ORDERS IN THE EUCLIDEAN COURT

CARLO FRANCISCO ADAJAR, KEVIN J. MCGOWN, PAUL POLLACK, AND ENRIQUE TREVIÑO

Abstract. Following Johnson, Queen, and Sevilla, we call an order $\mathcal{O}$ in a number field K generalized Euclidean if for all $\alpha, \beta \in \mathcal{O}$ with $\beta \neq 0$ for which $\alpha\mathcal{O} + \beta\mathcal{O}$ is a principal ideal of $\mathcal{O}$, there are $\gamma, \rho \in \mathcal{O}$ with $\alpha = \beta\gamma + \rho$ and $|N_{K/\mathbb{Q}}(\rho)| < |N_{K/\mathbb{Q}}(\beta)|$. We prove that only finitely many quadratic orders are generalized Euclidean. Additionally, assuming GRH, we show that for each fixed $d > 1$ there are only finitely many integers m for which $T^d - m$ is irreducible over $\mathbb{Q}$ and $\mathbb{Z}[m^{1/d}] = \mathbb{Z}[T]/(T^d - m)$ is generalized Euclidean. When d is even, we can remove the assumption of GRH.

1. Introduction

Let K be a number field with ring of integers $\mathcal{O}_K$. One calls $\mathcal{O}_K$ norm-Euclidean if, for every pair of $\alpha, \beta \in \mathcal{O}_K$ with $\beta \neq 0$, there are $\gamma, \rho \in \mathcal{O}_K$ for which

$$\alpha = \beta\gamma + \rho \quad \text{and} \quad |N_{K/\mathbb{Q}}(\rho)| < |N_{K/\mathbb{Q}}(\beta)|\,. \tag{1}$$

If $\mathcal{O}_K$ is norm-Euclidean, then every pair of $\alpha, \beta \in \mathcal{O}_K$ has a gcd $\delta \in \mathcal{O}_K$ that can be found by the Euclidean algorithm. It follows, as explained in a first algebra course, that $\mathcal{O}_K$ is a principal ideal domain and hence also a unique factorization domain.

Here we consider orders in number fields, not just the ring of integers. Moreover, we work with a more general notion, first introduced by Johnson–Queen–Sevilla (for rings of integers in quadratic fields) [JQS85]. We call an order $\mathcal{O}$ generalized Euclidean if for all $\alpha, \beta \in \mathcal{O}$ with $\beta \neq 0$ and (α, β) principal, there exists $\gamma, \rho \in \mathcal{O}$ satisfying (1). In other words, if the gcd of α and β exists (in a strong form), then it can be computed using the Euclidean algorithm (relative to the norm). (To align more with current practice, we should perhaps use the terminology "generalized norm-Euclidean", but we have chosen to use the shorter "generalized Euclidean".) A partial classification of quadratic rings of integers that are generalized Euclidean was given in [JQS85, Theorems 1 and 2], but they did not fully treat the case of $\mathbb{Q}(\sqrt{d})$ when $d \equiv 1 \pmod 4$. We prove a finiteness result for all quadratic orders. (Note that an order can be generalized Euclidean without being maximal; one example is $\mathbb{Z}[\sqrt{-3}]$.)

Theorem 1. *There are finitely many quadratic orders that are generalized Euclidean.*

Further, we now consider more general orders. Fix an integer $d \geq 2$. If m is an integer for which the polynomial $F_{d,m}(T) := T^d - m$ is irreducible over $\mathbb{Q}$, we let $K_{d,m} = \mathbb{Q}(m^{1/d})$ and $\mathcal{O}_{d,m} := \mathbb{Z}[m^{1/d}]$. Then $\mathcal{O}_{d,m}$ is an order inside the number field $K_{d,m}$; we will refer to $\mathcal{O}_{d,m}$ as a pure order of degree d.

