HALF-FACTORIAL REAL QUADRATIC ORDERS

PAUL POLLACK

In memory of Kevin James.

ABSTRACT. Recall that D is a half-factorial domain (HFD) when D is atomic and every equation $\pi_1 \cdots \pi_k = \rho_1 \cdots \rho_\ell$, with all π_i and ρ_j irreducible in D, implies $k = \ell$. We explain how techniques introduced to attack Artin's primitive root conjecture can be applied to understand half-factoriality of orders in real quadratic number fields. In particular, we prove that (a) there are infinitely many real quadratic orders that are half-factorial domains, and (b) under the Generalized Riemann Hypothesis, $\mathbb{Q}(\sqrt{2})$ contains infinitely many HFD orders.

1. INTRODUCTION

A half-factorial domain (HFD) is an integral domain D where every nonzero nonunit factors as a product of irreducibles and where any two factorizations of the same element have the same length. To spell out the second requirement more precisely, whenever we have an equation

$$\pi_1 \cdots \pi_k = \rho_1 \cdots \rho_\ell,$$

with all the π_i and ρ_j irreducible in D, we insist that $k = \ell$. Half-factorial domains first appear in a 1960 paper of Carlitz [Car60] where it is shown that the ring of integers of a number field K is an HFD if and only if the class number of K is at most 2. So for instance, $\mathbb{Z}[\sqrt{-5}]$ — which appears in introductory algebra courses as the example *par excellence* of nonunique factorization — is an HFD.

The term "half-factorial domain" is due to Zaks [Zak76, Zak80], who was the first to single out these rings as forming a class deserving study in its own right. Zaks observes in [Zak76] that HFDs, unlike UFDs, need not be integrally closed. He offers the example of $\mathbb{Z}[\sqrt{-3}]$ (details are deferred to [Zak80]).

To continue the discussion it is convenient to have available some standard notation and terminology. Let K be a quadratic field. An order in K is a subring of $\mathcal{O}_K$ that contains a $\mathbb{Q}$-basis for K. Write $K = \mathbb{Q}(\sqrt{d})$, d squarefree, and let $\omega = \omega_d = \sqrt{d}$ if $d \equiv 2, 3 \pmod 4$ and $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \pmod 4$. It can be shown that the distinct orders in $\mathbb{Q}(\sqrt{d})$ are the rings $\mathbb{Z}[f\omega]$, for $f = 1, 2, 3 \ldots$ (see pp. 45–48 of [Coh80]). Here taking $f = 1$ recovers $\mathcal{O}_K$, the so-called maximal order. The integer f is referred to as the conductor or index. For example, $\mathbb{Z}[\sqrt{-3}]$ is the order of index 2 inside $\mathbb{Q}(\sqrt{-3})$.

Several authors have investigated when quadratic orders are HFDs. See for instance [HK83] (the results of which are reproduced in [GHK06, pp. 226–229]), [Coy01], [Ala16], and [CMO17]. For imaginary orders, there is surprisingly little to say: $\mathbb{Z}[\sqrt{-3}]$ is the unique nonmaximal example! (This striking result appears as [Coy01, Theorem 2.3].) The real quadratic situation is more complicated.

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

Suppose that K is a real quadratic field. From either [HK83] or [Coy01], if K contains any HFD orders, then K has class number 1 or 2. Furthermore, the index of any HFD order is either p, with p prime, or $2p$, with p an odd prime.

Now fix a real quadratic field K of class number 1 or 2. In [Coy01], Coykendall gives a necessary and sufficient condition for the conductor p order in K to be an HFD. Let ε be the fundamental unit of K. Then $\mathbb{Z}[p\omega]$ is half-factorial if and only if

(i) p is inert in K,

(ii) the least positive integer j with $\varepsilon^j \in \mathbb{Z}[p\omega]$ is $j = p + 1$.

(See Theorems 3.8, 4.2, and Example 3 of [Coy01].) Later, Alan [Ala16] showed that for odd primes p, (i) and (ii) imply

(iii) ε has norm -1,

(iv) $p \equiv -1 \pmod 4$.

