k and p completes the proof of the theorem. □

3. Orders in $\mathbb{Z}[\sqrt{2}]$ with inert prime conductor and prescribed class number: Proofs of Lemmas 2.7 and 2.8

Throughout this section, $K = \mathbb{Q}(\sqrt{D})$ (with D squarefree) is a real quadratic field with discriminant Δ and fundamental unit ε_0 of norm -1. For each rational prime p inert in K, we let

$$u = u(p) \text{ denote the unit index of } \mathcal{O}_p,$$
$$u' = u'(p) \text{ denote the order of } \eta := \varepsilon_0^2 \text{ viewed in the group } (\mathbb{Z}_K/p\mathbb{Z}_K)^\times.$$

While it is u that is directly relevant to the proof of Lemma 2.7, it is u' that our methods allow us to control. Fortunately, u and u' are easily related.

Since $\eta^{u'} = \varepsilon_0^{2u'} \equiv 1 \pmod{p\mathbb{Z}_K}$, we see that $\varepsilon_0^{u'} \equiv \pm 1 \pmod{p\mathbb{Z}_K}$, and so $u \mid u'$. To get a relation in the opposite direction, observe that $\varepsilon_0^u \equiv a \pmod{p\mathbb{Z}_K}$ for some rational integer a coprime to p, and hence $\eta^{u(p-1)/2} = (\varepsilon_0^u)^{p-1} \equiv 1 \pmod{p\mathbb{Z}_K}$. Thus, $u' \mid u\frac{p-1}{2}$. As p is inert in K, the Frobenius element in $\mathrm{Gal}(K/\mathbb{Q})$ corresponding to p is the nontrivial automomorphism of K. Therefore, $\eta^{p+1} \equiv \eta \cdot \eta^p \equiv \eta \cdot \tilde{\eta} \equiv N\eta \equiv 1 \pmod{p\mathbb{Z}_K}$. Hence, $u' \mid p+1$ and so $u' \mid \gcd(u\frac{p-1}{2}, p+1) \mid u\gcd(\frac{p-1}{2}, p+1) \mid 2u$. We conclude that u and u' share the same odd part.

To understand the 2-part of u, we take cases according to the residue class of p modulo 4. Notice that

$$(\varepsilon_0^{(p+1)/2})^2 \equiv \varepsilon_0 \cdot \varepsilon_0^p \equiv \varepsilon_0 \cdot \tilde{\varepsilon}_0 \equiv -1 \pmod{p\mathbb{Z}_K}.$$

If $p \equiv -1 \pmod 4$, then $\sqrt{-1} \notin \mathbb{F}_p$, and so $\varepsilon_0^{(p+1)/2} \notin \mathcal{O}_p$. So $u \mid p+1$ while $u \nmid \frac{p+1}{2}$, implying that the 2-part of u is the same as that of $p+1$. If $p \equiv 1 \pmod 4$, then $\sqrt{-1} \in \mathbb{F}_p$, and $\varepsilon_0^{(p+1)/2} \in \mathcal{O}_p$. Thus, u divides the odd number $\frac{p+1}{2}$, and u itself is odd.

With h as in Lemma 2.7, let h' denote the odd part of h. To prove Lemma 2.7 we will produce primes p, inert in K, satisfying

$$p \equiv -1 \pmod{h'}, \quad \text{where } u' \text{ has the same odd part as } \frac{p+1}{h'},$$

and also

$$p \equiv \begin{cases} -1 \pmod 4 & \text{if } h \text{ is odd (i.e., } h = h'), \\ 1 \pmod 4 & \text{if } h \text{ is even (i.e., } h = 2h'). \end{cases}$$

Our work in the last few paragraphs implies that $u = \frac{p+1}{h}$ for such primes p, and so $h(\mathcal{O}_p) = h$. Conversely, any prime p inert in K with $h(\mathcal{O}_p) = h$ satisfies these two displayed conditions.

The primes we seek will come out of an application of the (GRH-conditional) Chebotarev density theorem by adapting a method of Chen [Che02] (see also related work of Roskam [Ros00]). A very similar adaptation was carried out by [Kat03]; however Kataoka's main theorems control a quantity subtly different than the ones relevant to our work. Rather than attempt to shoehorn Kataoka's intermediate calculations into our narrative we have chosen to keep the exposition self-contained.

The following version of Chebotarev's theorem is taken from Serre's paper [Ser81]; let $K = \mathbb{Q}$ in equation 20_R there. Below, $\mathrm{Li}(x)$ denotes the logarithmic integral, defined by $\mathrm{Li}(x) = \int_2^x \mathrm{d}t/\log t$, while $\mathrm{Frob}_{L/\mathbb{Q},p}$ refers to the conjugacy class in $\mathrm{Gal}(L/\mathbb{Q})$ of Frobenius elements of primes above p.