Theorem 2. *Fix an even positive integer d. There are finitely many pure orders of degree d that are generalized Euclidean.*

2020 *Mathematics Subject Classification.* Primary 11R27; Secondary 11R11, 13F07.

Theorem 3. *Assume GRH. For any fixed integer $d \geq 2$, there are finitely many pure orders of degree d that are generalized Euclidean.*

One might be interested in comparing Theorems 2 and 3 with results of Egami (see [Ega84]) for the fields $\mathbb{Q}(m^{1/p})$, p prime. However, the notion of $\mathbb{Q}(m^{1/p})$ containing a norm-Euclidean ideal class, considered by Egami, is different than the notion we consider here, so neither set of results implies the other.

2. Preparation

At the heart of all our proofs are the following variants of Heilbronn's criterion for non-Euclideanity. Heilbronn's criterion was first introduced in [Hei38], but can be considered implicit in earlier work of Erdős and Ko [EK38]. We remark that it is condition (i) in both Propositions 4 and 5 that allows the stronger conclusion of "not generalized Euclidean" versus "not norm-Euclidean".

Proposition 4 (Heilbronn's criterion for pure orders)**.** *Suppose $d \geq 2$. Let $\mathcal{O}_{d,m}$ be a pure order of degree d. Suppose there are positive integers a, b with*

$$|m| = a + b,$$

where

(i) $\gcd(a, m) = 1$,

(ii) *a is a dth power modulo m,*

(iii) *neither a nor $-b$ has the form $N_{K_{d,m}/\mathbb{Q}}(\alpha)$ for any $\alpha \in \mathcal{O}_{d,m}$.*

Then $\mathcal{O}_{d,m}$ is not generalized Euclidean.

Recall that to each quadratic order $\mathcal{O}$ there is associated a unique integer D for which either

$$\mathcal{O} = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\} \tag{2}$$

or

$$\mathcal{O} = \left\{\frac{1}{2}(a + b\sqrt{D}) : a, b \in \mathbb{Z}, a \equiv b \pmod 2\right\}. \tag{3}$$

The first case occurs when the order discriminant Δ is a multiple of 4, in which case $D = \Delta/4$, and the second case when $\Delta \equiv 1 \pmod 4$, in which case $D = \Delta$. In both cases, D is not a perfect square.

Proposition 5 (Heilbronn's criterion for quadratic orders)**.** *Let $\mathcal{O}$ be an order in a quadratic field K, and let $D \in \mathbb{Z}$ be such that (2) or (3) holds. Suppose there are positive integers a, b with*

$$|D| = a + b,$$

where

(i) $\gcd(a, D) = 1$,

(ii) *a is a square modulo D,*

(iii) *neither a nor $-b$ has the form $N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(\alpha)$ for any $\alpha \in \mathcal{O}$.*

Then $\mathcal{O}$ is not generalized Euclidean.

(Proposition 5 does not quite follow from Proposition 4; when $D \equiv 1 \pmod 4$, the corresponding order $\mathcal{O}$ is not $\mathcal{O}_{2,m}$ for any m.)

Perhaps the chief novelty in the proofs (and statements) of Propositions 4 and 5 is the lack of any (explicit) reference to ramification. Instead, we phrase the arguments in terms of properties of the corresponding norm forms.

We suspect the following lemma, needed for the proof of Proposition 4, is known to the experts. But lacking a suitable reference, we include the proof here.

Lemma 6. *Let $d \geq 2$, and let $\mathcal{O}_{d,m}$ be a pure order of degree d. Let $\tilde{N}(x_0, \ldots, x_{d-1})$ be the* norm form *associated to the $\mathbb{Q}$-basis $1, m^{1/d}, \ldots, m^{(d-1)/d}$ of $K_{d,m}$. That is, $\tilde{N}(x_0, \ldots, x_{d-1})$ is the polynomial in $x_0, \ldots, x_{d-1}$ defined by*

$$\tilde{N}(x_0, x_1, \ldots, x_{d-1}) = \prod_{\sigma\colon K_{d,m} \hookrightarrow \mathbb{C}} (x_0 + x_1\sigma(m^{1/d}) + \cdots + x_{d-1}\sigma(m^{(d-1)/d})),$$

where σ runs over all the embeddings of $K_{d,m}$ into $\mathbb{C}$. Then $\tilde{N}(x_0, \ldots, x_{d-1}) \in x_0^d + m\mathbb{Z}[x_0, \ldots, x_{d-1}]$.