To illustrate, suppose we are looking for HFD orders inside $K = \mathbb{Q}(\sqrt{2})$. Note that the fundamental unit $\varepsilon = 1 + \sqrt{2}$ of K has norm -1, so there is no contradiction to condition (iii). From (i) and (iv), in order that $\mathbb{Z}[p\sqrt{2}]$ be an HFD it is necessary that $p \equiv 3 \pmod 8$. Thus, we are led to restrict attention to primes $p \equiv 3 \pmod 8$ and to ask how often such primes satisfy (ii).

In [Ala16], Alan reports on computations suggesting (ii) holds for approximately 75% of primes $p \equiv 3 \pmod 8$. Both Alan and Coykendall ask whether or not it can be proved that (ii) holds infinitely often. Our first theorem answers this question in the affirmative, under the assumption of the Generalized Riemann Hypothesis (GRH).[1] Let $A = \prod_{q \text{ prime}}(1 - \frac{1}{q(q-1)})$ be the Artin constant.

Theorem 1 (conditional on GRH). *There are infinitely many primes $p \equiv 3 \pmod 8$ for which $\mathbb{Z}[p\sqrt{2}]$ is an HFD. In fact,*

$$\#\{p \le x : p \equiv 3 \pmod 8,\ \mathbb{Z}[p\sqrt{2}] \text{ is an HFD}\} \sim \frac{1}{2}A \cdot \frac{x}{\log x}, \quad \text{as } x \to \infty. \tag{1}$$

Since $A = 0.3739558\dots$, and asymptotically 25% of primes are 3 mod 8, the limiting proportion of $p \equiv 3 \pmod 8$ for which $\mathbb{Z}[p\sqrt{2}]$ is an HFD is $\approx 74.8\%$, in line with what Alan found experimentally.

The proof of Theorem 1, given in §2, uses a method of Chen [Che02] developed to study of Artin's primitive root conjecture in quadratic fields. (Closely related results were published by Roskam a bit earlier [Ros00].) In fact, Chen's results are a stone's throw away from immediately implying Theorem 1, and so our discussion in §2 is more in the nature of a sketch rather than a full proof.

It was conjectured by Coykendall ([Coy01]; see also [Coy05]) that there are infinitely many real quadratic orders that are HFDs. Certainly this holds if there are infinitely many real quadratic fields of class number at most 2; though that is doubtless true (cf. [CL84b, CL84a]), a proof remains elusive. Theorem 1 shows that Coykendall's conjecture would also follow from GRH. Our next theorem resolves the conjecture unconditionally.

[1] Here GRH refers to the Riemann Hypothesis for all Dedekind zeta functions.

Theorem 2. *Infinitely many real quadratic orders are HFDs. In fact, there is a real quadratic field containing infinitely many HFD orders.*

It is natural to ask which real quadratic fields contain infinitely many HFD orders. Call the real quadratic field K viable if K has class number 1 or 2 and fundamental unit of norm -1. From our above discussion, viability is necessary for K to contain an HFD order having index an odd prime p. Viability is also necessary for K to contain an HFD order of index $2p$. In fact, if the order of index $2p$ is an HFD, so is the order of index p (see Corollary 3.6 in [Coy01]). So viability is a necessary condition for K to contain infinitely many HFD orders.

Under GRH, Chen's methods will show viability is also sufficient. We do not know how to remove the assumption of GRH here, but we can at least show unconditionally that viability suffices "almost always".

Theorem 3. *All but (at most) finitely many viable K contain infinitely many HFD orders.*

The proofs of Theorems 2 and 3 use ideas introduced by Gupta–Murty [GM84], Murty–Srinivasan [MS87], and Heath-Brown [HB86] to study Artin's primitive root conjecture. The arguments are similar in spirit, and in many details, to the proof of the main theorem of Cohen in [Coh06] (which however cannot be directly applied).

Notation and terminology. We reserve the letters p and q for primes, whether or not this is explicitly noted. We let $P^-(n)$ denote the smallest prime factor of the positive integer n, with $P^-(1)=\infty$. If p is a rational prime unramified in a Galois extension $K/\mathbb{Q}$, we let $\mathrm{Frob}_{K/\mathbb{Q}}(p)$ denote the corresponding Frobenius conjugacy class inside $\mathrm{Gal}(K/\mathbb{Q})$. When $K/\mathbb{Q}$ is abelian, we sometimes abuse notation and identify $\mathrm{Frob}_{K/\mathbb{Q}}(p)$ with the corresponding element of $\mathrm{Gal}(K/\mathbb{Q})$.