Chebotarev density theorem (assuming GRH). *Let $L/\mathbb{Q}$ be a Galois extension, and let $\mathscr{C}$ be a subset of $\mathrm{Gal}(L/\mathbb{Q})$ stable under conjugation. For all $x \geq 2$,*

$$\#\{\textit{primes } p \leq x : \mathrm{Frob}_{L/\mathbb{Q},p} \subseteq \mathscr{C}\} = \frac{|\mathscr{C}|}{[L:\mathbb{Q}]}\mathrm{Li}(x) + O\left(|\mathscr{C}| x^{1/2} \log\left([L:\mathbb{Q}] x \prod_{\ell \mid \Delta_L} \ell\right)\right).$$

Here the implied constant is absolute.

All number fields appearing below will be subfields of $\mathbb{C}$. For each odd positive integer d coprime to Δ, we let

$$L_d = K(\zeta_d, \varepsilon_0^{1/d}).$$

Here and below, $\zeta_m = \exp(2\pi i/m)$, and roots of odd order of real numbers are understood as taking their real values.

Lemma 3.1. *Let d be an odd positive integer with $\gcd(d, \Delta) = 1$. Then $L_d/\mathbb{Q}$ is Galois with $[L_d : \mathbb{Q}] = 2d \cdot \varphi(d)$.*

Proof. Since $\varepsilon_0^{-1} = -\tilde{\varepsilon}_0$, we see that $\tilde{\varepsilon}_0^{1/d} = -1/\varepsilon_0^{1/d}$. So we can view L_d as the splitting field over $\mathbb{Q}$ of $(x^d - \varepsilon_0)(x^d - \tilde{\varepsilon}_0) = x^{2d} - \mathrm{Tr}(\varepsilon_0)x^d - 1$, implying that $L_d/\mathbb{Q}$ is Galois.

To compute the degree of this extension, we first observe that $K \subseteq \mathbb{Q}(\zeta_{|\Delta|})$ and that $\mathbb{Q}(\zeta_{|\Delta|})$ is linearly disjoint from $\mathbb{Q}(\zeta_d)$ (since $\gcd(d, \Delta) = 1$). Thus K is linearly disjoint from $\mathbb{Q}(\zeta_d)$ and $[K(\zeta_d) : K] = \varphi(d)$. Next, we claim that ε_0 is not an ℓth power in $K(\zeta_d)$ for any prime ℓ dividing d.

Suppose otherwise. Then $K(\varepsilon_0^{1/\ell}) \subseteq K(\zeta_d)$. Since $K(\zeta_d)$ is abelian over K, it must be that $K(\varepsilon_0^{1/\ell})$ is also abelian over K. Taking any $\sigma \in \mathrm{Gal}(K(\varepsilon_0^{1/\ell})/K)$, we see that $\frac{\sigma(\varepsilon_0^{1/\ell})}{\varepsilon_0^{1/\ell}}$ is a real ℓth root of 1, and so (as ℓ is odd) $\sigma(\varepsilon_0^{1/\ell}) = \varepsilon_0^{1/\ell}$. Since this holds for every σ, it must be that $\varepsilon_0^{1/\ell} \in K$. But this is absurd, since ε_0 is the fundamental unit of K. Now Capelli's characterization of irreducible binomials (see [Lan02, Theorem 9.1, p. 297]) implies that $x^d - \varepsilon_0$ is irreducible over $K(\zeta_d)$, so that

$$[L_d : \mathbb{Q}] = [K(\zeta_d, \varepsilon_0^{1/d}) : \mathbb{Q}] = [K(\zeta_d, \varepsilon_0^{1/d}) : K(\zeta_d)][K(\zeta_d) : K][K : \mathbb{Q}] = d \cdot \varphi(d) \cdot 2,$$

as desired. □

Write $\varepsilon_0 = \frac{1}{2}(u_0 + v_0\sqrt{D})$. It is important for the statement of our next lemma that every prime p not dividing dDv_0 is unramified in L_d. To prove this, notice that p is unramified in L_d whenever the polynomial $F_d(x) := x^{2d} - \mathrm{Tr}(\varepsilon_0)x^d - 1$ appearing in the proof of Lemma 3.1 has no multiple roots in $\bar{\mathbb{F}}_p$. If $p \nmid d$, each $\bar{\mathbb{F}}_p$-root of $F_d'(x)$ has $2x^d = \mathrm{Tr}(\varepsilon_0) = u_0$, and so for x to also be a root of $F_d(x)$ requires $4 + u_0^2 = Dv_0^2$ to vanish mod p.

The following lemma paves the way for an application of Chebotarev's theorem. (Compare with [Che02, Lemma 1.4].) Let σ_0 denote the nontrivial automorphism of $K/\mathbb{Q}$, and let τ denote complex conjugation. For each odd positive integer d with $\gcd(d, \Delta) = 1$, we let

$$\mathscr{C}_d = \{\sigma \in \mathrm{Gal}(L_d/\mathbb{Q}) : \sigma|_K = \sigma_0, \sigma|_{\mathbb{Q}(\zeta_d)} = \tau|_{\mathbb{Q}(\zeta_d)}, \sigma^2 = \mathrm{id.}\}$$

It is straightforward to check that $\mathscr{C}_d$, viewed as a subset of $\mathrm{Gal}(L_d/\mathbb{Q})$, is stable under conjugation.