Proof. Define a polynomial $\tilde{N}(\mathbf{x}, \mathbf{t})$ in indeterminates $\mathbf{x} = x_0, \ldots, x_{d-1}$ and $\mathbf{t} = t_0, \ldots, t_{d-1}$ by setting

$$\tilde{N}(\mathbf{x}, \mathbf{t}) := \prod_{j=0}^{d-1} (x_0 + x_1 t_j + x_2 t_j^2 + \cdots + x_{d-1} t_j^{d-1}).$$

Then $\tilde{N}(\mathbf{x}, \mathbf{t})$ can be viewed as a polynomial in $\mathbf{t}$ over $\mathbb{Z}[\mathbf{x}]$, symmetric with respect to the t_j. By the fundamental theorem of symmetric polynomials, $\tilde{N}(\mathbf{x}, \mathbf{t})$ is a polynomial, with $\mathbb{Z}[\mathbf{x}]$ coefficients, in the elementary symmetric functions of the t_j.

Continuing, we introduce a new indeterminate Z, and we let $\omega_j := \exp(2\pi \mathrm{i} j/d)$. Replacing each t_j by $\omega_j Z$, we conclude from our work in the last paragraph that

$$\tilde{N}(\mathbf{x}, Z) := \prod_{j=0}^{d-1} (x_0 + x_1\omega_j Z + x_2\omega_j^2 Z^2 + \cdots + x_{d-1}{\omega_j}^{d-1} Z^{d-1}) \tag{4}$$

is a polynomial over $\mathbb{Z}[\mathbf{x}]$ in the elementary symmetric functions of the $\omega_j Z$. These elementary symmetric functions all vanish, except for the last one (the dth), which is $\pm Z^d$; this can be read off from the formal expansion $\prod_{j=0}^{d-1}(T - \omega_j Z) = T^d - Z^d$. We conclude that $\tilde{N}(\mathbf{x}, Z)$ is a polynomial in $x_0, \ldots, x_{d-1}$ and Z^d, with integer coefficients. Setting $Z = 0$ in (4), we deduce that

$$\tilde{N}(\mathbf{x}, Z) = x_0^d + Z^d Q \quad \text{for some} \quad Q \in \mathbb{Z}[\mathbf{x}, Z^d].$$

To finish, it remains only to observe that

$$\tilde{N}(x_0, x_1, \ldots, x_{d-1}) = \tilde{N}(\mathbf{x}, m^{1/d}),$$

so that

$$\tilde{N}(x_0, x_1, \ldots, x_{d-1}) \in x_0^d + m\mathbb{Z}[x_0, \ldots, x_{d-1}],$$

as claimed. □

Proof of Proposition 4. It is convenient to abbreviate $\mathcal{O}_{d,m}$ to $\mathcal{O}$ throughout the proof, and to write N in place of $N_{K_{d,m}/\mathbb{Q}}$. Suppose for a contradiction that $\mathcal{O}$ is generalized Euclidean. Using conditions (i) and (ii), we may choose $A \in \mathbb{Z}$ with A coprime to m and $A^d \equiv a \bmod m\mathbb{Z}$. Since

$$A\mathcal{O} + m^{1/d}\mathcal{O} \supseteq A\mathbb{Z} + m\mathbb{Z} = \mathbb{Z},$$