If L_1 and L_2 are field extensions of K, we say that L_1 and L_2 are linearly disjoint over K if every finite set of elements of L_1 that is linearly independent over K remains linearly independent over L_2. If $L_1, L_2, \dots, L_n$ is a finite sequence of extensions of K, we say $L_1, \dots, L_n$ are linearly disjoint over K if the composite field $L_1 \cdots L_i$ is linearly disjoint from L_{i+1} for all $i = 1, 2, \dots, n-1$. In our applications, each L_i will have finite degree over K; in this case, linear disjointness holds precisely when $[L_1 L_2 \cdots L_n : K] = [L_1 : K][L_2 : K] \cdots [L_n : K]$. See [FJ23, §3.1] for the theory of linearly disjoint extensions of fields.

2. Half-factorial orders in $\mathbb{Q}(\sqrt{2})$: Proof of the GRH-conditional Theorem 1

Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field (with d squarefree). Let p be an odd prime inert in K, so that $\mathrm{Frob}_{K/\mathbb{Q}}(p)$ is conjugation on K. If η is a norm 1 unit of $\mathcal{O}_K$, then $\eta^{p+1} = \eta \cdot \eta^p \equiv 1 \pmod{p}$ in $\mathcal{O}_K$. Thus, viewing $\mathcal{O}_K/p\mathcal{O}_K$ as $\mathbb{F}_p(\sqrt{d})$, we see that η has order $p+1$ in the group $\mathbb{F}_p(\sqrt{d})^\times$. In [Che02], Chen describes how to compute, given a norm 1 unit η of $\mathcal{O}_K$, the proportion of inert primes p for which the order of η in $\mathbb{F}_p(\sqrt{d})^\times$ is precisely $p+1$. (The corresponding problem for split primes p is also treated, but we do not need those results here.)

Let us connect this back to the condition (ii) appearing in the introduction. Let K be a viable real quadratic field with fundamental unit ε, and let p be an odd prime inert in K. Then condition (ii) from the introduction says no more and no less than that ε has order $p+1$ in $\mathbb{F}_p(\sqrt{d})^\times/\mathbb{F}_p^\times$. To relate our problem to Chen's, we compare the order j of ε in $\mathbb{F}_p(\sqrt{d})^\times/\mathbb{F}_p^\times$ to the order J of

$\eta := \varepsilon^2$ in $\mathbb{F}_p(\sqrt{d})^\times$. Working in $\mathbb{F}_p(\sqrt{d})$, we have $\varepsilon^{2J} = \eta^J = 1$. Thus, $\varepsilon^J = \pm 1 \in \mathbb{F}_p^\times$, which implies that $j \mid J$. On the other hand, since $\varepsilon^j \in \mathbb{F}_p^\times$, we have $\eta^{j(p-1)/2} = \varepsilon^{j(p-1)} = 1$. Hence, $J \mid j\frac{p-1}{2}$. Since J also divides $p+1$, we conclude that J divides $\gcd(j\frac{p-1}{2}, p+1)$, which in turn divides $j\gcd(\frac{p-1}{2}, p+1)$. We now restrict to primes $p \equiv -1 \pmod 4$. For these primes, $\gcd(\frac{p-1}{2}, p+1) = 1$, and so $J \mid j$. It follows that $J = j$ whenever p is inert and $p \equiv -1 \pmod 4$.

In view of conditions (i)–(iv) from the introduction, counting odd primes p for which $\mathbb{Z}[p\omega]$ is an HFD is completely equivalent to counting primes $p \equiv -1 \pmod 4$ that are inert in K and have $\eta = \varepsilon^2$ of order $p+1$ in $\mathbb{F}_p(\sqrt{d})^\times$. Were it not for the requirement that $p \equiv -1 \pmod 4$, an asymptotic formula for this count could be read off from Chen's results in [Che02]. As matters stand, we have to modify her arguments slightly.

Since the details follow [Che02] closely we restrict ourselves to a sketch. We treat only $K = \mathbb{Q}(\sqrt{2})$, the case relevant to Theorem 3. Here $\varepsilon = 1 + \sqrt{2}$ and $\eta = \varepsilon^2 = 3 + 2\sqrt{2}$.