Lemma 3.2. *Let d be an odd positive integer with $\gcd(d, \Delta) = 1$. The following are equivalent for primes p not dividing dDv_0:*

(i) *p is inert in K, $p \equiv -1 \pmod{d}$, and $\eta^{\frac{p+1}{d}} \equiv 1 \pmod{p\mathbb{Z}_K}$,*

(ii) $\mathrm{Frob}_{L_d/\mathbb{Q},p} \subseteq \mathscr{C}_d$.

Proof. Suppose (i) holds, and let $\sigma \in \mathrm{Frob}_{L_d/\mathbb{Q},p}$. Since p is inert in K, we have that $\sigma|_K \in \mathrm{Frob}_{K/\mathbb{Q},p} = \{\sigma_0\}$. So $\sigma|_K = \sigma_0$. Moreover, $\sigma|_{\mathbb{Q}(\zeta_d)} \in \mathrm{Frob}_{\mathbb{Q}(\zeta_d)/\mathbb{Q},p}$, so that (recalling $p \equiv -1 \pmod{d}$)

$$\sigma|_{\mathbb{Q}(\zeta_d)}(\zeta_d) = \zeta_d^p = \zeta_d^{-1} = \tau(\zeta_d);$$

hence, $\sigma|_{\mathbb{Q}(\zeta_d)} = \tau|_{\mathbb{Q}(\zeta_d)}$. To show $\sigma^2 = \mathrm{id.}$ it suffices, in view of what has already been shown, to check that σ^2 acts trivially on $\eta^{1/d}$.

Let P be a prime of L_d lying above p for which σ is the Frobenius element of P. Then

$$\eta^{1/d}\sigma(\eta^{1/d}) \equiv \eta^{1/d} \cdot (\eta^{1/d})^p \equiv (((\eta)^{1/d})^d)^{\frac{p+1}{d}} \equiv \eta^{\frac{p+1}{d}} \equiv 1 \pmod{P}.$$

Applying σ once again yields $\sigma(\eta^{1/d})\sigma^2(\eta^{1/d}) \equiv 1 \pmod{P}$, which compared with the previous congruence shows

$$\sigma^2(\eta^{1/d}) \equiv \eta^{1/d} \pmod{P}. \tag{3}$$

It remains to promote the congruence (3) to an equality of elements. Notice that $(\sigma^2(\eta^{1/d}))^d = \sigma^2(\eta) = \eta$, so that $\sigma^2(\eta^{1/d}) = \zeta_d^a\eta^{1/d}$ for some rational integer a. So from (3), P contains $\eta^{1/d}(\zeta_d^a - 1)$ and so also contains $1 - \zeta_d^a$ (since $\eta^{1/d}$ is a unit). Thus, either $\zeta_d^a = 1$ or P contains $\prod_{a'=1}^{d-1}(1 - \zeta_d^{a'}) = d$. But P lies above p and $p \nmid d$. Hence, $\zeta_d^a = 1$ and $\sigma^2(\eta^{1/d}) = \eta^{1/d}$, which completes the proof that (i) implies (ii).

Now suppose (ii) holds, and let $\sigma \in \mathrm{Frob}_{L_d/\mathbb{Q},p}$. Starting from $\sigma|_K = \sigma_0$ and $\sigma|_{\mathbb{Q}(\zeta_d)} = \tau|_{\mathbb{Q}(\zeta_d)}$, the reasoning from the first paragraph of the proof (now in reverse) gives that p is inert in K and that $p \equiv -1 \pmod{d}$. Continuing, $(\sigma(\eta^{1/d}))^d = \sigma(\eta) = \tau(\eta) = 1/\eta$. Thus, $\sigma(\eta^{1/d}) = \zeta_d^a/\eta^{1/d}$, for some integer a, and

$$\eta^{1/d} = \sigma^2(\eta^{1/d}) = \sigma(\zeta_d^a)/\sigma(\eta)^{1/d} = \zeta_d^{-a} \cdot \eta^{1/d}/\zeta_d^a = \zeta_d^{-2a}\eta^{1/d}.$$

Hence, $\zeta_d^{2a} = 1$ and (as d is odd) also $\zeta_d^a = 1$, so that $\sigma(\eta^{1/d}) = 1/\eta^{1/d}$. Letting P be a prime of L_d above p having σ as its Frobenius,

$$\eta^{\frac{p+1}{d}} \equiv \eta^{1/d}\sigma(\eta^{1/d}) \equiv 1 \pmod{P}.$$

Since $P \cap \mathbb{Z}_K = p\mathbb{Z}_K$, it follows that $\eta^{(p+1)/d} \equiv 1 \pmod{p\mathbb{Z}_K}$, finishing the proof that (ii) implies (i). □

Lemma 3.3. *$|\mathscr{C}_d| = 1$ for every odd positive integer d coprime to Δ.*

Proof. Since K and $\mathbb{Q}(\zeta_d)$ are linearly disjoint with composite $K(\zeta_d)$, we have an isomorphism

$$\begin{aligned}\mathrm{Gal}(K(\zeta_d)/\mathbb{Q}) &\xrightarrow{\sim} \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \\ \sigma &\mapsto (\sigma|_K, \sigma|_{\mathbb{Q}(\zeta_d)}).\end{aligned}$$

So there is a unique $\sigma_1 \in \mathrm{Gal}(K(\zeta_d)/\mathbb{Q})$ for which $\sigma_1|_K = \sigma_0$ and $\sigma_1|_{\mathbb{Q}(\zeta_d)} = \tau|_{\mathbb{Q}(\zeta_d)}$.