the $\mathcal{O}$-ideal generated by A and $m^{1/d}$ is all of $\mathcal{O}$, and in particular is principal. As $\mathcal{O}$ is generalized Euclidean, there is an $\alpha \in \mathcal{O}$ with $A \equiv \alpha \pmod{m^{1/d}\mathcal{O}}$ and $|N(\alpha)| < |N(m^{1/d})| = |m|$. Write

$$\alpha = A_0 + A_1 m^{1/d} + \cdots + A_{d-1} m^{(d-1)/d}.$$

Then $A \equiv \alpha \equiv A_0 \pmod{m^{1/d}\mathcal{O}}$, so that $(A - A_0)/m^{1/d} \in \mathcal{O}$. But

$$\frac{A - A_0}{m^{1/d}} = \frac{A - A_0}{m} m^{(d-1)/d};$$

as $\mathcal{O} = \mathbb{Z}[m^{1/d}]$, for the final displayed expression to land in $\mathcal{O}$ requires that $(A - A_0)/m \in \mathbb{Z}$. Hence, $A_0 \equiv A \pmod m$. By Lemma 6,

$$\begin{aligned} N(\alpha) &= \tilde{N}(A_0, \ldots, A_{d-1}) \\ &\equiv A_0^d \equiv A^d \equiv a \pmod{m\mathbb{Z}}. \end{aligned}$$

We have $0 < a < |m|$ and $|N(\alpha)| < |m|$. If $0 \le N(\alpha) < |m|$, then the congruence $N(\alpha) \equiv a \pmod{m\mathbb{Z}}$ forces $a = N(\alpha)$. Similarly, if $-|m| < N(\alpha) \le 0$, then $-b = a - |m| = N(\alpha)$. In either case we contradict our condition (iii). □

Proof of Proposition 5. This is very similar to the proof of Proposition 4, so we only sketch it. Using (i) and (ii), choose $A \in \mathbb{Z}$, $\gcd(A, D) = 1$, with $A^2 \equiv a \pmod D$. Then $A\mathcal{O} + \sqrt{D}\mathcal{O} \supseteq A\mathbb{Z} + D\mathbb{Z} = \mathbb{Z}$. Hence, $A, \sqrt{D}$ generate the unit ideal of $\mathcal{O}$. Thus, assuming $\mathcal{O}$ is generalized Euclidean, there is an $\alpha \in \mathcal{O}$ with $A \equiv \alpha \pmod{\sqrt{D}\mathcal{O}}$ and $|N(\alpha)| < |N(\sqrt{D})| = |D|$, where N denotes the norm $N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}$.

Let σ denote the nontrivial automorphism of $\mathbb{Q}(\sqrt{D})$. Since σ carries $\sqrt{D}\mathcal{O}$ into $\sqrt{D}\mathcal{O}$, the congruence

$$A \equiv \alpha \pmod{\sqrt{D}\mathcal{O}}$$

implies

$$A \equiv \sigma(\alpha) \pmod{\sqrt{D}\mathcal{O}}.$$

Thus, $A^2 \equiv \alpha\sigma(\alpha) \equiv N(\alpha) \pmod{\sqrt{D}\mathcal{O}}$, and

$$\frac{A^2 - N(\alpha)}{\sqrt{D}} = \frac{A^2 - N(\alpha)}{D}\sqrt{D} \in \mathcal{O}.$$

Regardless of whether we are in case (2) or (3), this last containment forces $(A^2 - N(\alpha))/D \in \mathbb{Z}$. Hence,

$$a \equiv A^2 \equiv N(\alpha) \pmod{D\mathbb{Z}}.$$

Reasoning as in Proposition 4, we deduce from $|N(\alpha)| < |D|$ that either $N(\alpha) = a$ or $N(\alpha) = -b$, contradicting (iii). □

3. Proofs of Theorems 1–3

Theorems 1–3 follow immediately from Propositions 4 and 5 via the following lemmata.