Let p be a prime inert in K. Since $\eta^{(p+1)/2} = \varepsilon \cdot \varepsilon^p = -1$ in $\mathbb{F}_p(\sqrt{2})$, we see that the 2-power part of the order of η in $\mathbb{F}_p(\sqrt{2})^\times$ is the same as the 2-power part of $p+1$. For each odd prime q, let us say that p fails the q-test if

$$q \mid p+1 \quad \text{and} \quad \eta^{(p+1)/q} = 1 \text{ in } \mathbb{F}_p(\sqrt{2}). \tag{2}$$

Otherwise, we say p passes the q-test. Then the q-power part of the order of η in $\mathbb{F}_p(\sqrt{2})^\times$ agrees with the q-power part of $p+1$ precisely when p passes the q-test. Hence, η has order $p+1$ in $\mathbb{F}_p(\sqrt{2})^\times$ exactly when p passes the q-test for every odd prime q.

Let σ_0 denote conjugation on K, and let τ denote complex conjugation. For each odd positive integer Q, let $\zeta_Q = \exp(2\pi i/Q)$, and let

$$E_Q = K(\zeta_Q, \sqrt[Q]{1+\sqrt{2}}).$$

Then $E_Q/\mathbb{Q}$ is Galois. We let

$$C_Q = \{\sigma \in \mathrm{Gal}(E_Q/\mathbb{Q}) : \sigma^2 = \mathrm{id.}, \sigma|_K = \sigma_0, \sigma|_{\mathbb{Q}(\zeta_Q)} = \tau|_{\mathbb{Q}(\zeta_Q)}\}.$$

Then p is inert and fails the q-test, for a given odd prime q, precisely when $\mathrm{Frob}_{E_q/\mathbb{Q}}(p) \subseteq C_q$ (see [Che02, Lemma 1.4]). Following Hooley's GRH-conditional proof of Artin's conjecture [Hoo67] (see also [Mur83]), one deduces that the count of inert primes $p \le x$ passing all the q-tests is $(\delta + o(1))x/\log x$ (as $x \to \infty$), for the constant

$$\delta := \sum_{Q \text{ odd}} \mu(Q) \frac{|C_Q|}{[E_Q : \mathbb{Q}]} \tag{3}$$

(cf. [Che02, Theorem 2.1]). From Lemmas 1.6 and 1.7 of [Che02], $|C_Q| = 1$ and $[E_Q : \mathbb{Q}] = 2Q\phi(Q)$, for all odd squarefree Q. Hence,

$$\delta = \frac{1}{2}\sum_{Q \text{ odd}} \frac{\mu(Q)}{Q\phi(Q)} = \frac{1}{2}\prod_{q>2}\left(1 - \frac{1}{q(q-1)}\right) = A.$$

So far we have shown that there are $\sim Ax/\log x$ primes $p \le x$ (as $x \to \infty$) that are inert in K and pass all the q-tests. However this is an overcount for our purposes; we wish to count only p that satisfy $p \equiv -1 \bmod 4$. Provided that $\mathbb{Q}(i)$ is linearly disjoint from each E_Q, this congruence condition — which is a prescription of $\mathrm{Frob}_{\mathbb{Q}(i)/\mathbb{Q}}(p)$ — can be folded into Chen's arguments;

it has the effect of multiplying each term on the right of (3) by $\frac{1}{[\mathbb{Q}(i):\mathbb{Q}]} = \frac{1}{2}$, thus yielding the asymptotic formula (1).

It remains only to check the needed linear disjointness. If disjointness fails, then $i \in E_Q$ for some odd Q. Let $L_Q = K(\zeta_Q)$, so that $E_Q = L_Q(\sqrt[Q]{1+\sqrt{2}})$. Since $\zeta_Q \in L_Q$ and Q is odd, E_Q/L_Q is an odd degree extension (e.g., by Kummer theory [Lan02, §6.8, pp. 293–296]). Therefore, if $i \in E_Q$, it must be that $i \in L_Q$ and $L_Q = L_Q(i)$. But $[L_Q : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \zeta_Q)] \leq [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_Q) : \mathbb{Q}] = 2\phi(Q)$ whereas

$$[L_Q(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i, \zeta_Q) : \mathbb{Q}] = [\mathbb{Q}(\zeta_8, \zeta_Q) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{8Q}) : \mathbb{Q}] = \phi(8Q) = 4\phi(Q).$$

This completes our sketch of the proof of Theorem 1.