The elements of $\mathscr{C}_d$ are precisely those lifts σ of σ_1 to an automorphism of L_d satisfying $\sigma^2 = \mathrm{id}$. Each lift to L_d has $\sigma(\varepsilon_0^{1/d})^d = \sigma(\varepsilon_0) = \tau(\varepsilon_0) = -1/\varepsilon_0$ and thus $\sigma(\varepsilon_0^{1/d}) = -\zeta_d^a/\varepsilon_0^{1/d}$, for some integer a determined mod d. Moreover, as $[L_d : K(\zeta_d)] = d$, each choice of a mod d corresponds to a unique lift σ. Since

$$\sigma^2(\varepsilon_0^{1/d}) = \sigma(-\zeta_d^a/\varepsilon_0^{1/d}) = \varepsilon_0^{1/d}\zeta_d^{-2a},$$

to satisfy $\sigma^2 = \mathrm{id}$. we must select the unique lift corresponding to $a \equiv 0 \pmod{d}$. □

Proof of Lemma 2.7. We let $K = \mathbb{Q}(\sqrt{2})$, which has discriminant $\Delta = 8$ and fundamental unit $\varepsilon_0 = 1 + \sqrt{2}$. Then $\gcd(d, \Delta) = 1$ for all odd d and the fields L_d are unramified away from the primes dividing $2d$.

As above we let h' denote the odd part of h. We set $\delta = -1$ if h is odd and $\delta = 1$ if h is even. A prime p inert in K has $h(\mathcal{O}_p) = h$ precisely when

(i) $p \equiv \delta \pmod{4}$,

(ii) u' and $\frac{p+1}{h'}$ share the same odd part.

We can rephrase (ii) as the requirement that h' be the odd part of $\frac{p+1}{u'}$. Actually, it is more convenient to work with the weaker condition

(ii′) h' is the largest odd factor of the y-smooth part of $\frac{p+1}{u'}$, where $y := \log x$.

(Recall that the y-smooth part of a positive integer is its largest divisor supported on primes not exceeding y.) It will turn out that the difference between requiring (ii) and (ii′) is negligible.

Let $P^+(n)$ stand for the largest prime factor of n, with the convention that $P^+(1) = 1$. Assume x is large enough that $P^+(h) \le y$. By inclusion-exclusion, we can write the count of inert $p \le x$

satisfying (i) and (ii′) as

$$\sum_{\substack{p\le x\\ p \text{ inert}\\ p\equiv\delta \pmod 4\\ h'\mid \frac{p+1}{u'}}} \sum_{\substack{d \text{ odd}\\ P^+(d)\le y\\ d\mid \frac{p+1}{u'h'}}} \mu(d) = \sum_{\substack{d \text{ odd}\\ P^+(d)\le y}} \mu(d) \sum_{\substack{p\le x\\ p \text{ inert}\\ p\equiv\delta \pmod 4\\ dh'\mid \frac{p+1}{u'}}} 1. \tag{4}$$

Let us work on the inner sum. For primes p inert in K with p not dividing $2dh'$,

$$\begin{aligned} dh' \mid \frac{p+1}{u'} &\iff p\equiv -1 \pmod{dh'} \text{ and } u' \mid \frac{p+1}{dh'}\\ &\iff p\equiv -1 \pmod{dh'} \text{ and } \eta^{\frac{p+1}{dh'}}\equiv 1 \pmod{p\mathbb{Z}_K} \iff \mathrm{Frob}_{L_{dh'}/\mathbb{Q},\,p}\in \mathscr{C}_{dh'}, \end{aligned}$$

using Lemma 3.2 for the last equivalence. The condition $p\equiv\delta \pmod 4$ can also be treated as a Frobenius condition; it says that $\mathrm{Frob}_{\mathbb{Q}(i)/\mathbb{Q},\,p}$ is a certain singleton conjugacy class in $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