Lemma 7. *Let $\mathcal{O}_{d,m}$ be a pure order of even degree $d \geq 2$. Provided $|m|$ is sufficiently large, there are positive integers a, b with $|m| = a + b$ and conditions (i)–(iii) of Proposition 4 satisfied.*

Lemma 8. *Let $\mathcal{O}$ be a quadratic order with $D \in \mathbb{Z}$ satisfying (2) or (3). Provided $|D|$ is sufficiently large, there are positive integers a, b with $|D| = a + b$ and conditions (i)–(iii) of Proposition 5 satisfied.*

Lemma 9. *Assume GRH. Let $d \geq 2$. For every $m \in \mathbb{Z}$ with $|m|$ sufficiently large, there are positive integers a, b with $|m| = a + b$ and conditions (i)–(iii) of Proposition 4 satisfied.*

Our proofs of Lemmas 7 and 8 rely on the following result of Pollack [Pol17, Theorem 1.1].

Proposition 10. *For each $\epsilon > 0$, there are $m_0 = m_0(\epsilon)$ and $\kappa = \kappa(\epsilon) > 0$ for which the following holds. For all $m > m_0$ and every nontrivial Dirichlet character $\chi \bmod m$, there are more than m^κ primes $q \leq m^{\frac{1}{4\sqrt{\mathrm{e}}}+\epsilon}$ for which $\chi(q) \notin \{0, 1\}$.*

Proofs of Lemmas 7 and 8. In order to treat both Lemmas in a unified fashion, we adopt the following convention. When Lemma 7 is in view, the letters d, m have the meanings of that lemma, $K = K_{d,m}$ and $\mathcal{O} = \mathcal{O}_{d,m}$. If we are considering Lemma 8, we take $d = 2$, $m = D$, $K = \mathbb{Q}(\sqrt{D})$ and $\mathcal{O}$ the quadratic order appearing in that lemma.

To start with, we produce positive integers a and b summing to $|m|$ and satisfying conditions (i) and (ii) in Proposition 4 (respectively, Proposition 5). At the end of the proof we will see that our particular construction of a and b also satisfies condition (iii) of these Propositions.

Let χ be the quadratic character mod $4|m|$ given by $\chi(n) = (\frac{4m}{n})$ (the Kronecker symbol), and note that if $\chi(q) \notin \{0, 1\}$ for the prime q, then q is odd and $(\frac{m}{q}) = -1$. By Proposition 10, it follows that for all $\epsilon > 0$, there is a $\kappa > 0$ with

$$\#\left\{q \leq |m|^{1/4\sqrt{\mathrm{e}}+\epsilon} : q \text{ odd prime}, \left(\frac{m}{q}\right) = -1\right\} \geq |m|^\kappa$$

whenever m is sufficiently large in absolute value. Since $4\sqrt{\mathrm{e}} > 6$, we can take, for m large in absolute value, $2 < q_1 < q_2 \leq |m|^{1/6}$ with $(\frac{m}{q_1}) = (\frac{m}{q_2}) = -1$. (In particular, $q_1, q_2 \nmid m$.)

We now proceed to count the number of integers a', b' for which

$$q_1 a' + q_2 b' = |m| \tag{5}$$

and for which all of the following hold:

1. $0 < a' < \dfrac{|m|}{q_1}$;
2. $q_1 a'$ is a dth power mod m with $\gcd(q_1 a', m) = 1$;
3. $q_1 \nmid a'$;
4. $q_2 \nmid b'$.

If at least one such pair of a', b' exist, then conditions (i) and (ii) in Proposition 4 (or Proposition 5) are satisfied by taking $a = q_1 a', b = q_2 b'$.

Equation (5) implies that $b' = (|m| - q_1 a')/q_2$ is entirely determined by a'. So we can phrase the problem entirely in terms of counting certain integers a'. To ensure b' is an integer, we tack on the condition

5. $a' \equiv |m| q_1^{-1} \pmod{q_2}$.

Our task then becomes counting all the integers a' simultaneously satisfying conditions 1–5, thinking of condition 4 as $a' \not\equiv |m| q_1^{-1} \pmod{q_2^2}$.