3. Unconditional results: Proof of Theorem 3

Both Theorem 2 and Theorem 3 follow quickly from the next proposition.

Proposition 4. *Among any 46 viable, linearly disjoint real quadratic fields, at least one contains infinitely many HFD orders.*

Proof of Theorems 2 and 3, assuming Proposition 4. Consider the following list of 46 prime numbers, each of which is congruent to 1 modulo 4:

$$\begin{multline}5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, 181, \\ 193, 197, 233, 241, 269, 277, 281, 293, 313, 317, 337, 349, 353, 373, 389, 397, \\ 409, 421, 433, 449, 457, 461, 509, 521, 541, 557, 569.\end{multline}$$

For each prime ℓ on this list, one can check that the field $\mathbb{Q}(\sqrt{\ell})$ has class number 1. All of the corresponding fundamental units have norm -1 as well: In fact, the fundamental unit of $\mathbb{Q}(\sqrt{\ell})$ has norm -1 for *every* prime $\ell \equiv 1 \pmod 4$ (see [Coh80, Theorem 3, p. 185]). Furthermore, the 46 fields $\mathbb{Q}(\sqrt{\ell})$ here are linearly disjoint (by Kummer theory or by considering ramification). Theorem 2 is now immediate from Proposition 4.

We turn to Theorem 3. Here is the key observation: Among any 2^{45} distinct real quadratic fields, one can select 46 that are linearly disjoint. To see this, write each of these fields in the form $\mathbb{Q}(\sqrt{d})$, where d is squarefree. We view the integers d as elements of $\mathbb{Q}^{\times}/(\mathbb{Q}^{\times})^2$, which is naturally thought of as an $\mathbb{F}_2$-vector space. Then the d in question clearly span a subspace of size at least $2^{45}+1$ (the $+1$ coming from 1 also belonging to the span). So if we choose a basis for our subspace from among the d, this basis will have size at least 46. Our observation now follows from Kummer theory. Combining the observation with Proposition 4, we see that the number of viable K not containing infinitely many HFD orders is smaller than 2^{45}. □

The remainder of this section is devoted to the proof of Proposition 4. Let K_i, for $i = 1, 2, \ldots, 46$, be linearly disjoint, viable real quadratic fields. Write each $K_i = \mathbb{Q}(\sqrt{d_i})$, where the d_i are squarefree, and let Δ_i denote the discriminant of K_i. We let ε_i be the fundamental unit of K_i. We view the K_i as subfields of $\mathbb{R} \subseteq \mathbb{C}$, and we let $K \subseteq \mathbb{R}$ be the compositum of all the K_i. For each rational prime p, we fix a prime ideal P of $\mathcal{O}_K$ lying above p, and we let $\mathbb{F}_P = \mathcal{O}_K/P$. (Which prime P above p we choose is unimportant here.) Recalling (i) and (ii) from the introduction, Proposition 4 will follow if we show that for some $i = 1, 2, \dots, 46$, there are infinitely many primes p which are inert in K_i and for which ε_i has order $p + 1$ in the group $\mathbb{F}_P^\times/\mathbb{F}_p^\times$.

By the pigeonhole principle, it suffices to show that for all large x, there are $\gg x/(\log x)^2$ primes $p \le x$ which are inert in all of $K_1, \dots, K_{46}$ and have the property that ε_i has order $p+1$ in $\mathbb{F}_P^\times/\mathbb{F}_p^\times$ for *some* $i = 1, 2, \dots 46$.

The primes we produce will come from a carefully tailored arithmetic progression. To begin its construction, observe that K, $\mathbb{Q}(i)$, and $\mathbb{Q}(\sqrt{-3})$ are linearly disjoint. Otherwise, there are exponents a, a', and $a_1, \dots, a_{46}$, each in $\{0, 1\}$ and not all 0, such that

$$(-3)^a(-1)^{a'}\prod_{i=1}^{46} d_i^{a_i} \in (\mathbb{Q}^\times)^2.$$

Since the K_i are assumed linearly disjoint, either a or a' must be nonzero. Noting that $(\mathbb{Q}^\times)^2 \subseteq \mathbb{R}_{>0}$, we are now forced to have $a = a' = 1$, so that $3\prod_{i=1}^{46} d_i^{a_i}$ is a square. Thus, 3 divides some d_i. But then it is impossible for ε_i to have norm -1, as -1 is not a square mod 3.