We can detect the primes that simultaneously satisfy both Frobenius conditions by working in the composite field L of $L_{dh'}$ and $\mathbb{Q}(i)$. We use here that the fields $\mathbb{Q}(i)$ and $L_{dh'}$ are linearly disjoint. Otherwise, $i\in L_{dh'}=K(\zeta_{dh'},\varepsilon_0^{1/dh'})$. Since $L_{dh'}/K(\zeta_{dh'})$ is an extension of odd degree (in fact, degree dividing dh'), it must be that $i\in K(\zeta_{dh'})$, so that $K(\zeta_{dh'})=K(i,\zeta_{dh'})$. But $[K(\zeta_{dh'}):\mathbb{Q}]=2\varphi(dh')$ whereas

$$[K(i,\zeta_{dh'}):\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},i,\zeta_{dh'}):\mathbb{Q}]=[\mathbb{Q}(\zeta_8,\zeta_{dh'}):\mathbb{Q}]=[\mathbb{Q}(\zeta_{8dh'}):\mathbb{Q}]=\varphi(8dh')=4\varphi(dh'),$$

a contradiction. This allows us to combine our conditions on $\mathrm{Frob}_{L_{dh'},\,p}$ and $\mathrm{Frob}_{\mathbb{Q}(i)/\mathbb{Q},\,p}$ into the single restriction that $\mathrm{Frob}_{L,\,p}$ be a certain singleton conjugacy class of $\mathrm{Gal}(L/\mathbb{Q})$.

Since $[L:\mathbb{Q}]=2[L_{dh'}:\mathbb{Q}]=4dh'\varphi(dh')$ and every prime that ramifies in L divides $2dh'$, the GRH-conditional Chebotarev theorem yields

$$\sum_{\substack{p\le x\\ p \text{ inert}\\ p\equiv\delta \pmod 4\\ dh'\mid \frac{p+1}{u}}} 1 = \frac{1}{4dh'\varphi(dh')}\mathrm{Li}(x)+O(x^{1/2}\log(dx)). \tag{5}$$

Here and below, we suppress the dependence of implied constants on the fixed parameter h.

We now insert (5) back into (4). The total contribution of the O-terms is at most $x^{\frac12+o(1)}$. Indeed, each d with $P^+(d)\le y$ and $\mu(d)\neq 0$ has $d\le\prod_{\ell \text{ prime}\le y}\ell = x^{1+o(1)}$ and $x^{1/2}\log(dx)=x^{\frac12+o(1)}$, while the number of such d does not exceed $2^{\pi(y)}=x^{o(1)}$. The main term is given by

$$\frac{\mathrm{Li}(x)}{4h'}\sum_{\substack{d \text{ odd}\\ P^+(d)\le y}}\frac{\mu(d)}{d\varphi(dh')} = \frac{\mathrm{Li}(x)}{4h'\varphi(h')}\sum_{\substack{d_1 \text{ odd}\\ P^+(d_1)\le y\\ \gcd(d_1,h)=1}}\frac{\mu(d_1)}{d_1\varphi(d_1)}\sum_{\substack{d_2 \text{ odd}\\ \ell\mid d_2\Rightarrow \ell\mid h}}\frac{\mu(d_2)}{d_2^2}.$$

Here

$$\sum_{\substack{d_1 \text{ odd}\\ P^+(d_1)\le y\\ \gcd(d_1,h)=1}}\frac{\mu(d_1)}{d_1\varphi(d_1)} = \prod_{\substack{2<p\le y\\ p\nmid h}}\left(1-\frac{1}{p(p-1)}\right) = \left(\prod_{p>2,\ p\nmid h}\left(1-\frac{1}{p(p-1)}\right)\right)\cdot(1+O(1/\log x))$$

while

$$\sum_{\substack{d_2 \text{ odd} \\ \ell | d_2 \Rightarrow \ell | h}} \frac{\mu(d_2)}{d_2^2} = \prod_{p | h'} \left(1 - \frac{1}{p^2}\right).$$

Piecing everything together, and keeping in mind that $\mathrm{Li}(x) = x/\log x + O(x/(\log x)^2)$, we conclude that the count of inert primes $p \le x$ satisfying (i) and (ii′) is

$$C_h \frac{x}{\log x} + O\left(\frac{x}{(\log x)^2}\right)$$

for a certain positive constant C_h (expressible as an Euler product).

It remains to account for the difference between conditions (ii) and (ii′). If p satisfies (ii′) but not (ii), then $\frac{p+1}{u'}$ has a prime factor $\ell > y$. We proceed to show that such p are rare by considering different ranges for ℓ.

Given a prime ℓ, we can bound the number of inert $p \le x$ for which $\ell \mid \frac{p+1}{u'}$ via the Chebotarev density theorem. (This is almost the same application of Chebotarev we had above, but now ℓ replaces dh', and there is no need to bring $\mathbb{Q}(i)$ into the picture since we do not care about p mod 4.) We find that the count of such p is

$$\ll \frac{\mathrm{Li}(x)}{\ell\varphi(\ell)} + x^{1/2}\log(\ell x) \ll \frac{\mathrm{Li}(x)}{\ell^2} + x^{1/2}\log(\ell x).$$

We use this estimate in the range $y < \ell \le x^{1/2}/(\log x)^2$. Summing on ℓ from this interval, we conclude that $\frac{p+1}{u'}$ has a prime factor ℓ from here for only $O(x/(\log x)^2)$ inert primes $p \le x$.