We detect condition 2 using character sums; we have that

$$\frac{1}{N} \sum_{\chi^d = \chi_0} \chi(a) = \begin{cases} 1 & \text{if } a \text{ is a } d\text{th power mod } m \text{ and } \gcd(a,m) = 1; \\ 0 & \text{otherwise,} \end{cases}$$

where N is the number of characters χ mod m satisfying $\chi^d = \chi_0$.

We use an inclusion-exclusion argument to account for conditions 3 and 4. We thus write our count as

$$\frac{1}{N} \sum_{0 \le i,j \le 1} (-1)^{i+j} \sideset{}{^{(i,j)}}\sum_{a'} \sum_{\chi^d = \chi_0} \chi(q_1 a')$$

where the sums $\sum_{a'}^{(i,j)}$ are taken over all a' satisfying conditions 1 and 5, but possibly violating conditions 3 and/or 4: here $i = 1$ if (and only if) condition 3 is violated, and $j = 1$ if (and only if) 4 is violated.

We proceed to estimate the sums $\sum_{a'}^{(i,j)} \sum_{\chi^d = \chi_0} \chi(q_1 a')$. First, we look at the contribution of the nonprincipal characters. A violation of condition 3 means that we have $a' \equiv 0 \pmod{q_1}$. Similarly, a violation of condition 4 means that condition 5 can be strengthened to $a' \equiv |m| q_1^{-1} \pmod{q_2^2}$. Thus, depending on i and j, we have by the Chinese Remainder Theorem that each a' lies in one specific residue class mod $m_{i,j} := q_1^i q_2^{j+1}$, i.e., we can write $a' = a_{i,j} + n m_{i,j}$ where n lies in an interval $I_{i,j}$ of length $|m|/(q_1^{i+1} q_2^{j+1})$. We then write, for each $\chi \neq \chi_0$,

$$\begin{aligned} \sum_{a'}^{(i,j)} \chi(q_1 a') &= \chi(q_1) \sum_{a'}^{(i,j)} \chi(a') \\ &= \chi(q_1) \sum_{n \in I_{i,j}} \chi(n m_{i,j} + a_{i,j}) \\ &= \chi(q_1) \chi(m_{i,j}) \sum_{n \in I_{i,j}} \chi(n + a_{i,j} m_{i,j}^{-1}) \\ &= O\left(\sqrt{|m|} \log |m| \right) \end{aligned}$$

by Pólya–Vinogradov. Here we write $m_{i,j}^{-1}$ for the inverse of $m_{i,j}$ mod m.

We now look at the contribution of the principal character. We write

$$\begin{aligned}\sum_{a'}^{(i,j)} \chi_0(q_1 a') &= \sum_{a'}^{(i,j)} \chi_0(a) \\ &= \sum_{a'}^{(i,j)} \mathbf{1}_{\gcd(a',m)=1} \\ &= \sum_{a'}^{(i,j)} \sum_{e \mid \gcd(a',m)} \mu(e) \\ &= \sum_{e \mid m} \mu(e) \sum_{a'}^{(i,j)} \mathbf{1}_{e \mid a'} \\ &= \sum_{e \mid m} \mu(e) \left(\frac{|m|}{e q_1^{i+1} q_2^{j+1}} + O(1) \right) \\ &= \frac{\varphi(|m|)}{q_1^{i+1} q_2^{j+1}} + O\left(2^{\omega(|m|)}\right).\end{aligned}$$

Collecting estimates,

$$\sum_{a'}^{(i,j)} \sum_{\chi^d = \chi_0} \chi(q_1 a') = \frac{\varphi(|m|)}{q_1^{i+1} q_2^{j+1}} + O\left(2^{\omega(|m|)}\right) + O\left(N \sqrt{|m|} \log |m|\right).$$