By the Chebotarev density theorem, there are infinitely many primes p such that

(I) p is inert in every K_i,

(II) p splits completely in $\mathbb{Q}(\sqrt{-3})$ (i.e., $p \equiv 1 \pmod 3$),

(III) p is inert in $\mathbb{Q}(i)$ (i.e., $p \equiv -1 \pmod 4$).

We fix a prime p_0 satisfying (I)–(III). For each odd prime q dividing $\prod_{i=1}^{46}\Delta_i$, we let $u_q = p_0$ or $4p_0$, selected in such a way that $q \nmid 1 + u_q$. Such a choice of u_q is clearly possible when $q \ge 5$, and condition (II) above guarantees there is no problem when $q = 3$. We choose M so that $2^M \parallel p_0 + 1$. (Note that $M \ge 2$.) Let U be a solution to the system

$$\begin{aligned} U &\equiv u_q \pmod q, \quad \text{for all odd primes } q \mid \prod\nolimits_{i=1}^{46}\Delta_i,\\ U &\equiv p_0 \pmod{2^{M+1}}, \end{aligned}$$

and let

$$V = 2^{M+1}\prod_{\substack{q \mid \Delta_1\cdots\Delta_{46}\\ q>2}} \ell.$$

Then $U \bmod V$ is a coprime residue class. Furthermore, $\gcd(U+1, V) = 2^M$, and each integer $u \equiv U \pmod V$ is such that $2^M \parallel u + 1$.

We claim that every prime $p \equiv U \pmod V$ satisfies conditions (I) and (III) above. For the proof, we must show that if $\Delta \in \{-4, \Delta_1, \dots, \Delta_{46}\}$, and p is a prime with $p \equiv U \pmod V$, then $\left(\frac{\Delta}{p}\right) = \left(\frac{\Delta}{p_0}\right)$. We may factor Δ as a product of prime discriminants Δ', meaning $-4, \pm 8$, and $(-1)^{(q-1)/2}q$ for an odd prime q. It thus suffices to prove that $\left(\frac{\Delta'}{p}\right) = \left(\frac{\Delta'}{p_0}\right)$ for each of these prime discriminants Δ'. If $\Delta' = -4$ or ± 8, then $\left(\frac{\Delta'}{p}\right) = \left(\frac{\Delta'}{U}\right) = \left(\frac{\Delta'}{p_0}\right)$, since $p \equiv U \equiv p_0 \pmod 8$. Otherwise, $\Delta' = (-1)^{(q-1)/2}q$ for an odd prime q dividing V. In this case the character $\left(\frac{\Delta'}{\cdot}\right)$ coincides with the Legendre symbol $\left(\frac{\cdot}{q}\right)$. Since $p \equiv u_q \pmod q$, we have that $\left(\frac{p}{q}\right) = \left(\frac{u_q}{q}\right)$, and $\left(\frac{u_q}{q}\right) = \left(\frac{p_0}{q}\right)$ regardless of whether $u_q = p_0$ or $4p_0$.

We now sieve the primes $p \equiv U \pmod{V}$. The linear sieve, in conjunction with the Bombieri–Vinogradov theorem, produces $\gg x/(\log x)^2$ primes $p \le x$ with $p \equiv U \pmod{V}$ and

$$P^-\left(\frac{p+1}{2^M}\right) > x^{0.24}. \tag{4}$$

(See [DH08, Theorem 7.1, p. 81] for a statement of the linear sieve, and see Chapter 8 of this same reference for details of an application similar to this one. The exponent 0.24 here may be replaced by any number smaller than $\frac{1}{4}$.) The proof of Proposition 4 will be completed by showing all but $o(x/(\log x)^2)$ of these primes p are such that some ε_i has order $p+1$ in $\mathbb{F}_P^\times/\mathbb{F}_p^\times$.