Next, we handle the range $x^{1/2}/(\log x)^2 < \ell \le x^{1/2}(\log x)^2$. If $\frac{p+1}{u'}$ is divisible by such an ℓ, then certainly $p \equiv -1 \pmod{\ell}$. For a given ℓ, the Brun–Titchmarsh inequality guarantees that there are $\ll x/\ell \log x$ corresponding $p \le x$. Summing on ℓ gives an upper bound of $O(\frac{x}{(\log x)^2}\log\log x)$.

Finally, suppose $\frac{p+1}{u'}$ is divisible by an $\ell > x^{1/2}(\log x)^2$. Then $u' < 2x^{1/2}/(\log x)^2$. Hence, $\eta^j \equiv 1 \pmod{p\mathbb{Z}_K}$ for some $j < 2x^{1/2}/(\log x)^2$ and

$$p \text{ divides } \prod_{1 \le j < 2x^{1/2}/(\log x)^2} N(1 - \eta^j), \quad \text{over } \mathbb{Z}.$$

Each term in the product is a nonzero integer and the jth term has absolute value $\exp(O(j))$. So the product has absolute value $\exp(O(x/(\log x)^4))$ and thus only $O(x/(\log x)^4)$ prime divisors.

Assembling the above estimates, there are only $O(x(\log\log x)/(\log x)^2)$ inert primes $p \le x$ obeying (ii′) but not (ii). We conclude that the number of inert $p \le x$ with $h(\mathcal{O}_p) = h$ is $C_h x/\log x + O(x\log\log x/(\log x)^2)$. We let x tend to infinity to finish the proof of the lemma. □

Proof of Lemma 2.8. Again we take $K = \mathbb{Q}(\sqrt{2})$. The primes p inert in K are precisely those $p \equiv 3, 5 \pmod 8$. We sift the primes $p \equiv 3 \pmod 8$, $p \le x$, removing those for which $p+1$ has an odd prime factor at most $y := \log\log x$. By the Siegel–Walfisz theorem, the number of surviving

primes is

$$\sum_{\substack{p\le x\\ p\equiv 3 \pmod 8}} \sum_{\substack{d\mid p+1\\ d \text{ odd}\\ P^+(d)\le y}} \mu(d) = \sum_{\substack{d \text{ odd}\\ P^+(d)\le y}} \mu(d)\left(\frac{\mathrm{Li}(x)}{\varphi(8d)} + O(x/(\log x)^{100})\right)$$
$$= \frac{\mathrm{Li}(x)}{4} \prod_{\substack{2<\ell\le y\\ \ell \text{ prime}}} \left(\frac{\ell-2}{\ell-1}\right) + O(x/(\log x)^{99}),$$

which is $\gg \frac{1}{\log y}\frac{x}{\log x}$ for large x. Certainly $\gcd(p+1, 15) = 1$ for all these p once $y \ge 5$.

We claim that almost all the remaining p are such that the odd part of u' and the odd part of $p+1$ coincide. Since u and u' share the same odd part, and the 2-part of u agrees with the 2-part of $p+1$ when $p \equiv 3 \pmod 4$, we find $u = p+1$ and $h(\mathcal{O}_p) = 1$. So once the claim is proved, we will have produced many primes satisfying the conclusion of Lemma 2.8.

If p survives the sieving process but the odd part of u' is smaller than the odd part of $p+1$, then there is a prime $\ell > y$ dividing $\frac{p+1}{u'}$. The number of p corresponding to an ℓ with $y < \ell \le x^{1/2}/(\log x)^2$ is (as in the last proof)

$$\ll \sum_{y<\ell\le x^{1/2}/(\log x)^2} \left(\frac{\mathrm{Li}(x)}{\ell^2} + x^{1/2}\log(\ell x)\right) \ll \frac{1}{y}\frac{x}{\log x},$$

which is of smaller order than $\frac{1}{\log y}\frac{x}{\log x}$. The number of p corresponding to an $\ell > x^{1/2}/(\log x)^2$ is $O(x \log\log x/(\log x)^2)$ (again, by the reasoning of the last proof), and this is also $o(\frac{1}{\log y}\frac{x}{\log x})$. □

4. Discussion of Conjecture 1.2

We do not know how to prove Conjecture 1.2, even assuming GRH. But we can show that Conjecture 1.2 follows from GRH coupled with a hypothesis on the distribution of certain quadratic field analogues of Wieferich primes.

Recall that a (rational) prime p is a Wieferich prime if $p^2 \mid 2^{p-1} - 1$. The only known Wieferich primes are 1093 and 3511, and it has been checked that there are no others below 10^{17}. It seems likely that the set of Wieferich primes is infinite but that its counting function tends to infinity too gradually for mortals of the present age to observe. In fact, Crandall, Dilcher, and Pomerance [CDP97] conjecture that the count of Wieferich primes up to x is $\sim \log\log x$, as $x \to \infty$.