Putting everything together, we get that, as $|m| \to \infty$, the number of integer solutions a, b to (5) satisfying conditions 1–5 is

$$\frac{\varphi(|m|)}{N q_1 q_2} \left(1 - \frac{1}{q_1}\right) \left(1 - \frac{1}{q_2}\right) + O\left(\frac{2^{\omega(|m|)}}{N}\right) + O\left(\sqrt{|m|} \log |m|\right).$$

Let us estimate the various terms in this expression. Writing τ for the divisor function, we have $2^{\omega(|m|)} \leq \tau(|m|) \leq |m|^{o(1)}$ (see Theorem 315 in [HW08] for this last bound on τ). Since the multiplicative group mod m has a direct product decomposition into at most $\omega(|m|) + 1$ cyclic groups (see for instance [IR90, Theorem 3, p. 44]),

$$N \leq d \cdot d^{\omega(|m|)} \leq d \cdot 2^{d\omega(|m|)} \leq d \cdot \tau(|m|)^d \leq |m|^{o(1)}.$$

Furthermore, Theorem 327 in [HW08] ensures that for sufficiently large $|m|$, we have $\varphi(|m|) \geq |m|^{0.99}$. Putting these estimates together, keeping in mind that $q_1, q_2 \leq |m|^{1/6}$, we see that the main term in the last display exceeds $m^{0.6}$ for large $|m|$, while the contribution of the O-terms is smaller than $m^{0.51}$ (say). In particular, the displayed expression is positive for all large $|m|$, allowing us to find our a', b'.

Finally we return to proving our choices of a and b satisfy part (iii) of Propositions 4 and 5. Suppose that $a = N(\alpha)$, with $\alpha \in \mathcal{O}$. We consider the prime factorization of $\alpha \mathcal{O}_K$ in the Dedekind domain $\mathcal{O}_K$. By our condition 3 above, $q_1 \parallel a$. Thus, the prime factorization of $\alpha \mathcal{O}_K$ contains a unique prime ideal Q_1 lying above q_1; furthermore, Q_1 has degree one. Then $\mathcal{O}_K / Q_1 \cong \mathbb{Z}/q_1\mathbb{Z}$, with the isomorphism induced by the inclusion of $\mathbb{Z}$ into $\mathcal{O}_K$. Since $m = (m^{1/d})^d$ is a dth power in $\mathcal{O}_K$, it is also a dth power in $\mathcal{O}_K/Q_1$ and thus in $\mathbb{Z}/q_1\mathbb{Z}$. But d is even, and so the stipulation that m is a quadratic nonresidue modulo q_1 implies that m is not a dth power modulo q_1. This contradiction establishes that a is not a norm in $\mathcal{O}$. An entirely analogous argument shows that $-b$ is not a

norm in $\mathcal{O}$. Here we use that $q_2 \parallel b$ (by condition 4 above) and that m is a quadratic nonresidue modulo q_2. □

We now settle Lemma 9. In view of Lemma 7, we may assume d is odd. We make use of the following GRH-conditional version of the Chebotarev density theorem:

Proposition 11. *Assume GRH. Let $E/\mathbb{Q}$ be a finite Galois extension of number fields, and let G be the Galois group of $E/\mathbb{Q}$. Let C be a subset of G that is invariant under conjugation. Let $\pi_C(x)$ denote the number of primes up to x whose associated Frobenius conjugacy class is in C. Let P be the product of the distinct rational primes ramifying in E. Then*

$$\left|\pi_C(x) - \frac{|C|}{|G|}\operatorname{Li}(x)\right| \leq A|C|x^{1/2}\log\left([E:\mathbb{Q}]Px\right)$$

for some absolute constant A.

Proposition 11 is the special case of Serre's [Ser81, eq. (20_R)] where $K = \mathbb{Q}$.

Proof of Lemma 9. Let $d > 1$ be odd, and let $p > 2$ be the least prime dividing d. Arguing as in the proof of Lemma 7, it is enough to show that there are two primes $q_1 < q_2 \leq |m|^{1/6}$, not dividing m, modulo which m is not a pth power.