Let $p \le x$ be one of these primes produced by the sieve. Then $p \equiv -1 \pmod 4$ and so $-1 \notin (\mathbb{F}_p^\times)^2$. As $(\varepsilon_i^{(p+1)/2})^2 = \varepsilon_i^{p+1} = -1$ in $\mathbb{F}_P$, it follows that $\varepsilon_i^{p+1} \in \mathbb{F}_p^\times$ while $\varepsilon_i^{(p+1)/2} \notin \mathbb{F}_p^\times$. So if write w_i for the order of ε_i in the group $\mathbb{F}_P^\times/\mathbb{F}_p^\times$, then w_i has the same 2-power-part 2^M as $p+1$, and

$$w_i = 2^M d_i \quad \text{where} \quad d_i \mid \frac{p+1}{2^M}.$$

From (4), the integer $\frac{p+1}{2^M}$ has at most 4 prime factors (counted with multiplicity) and therefore at most 15 proper divisors. Thus if all of the w_i are proper divisors of $p+1$, then among the numbers $w_1, \dots, w_{46}$ we can choose 4 that coincide, say $w_{i_1} = w_{i_2} = w_{i_3} = w_{i_4} =: w$ where $1 \le i_1 < i_2 < i_3 < i_4 \le 46$. As $\mathbb{F}_P^\times$ is cyclic, it follows that $\varepsilon_{i_1}, \dots, \varepsilon_{i_4}$ generate the same order w subgroup of $\mathbb{F}_P^\times/\mathbb{F}_p^\times$. Since $\frac{p+1}{w}$ is an integer larger than 1 and composed of primes exceeding $x^{0.24}$, we have $w < \frac{p+1}{x^{0.24}} < x^{0.77}$ (for large x).

In summary, if a prime $p \le x$ given to us by the linear sieve has none of the ε_i of desired order $p+1$ in $\mathbb{F}_P^\times/\mathbb{F}_p^\times$, then some four of the ε_i generate a subgroup of $\mathbb{F}_P^\times/\mathbb{F}_p^\times$ having order less than $x^{0.77}$. We now argue, following Matthews [Mat82], that the number of p with this last property is quite a bit smaller than $x/(\log x)^2$.

Consider all products $\varepsilon_{i_1}^{e_1} \cdots \varepsilon_{i_4}^{e_4}$, where the exponents are nonnegative integers not exceeding $x^{0.195}$. Since there are $> x^{0.78}$ exponent tuples, while $\#\langle \varepsilon_{i_1}, \dots, \varepsilon_{i_4}\rangle < x^{0.77}$, two of our products must coincide when viewed within $\mathbb{F}_P^\times/\mathbb{F}_p^\times$. It follows that for some integers E_1, E_2, E_3, E_4, not exceeding $x^{0.195}$ in absolute value and not all zero, $\varepsilon_{i_1}^{E_1} \cdots \varepsilon_{i_4}^{E_4} \in \mathbb{F}_p^\times$ (inside $\mathbb{F}_P$). Viewed in $\mathbb{F}_P$, all of $\varepsilon_{i_1}, \dots, \varepsilon_{i_4}$ lie within the subfield $\mathbb{F}_{p^2}$, and

$$(\varepsilon_{i_1}^{E_1} \cdots \varepsilon_{i_4}^{E_4})^2 = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\varepsilon_{i_1}^{E_1} \cdots \varepsilon_{i_4}^{E_4}) = (-1)^{E_1 + \dots + E_4} = \pm 1.$$

Thus, in $\mathcal{O}_K$,

$$\varepsilon_{i_1}^{4E_1} \cdots \varepsilon_{i_4}^{4E_4} \equiv 1 \pmod{P}.$$

But then

$$p \mid N_{K/\mathbb{Q}}(\varepsilon_{i_1}^{4E_1} \cdots \varepsilon_{i_4}^{4E_4} - 1).$$

We now bound the number of p for which this divisibility relation holds. We start by noticing that the norm on the right-hand side is nonvanishing. Otherwise, with j the largest index for which $E_j \ne 0$, we have $\varepsilon_{i_j}^{4E_j} = \varepsilon_{i_1}^{-4E_1} \cdots \varepsilon_{i_{j-1}}^{-4E_{j-1}}$. But $\varepsilon_{i_j}^{4E_j}$ belongs to $K_{i_j} \setminus \mathbb{Q}$ while $\varepsilon_{i_1}^{-4E_1} \cdots \varepsilon_{i_{j-1}}^{-4E_{j-1}}$ belongs to the compositum of $K_{i_1}, \dots, K_{i_{j-1}}$, contradicting the linear disjointness of $\{K_i\}_{i=1}^{46}$.