Let K be a real quadratic field with discriminant Δ and fundamental unit ε_0. For each rational prime p,

$$\varepsilon_0^{p-\left(\frac{\Delta}{p}\right)} \in \mathcal{O}_p.$$

We say p is K-Wieferich of type 1 if p is split in K and $\varepsilon_0^{p-1} \in \mathcal{O}_{p^2}$, and we say p is K-Wieferich of type -1 if if p is inert in K and $\varepsilon_0^{p+1} \in \mathcal{O}_{p^2}$. For example, 13 (type -1) and 31 (type $+1$) are $\mathbb{Q}(\sqrt{2})$-Wieferich, since

$$(1+\sqrt{2})^{14} = 114243 + 13^2 \cdot 478\sqrt{2}, \quad \text{and} \quad (1+\sqrt{2})^{30} = 152139002499 + 31^2 \cdot 111944350\sqrt{2}.$$

A short `gp/PARI` script verifies that $13, 31$, and 1546463 (type 1) are the only $\mathbb{Q}(\sqrt{2})$-Wieferich primes up to 10^7.

Plausibly the count of K-Wieferich primes is $\sim \log\log x$, as $x \to \infty$, for each fixed real quadratic field K. The following radically more conservative conjecture suffices for our purposes.

Conjecture 4.1. *For every fixed real quadratic field K, the limiting proportion of K-Wieferich primes is 0%. More precisely, the count of K-Wieferich primes up to x is $o(x/\log x)$, as $x \to \infty$.*

The rest of this section is devoted to the proof of the following proposition.

Proposition 4.2. *Conjecture 1.2 follows from Conjecture 4.1 and GRH.*

Proof. Halter-Koch's [HK95, Corollary 4] implies that the elasticity ∞ is realized by all orders $\mathcal{O}_{pm}$ ($m = 1, 2, 3, \dots$), for any prime p that splits in K. (And Chebotarev's density theorem furnishes an endless supply of such p.) So we focus on the finite elasticities in $\mathscr{E}$.

Let $\delta \in \{\pm 1\}$. We will show below that there are $\gg x/\log x$ odd primes $p \le x$ that are inert in K, satisfy $p \equiv \delta \pmod 4$, and have the odd part of u' equal to the odd part of $p+1$. By Conjecture 4.1, this lower bound will continue to hold if we throw away p that are K-Wieferich.

Suppose the claim to be proved. If $\delta = -1$, then $u = p+1$ for each of our primes p. Since p is not K-Wieferich, $\mathcal{O}_{p^k}$ has unit index $(p+1)p^{k-1}$, for every $k = 1, 2, \dots$ (apply Lemma 2.9). Thus $h(\mathcal{O}_{p^k}) = 1$, so that Lemma 2.5 gives $\rho(\mathcal{O}_{p^k}) = k$. If $\delta = 1$, then $u = \frac{p+1}{2}$ and $\mathcal{O}_{p^k}$ has unit index $\frac{1}{2}(p+1)p^{k-1}$ for each k. Hence, $h(\mathcal{O}_{p^k}) = 2$ and Lemma 2.5 gives $\rho(\mathcal{O}_{p^k}) = k + \frac{1}{2}$. Varying δ, p, and k completes the proof of Conjecture 1.

It remains to prove the claimed estimate. We borrow some ideas from [Pol24, §3] (which in turn draws from Heath-Brown's paper [HB86]).

Write $K = \mathbb{Q}(\sqrt{D})$ with D squarefree. The fields K, $\mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-1})$ are linearly disjoint: Otherwise, there are three integers $a_1, a_2, a_3 \in \{0, 1\}$, not all 0, with

$$D^{a_1}(-3)^{a_2}(-1)^{a_3} \in (\mathbb{Q}^\times)^2.$$

Since D is not a square, at least one of a_1 and a_2 is nonzero. Then to have $D^{a_1}(-3)^{a_2}(-1)^{a_3} > 0$, it must be that $a_2 = a_3 = 1$. So $3D^{a_1} \in (\mathbb{Q}^\times)^2$, implying that $D = 3$ and $K = \mathbb{Q}(\sqrt{3})$. But then $\varepsilon_0 = 2 + \sqrt{3}$ has norm 1 rather than -1.

By the Chebotarev density theorem, we can choose a prime p_0 inert in K with $p_0 \equiv 1 \pmod 3$ and $p_0 \equiv \delta \pmod 4$; here the mod 3 and mod 4 conditions are to be viewed as splitting conditions on p in $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(i)$, respectively. For each odd prime q dividing D, let $u_q = p_0$ or $4p_0$, chosen so that $q \nmid 1 + u_q$. (This is clearly possible for $q > 3$, while the congruence $p_0 \equiv 1 \pmod 3$ ensures there is no obstruction for $q = 3$.) Choose $U \in \mathbb{Z}$ so that

$$U \equiv u_q \pmod q \quad \text{for all odd primes } q \mid D, \quad \text{and} \quad U \equiv p_0 \pmod 8,$$

and put $V = 8D$. Then $\gcd(U, V) = 1$, while $U + 1$ and V share no odd prime factors.