We let $\zeta_p = \mathrm{e}^{2\pi i/p}$ and we consider $E := \mathbb{Q}(m^{1/p}, \zeta_p)$, the splitting field of the polynomial $T^p - m$. As E is the normal closure of $K := \mathbb{Q}(m^{1/p})$, every prime ramifying in E divides $\operatorname{disc}(K)$, which in turn divides $\operatorname{disc}(T^p - m) = (-1)^{(p-1)/2}p^p m^{p-1}$. Hence: Every prime ramifying in E divides mp. This observation will be useful momentarily when we apply Proposition 11.

Let q be a prime not dividing mp. In order that m not be a pth power modulo q, it is sufficient that the action of the Frobenius conjugacy class associated to q, on the roots of $T^p - m$, have no fixed points. We let C be the (conjugation-invariant) set of fixed-point-free elements of G.

The Galois group G of $E/\mathbb{Q}$ is made up of $p(p-1)$ elements $\sigma_{j,k}$ for $0 \leq j \leq p-1$, $1 \leq k \leq p-1$, determined by the conditions that $\sigma_{j,k}(m^{1/p}) := m^{1/p}\zeta_p^j$, $\sigma_{j,k}(\zeta_p) := \zeta_p^k$. Furthermore, it is straightforward to check that the set C defined above is precisely the collection of $\sigma_{j,1}$ with $j \neq 0$. Hence, $|C|/|G| = 1/p$.

Applying Proposition 11, we conclude that $|\pi_C(x) - \frac{1}{p}\operatorname{Li}(x)| \leq A_d x^{1/2}\log|pmx|$ for some constant A_d depending only on d. It follows that

$$\pi_C(x) \geq \frac{1}{p}\operatorname{Li}(x) - A_d x^{1/2}\log|pmx|. \tag{6}$$

It is certainly possible to choose our two primes q_1, q_2 as long as

$$\pi_C(|m|^{1/6}) \geq 2 + \omega(p|m|). \tag{7}$$

We will show this inequality holds for $x = (\log|m|)^3$, provided m is large enough. As $(\log|m|)^3 \leq |m|^{1/6}$ for large $|m|$, this suffices.

Allowing implied constants to depend on d (which is fixed), we have $\operatorname{Li}(x) \gg \log^3|m|/\log\log|m|$, while $x^{1/2}\log|pmx| \ll \log^{5/2}|m|$. Hence, (6) yields $\pi_C(x) \gg \log^3|m|/\log\log|m|$ for large $|m|$. On the other hand, $\omega(p|m|) \ll \log|m|$, which is of smaller order. Thus (7) holds whenever $|m|$ is sufficiently large, as desired. □

References

[Ega84] S. Egami, *On finiteness of the numbers of Euclidean fields in some classes of number fields*, Tokyo J. Math. **7** (1984), 183–198.

[EK38] P. Erdös and C. Ko, *Note on the Euclidean Algorithm*, J. London Math. Soc. **13** (1938), 3–8.

[Hei38] H. Heilbronn, *On Euclid's algorithm in real quadratic fields*, Proc. Camb. Philos. Soc. **34** (1938), 521–526.

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

[IR90] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990.

[JQS85] D. H. Johnson, C. S. Queen, and A. N. Sevilla, *Euclidean real quadratic number fields*, Arch. Math. (Basel) **44** (1985), 340–347.

[Pol17] P. Pollack, *Bounds for the first several prime character nonresidues*, Proc. Amer. Math. Soc. **145** (2017), 2815–2826.

[Ser81] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 123–201.

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

Email address: paco@uga.edu

Department of Mathematics and Statistics, California State University, Chico, Chico, CA 95929

Email address: kmcgown@csuchico.edu

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

Email address: pollack@uga.edu

Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, IL 60045

Email address: trevino@lakeforest.edu