Continuing, choose $B = \max_{1\le i\le 46} |\varepsilon_i|$. Recalling that each $|E_i| \le x^{0.195}$ and noting that the conjugate of a quadratic unit has the same absolute value as its inverse,

$$\left|N_{K/\mathbb{Q}}(\varepsilon_{i_1}^{4E_1}\cdots\varepsilon_{i_4}^{4E_4}-1)\right| \le (B^{16x^{0.195}}+1)^{[K:\mathbb{Q}]} \le \exp(B'x^{0.195}),$$

for some constant B' depending on the K_i. It follows that only $O(x^{0.195})$ primes can divide $N_{K/\mathbb{Q}}(\varepsilon_{i_1}^{4E_1}\cdots\varepsilon_{i_4}^{4E_4}-1)$, given $E_1,\dots,E_4$. There are $\ll (x^{0.195})^4 = x^{0.78}$ choices of $E_1,\dots,E_4$ and so in total there are $\ll x^{0.78}\cdot x^{0.195} = x^{0.975}$ possibilities for p, for any given $i_1,\dots,i_4$. Finally, there are only $O(1)$ cases for $i_1,\dots,i_4$. We conclude that from the set of $\gg x/(\log x)^2$ primes $p \le x$ given to us by the linear sieve, all but $O(x^{0.975})$ of these have some ε_i of order $p+1$ in $\mathbb{F}_P^\times/\mathbb{F}_p^\times$. This completes the proof of Proposition 4.

Remark. The constants 46 and 2^{45} above could be reduced by employing stronger analytic tools (cf. [HB86, §§2–4], [Coh06, §4]).

Acknowledgements. The author is supported by the National Science Foundation (NSF) under award DMS-2001581. He expresses his thanks to Komal Agrawal for helpful discussions around Chen's paper [Che02], as well as to the referee for valuable feedback.

References

[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.

[Che02] Y.-M. J. Chen, *On primitive roots of one-dimensional tori*, J. Number Theory **93** (2002), 23–33.

[CL84a] H. Cohen and H. W. Lenstra, Jr., *Heuristics on class groups*, Number theory (New York, 1982), Lecture Notes in Math., vol. 1052, Springer, Berlin, 1984, pp. 26–36.

[CL84b] ———, *Heuristics on class groups of number fields*, Number theory, Noordwijkerhout 1983, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

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

[Coh80] H. Cohn, *Advanced number theory*, Dover Publications, Inc., New York, 1980.

[Coh06] J. Cohen, *Primitive roots in quadratic fields*, Int. J. Number Theory **2** (2006), 7–23.

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

[Coy05] ———, *Extensions of half-factorial domains: a survey*, Arithmetical properties of commutative rings and monoids, Lect. Notes Pure Appl. Math., vol. 241, Chapman & Hall/CRC, Boca Raton, FL, 2005, pp. 46–70.

[DH08] H. G. Diamond and H. Halberstam, *A higher-dimensional sieve method*, Cambridge Tracts in Mathematics, vol. 177, Cambridge University Press, Cambridge, 2008.

[FJ23] M. D. Fried and M. Jarden, *Field arithmetic*, fourth ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., vol. 11, Springer, Cham, 2023.

[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.

[GM84] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), 127–130.

[HB86] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), 27–38.

[HK83] F. Halter-Koch, *Factorization of algebraic integers*, Grazer Math. Berichte **191** (1983).

[Hoo67] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[Lan02] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[Mat82] C. R. Matthews, *Counting points modulo p for some finitely generated subgroups of algebraic groups*, Bull. London Math. Soc. **14** (1982), 149–154.

[MS87] M. R. Murty and S. Srinivasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull. **30** (1987), 80–85.

[Mur83] M. R. Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), 147–168.

[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.

[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: pollack@uga.edu