We now consider primes $p \equiv U \pmod V$. Certainly each such $p \equiv p_0 \equiv \delta \pmod 4$. We can also show that $\left(\frac{\Delta}{p}\right) = -1$, so that p is inert in K. To prove this last claim, recall that Δ can be factored as a product of prime discriminants $-4, \pm 8$, and $(-1)^{(\ell-1)/2}\ell$ for prime numbers ℓ. So it suffices to show that $\left(\frac{\Delta^*}{p_0}\right) = \left(\frac{\Delta^*}{p}\right)$ for each prime discriminant Δ^*. For $\Delta^* \in \{-4, \pm 8\}$, this follows from $p \equiv U \equiv p_0 \pmod 8$. For $\Delta^* = (-1)^{(\ell-1)/2}\ell$, we have $\left(\frac{\Delta^*}{p}\right) = \left(\frac{p}{\ell}\right)$; as $p \equiv p_0$ or $4p_0$ modulo ℓ, the symbol $\left(\frac{p}{\ell}\right) = \left(\frac{p_0}{\ell}\right) = \left(\frac{\Delta^*}{p_0}\right)$.

In what follows, we assume $x \geq 3$ and that y is a real parameter with $P^+(|\Delta|) \leq y \leq \log x$. Implied constants are to be understood as uniform in these x, y. We suppress the dependence of these constants on K.

We sift the primes $p \equiv U \pmod V$, removing those for which $p+1$ has an odd prime factor not exceeding y. Since $\gcd(U+1, V)$ has no odd prime factors, it is enough to carry out the sieve with the odd primes up to y that do not divide V. Proceeding as in the last section, the Siegel–Walfisz theorem gives that the count N_1 (say) of remaining $p \leq x$ satisfies $N_1 \gg \frac{1}{\log y}\frac{x}{\log x}$, as soon as x exceeds a certain constant depending only on K. Furthermore, reasoning as in the proofs of Lemmas 2.7 and 2.8, the number N_2 (say) of these p for which the odd part of u' is smaller than that of $p+1$ is

$$\ll \frac{1}{y}\frac{x}{\log x} + \frac{x \log\log x}{(\log x)^2}.$$

(To carry out the Chebotarev argument here, we use that primes ℓ exceeding y are coprime to Δ, so that Lemmas 3.1–3.3 all apply when $d = \ell$.) Now choosing y as a sufficiently large constant (depending only on K), we see that $N_1 > 2N_2$ for all x large enough in terms of K. Hence, $N_1 - N_2 \gg N_1 \gg x/\log x$. This completes the proof of the claimed estimate and also of Proposition 4.2. □

Remarks. Several questions about elasticities of general quadratic orders seem worthy of further investigation. For instance, is it true that for every real quadratic field K, the set of elasticities realized by infinitely many orders of K is cofinite in $\mathcal{E}$? This does not seem easy but is perhaps attackable assuming GRH and Conjecture 4.1.

If K is imaginary quadratic, it is not hard to show that each elasticity is attained by at most finitely orders of K. To fix ideas, let $K = \mathbb{Q}(i)$, and let $\mathcal{E}'$ be the set of elasticities of orders in K. Can one prove or disprove either of the following two assertions: (a) $\mathcal{E}'$ is cofinite in $\mathcal{E}$, (b) (in the opposite direction) the number of elements of $\mathcal{E}'$ not exceeding x is $o(x)$, as $x \to \infty$?

Acknowledgements

The author is supported by NSF Award DMS-2001581. Thanks are owed to Komal Agrawal for valuable discussions around Chen's arguments in [Che02], and to the referee for their careful review of the manuscript and numerous helpful suggestions.

References

[AA92] D. D. Anderson and D. F. Anderson, *Elasticity of factorizations in integral domains*, J. Pure Appl. Algebra **80** (1992), 217–235.
[Ala16] M. Alan, *Half-factorial domains and quadratic orders*, Int. J. Number Theory **12** (2016), 465–472.
[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.
[CDP97] R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449.
[Che02] Y.-M. J. Chen, *On primitive roots of one-dimensional tori*, J. Number Theory **93** (2002), 23–33.
[Coh80] H. Cohn, *Advanced number theory*, Dover Publications, Inc., New York, 1980.
[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.

[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.
[HB86] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), 27–38.
[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.
[HK20] ———, *An invitation to algebraic numbers and algebraic functions*, CRC Press, Boca Raton, FL, 2020.
[Kat03] N. Kataoka, *The distribution of prime ideals in a real quadratic field with units having a given index in the residue class field*, J. Number Theory **101** (2003), 349–375.
[Lan02] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
[Nar95] W. Narkiewicz, *A note on elasticity of factorizations*, J. Number Theory **51** (1995), 46–47.
[PL01] M. Picavet-L'Hermitte, *Weakly factorial quadratic orders*, Arab. J. Sci. Eng. Sect. C Theme Issues (Commutative algebra) **26** (2001), 171–186.
[Pol24] P. Pollack, *Half-factorial real quadratic orders*, Arch. Math. (Basel) **122** (2024), 491–500.
[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.
[Ser81] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401.
[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.
[Web82] H. Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Ann. **20** (1882), 301–329.

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

Email address: pollack@uga.edu