A POSITIVE PROPORTION OF CUBIC FIELDS ARE NOT MONOGENIC YET HAVE NO LOCAL OBSTRUCTION TO BEING SO

LEVENT ALPÖGE, MANJUL BHARGAVA, AND ARI SHNIDMAN

Abstract. We show that a positive proportion of cubic fields are not monogenic, despite having no local obstruction to being monogenic. Our proof involves the comparison of 2-descent and 3-descent in a certain family of Mordell curves $E_k\colon y^2 = x^3 + k$. As a by-product of our methods, we show that, for every $r \geq 0$, a positive proportion of curves E_k have Tate–Shafarevich group with 3-rank at least r.

1. Introduction

One of the most common errors made in a first course in algebraic number theory is the assumption that every number field K is *monogenic*, i.e., that the ring of integers $\mathcal{O}_K$ of K is of the form $\mathbb{Z}[\alpha]$ for some $\alpha \in K$. While this assertion is true for quadratic fields, it is expected to be false for 100% of number fields of any given degree $d \geq 3$, although this expectation has not been proven for any d.

It is easy to construct number fields that fail to be monogenic for *local* reasons. The first example of such a non-monogenic number field was given by Dedekind, who showed that the field $\mathbb{Q}[x]/(x^3 - x^2 - 2x - 8)$, in which 2 splits completely, is not monogenic [12]. His result is a special case of the assertion that: if 2 splits completely in a number field K of degree $d \geq 3$, then K cannot be monogenic. Indeed, if $\mathcal{O}_K \cong \mathbb{Z}[x]/(f(x))$ for a monic integral polynomial $f(x)$ of degree $d \geq 3$, then 2 factors in $\mathcal{O}_K$ as $f(x)$ factors (mod 2); but f cannot split completely (mod 2), as there are only two monic linear polynomials (mod 2).

However, it has not previously been known even that a positive proportion of number fields of degree $d \geq 3$, *that have no local obstruction to being monogenic*, are not monogenic. The purpose of this paper is to prove this result in the case $d = 3$, i.e., for cubic fields.

Theorem 1. *When isomorphism classes of cubic fields are ordered by absolute discriminant, a positive proportion are not monogenic and yet have no local obstruction to being monogenic.*

In other words, we prove that a positive proportion of cubic fields, up to isomorphism, are non-monogenic for truly global reasons. In fact we produce such positive proportions of cubic fields having both possible real signatures.

It is interesting to note that the condition of having *no local obstruction to being monogenic* is stronger than the condition of being *locally monogenic*!

Definition 2. A number field K is *locally monogenic at p* if $\mathcal{O}_K \otimes \mathbb{Z}_p$ is generated by one element as a $\mathbb{Z}_p$-algebra; it is called *locally monogenic* if it is locally monogenic at all p.

However, it is possible for a number field to *have a local obstruction to being monogenic* even if it is locally monogenic! The obstruction comes from the *index form* $f_K : \mathcal{O}_K/\mathbb{Z} \to \wedge^d \mathcal{O}_K$ given by $\alpha \mapsto 1 \wedge \alpha \wedge \alpha^2 \wedge \cdots \wedge \alpha^{d-1}$. A choice of $\mathbb{Z}$-basis for $\mathcal{O}_K$ induces an isomorphism $\wedge^d \mathcal{O}_K \simeq \mathbb{Z}$, and, via this isomorphism, f_K may be viewed as a homogeneous form of degree $\binom{d}{2}$ in $d-1$ variables. Then the number field K is monogenic if and only if f_K represents ± 1 over $\mathbb{Z}$. In terms of f_K, the number field K is locally monogenic at p if and only if f_K represents a unit over $\mathbb{Z}_p$, but this does not imply that f_K represents ± 1 over $\mathbb{Z}_p$.

Definition 3. We say that K *has no local obstruction to being monogenic* if f_K represents 1 over $\mathbb{Z}_p$ for all primes p or represents -1 over $\mathbb{Z}_p$ for all primes p.

See §2.3 for an example of a number field that is locally monogenic but nevertheless has a local obstruction to being monogenic. Note that the index form of a number field $K \neq \mathbb{Q}$ always represents $+1$ and -1 over $\mathbb{R}$, so we need not consider obstructions over $\mathbb{R}$.

We now specialize to the case of cubic fields K, so that f_K is then an integral binary cubic form. The following theorem gives the proportion of cubic fields that are locally monogenic, as well as the proportion of those that have no local obstruction to being monogenic.

Theorem 4. *When isomorphism classes of either totally real or complex cubic fields are ordered by absolute discriminant:*

(*a*) *the proportion of these cubic fields that are locally monogenic is* $19/21 \approx 90.48\%$*;*

(*b*) *the proportion of these cubic fields that have no local obstruction to being monogenic is*

$$\frac{19}{21} \cdot \frac{316}{351} \cdot \frac{965}{1026} \cdot \prod_{\substack{p \equiv 1 \pmod 6 \\ p \neq 7}} \left(1 - \frac{2}{3(p^2+p+1)}\right) \approx 75.99\%.$$

Theorem 1 thus shows, for the first time, that a positive proportion of the set of cubic fields in Theorem 4(a) and indeed in Theorem 4(b) are not monogenic. The analogous result for cubic orders was proved by Akhtari and the second author [2], but these orders were not maximal due to the methods employed there involving the study of Thue equations.

While previous work on the monogenicity of general number rings and fields has focused on solving integral Thue equations and index form equations through techniques of Diophantine approximation (cf. [1, 2, 4, 5, 15, 16, 17, 18, 19, 22, 25]), our method instead involves a careful study of rational points on related genus one curves. Namely, we study the index forms f_K by comparing 2-descent and 3-descent in the family of Mordell curves $E_k : y^2 = x^3 + k$, as k ranges over certain sets of integers defined by congruence conditions, as studied in [3] and [7], respectively. As a by-product, we prove the following theorem.

Theorem 5. *When* $\mathrm{GL}_2(\mathbb{Z})$*-classes of integral binary cubic forms* $f(x,y)$ *are ordered by absolute discriminant, a positive proportion of the genus one curves* $z^3 = f(x,y)$ *over* $\mathbb{Q}$ *fail the Hasse principle.*

The same statement remains true even if one restricts just to index forms $f_K(x,y)$ *of cubic fields* K*: when isomorphism classes of cubic fields* K *are ordered by absolute discriminant, a positive proportion of the corresponding genus one curves* $C_K \colon z^3 = f_K(x,y)$ *over* $\mathbb{Q}$ *fail the Hasse principle.*

Our proof of Theorem 5 also implies the following statement regarding the Tate–Shafarevich groups $Ш(E_k)$ of the elliptic curves E_k:

Theorem 6. *Fix $r \geq 0$. For a positive proportion of k, we have* $\dim_{\mathbb{F}_3} Ш(E_k)[3] \geq r$.

In fact, our proof implies that the same statement remains true if one ranges over just the integers k satisfying any finite set of congruences, or even if one ranges over those integers k that are cubefree and satisfy any further finite set of congruence conditions.

Methods. To prove Theorem 1, we must bound how often the Thue equation $f_K(x, y) = 1$ has integer solutions as K ranges over (isomorphism classes of) cubic fields ordered by absolute discriminant. This equation defines a genus one curve $C_K : z^3 = f_K(x, y)$ in $\mathbb{P}^2$, and an integer solution gives rise to a rational point P_K on the Jacobian of C_K, namely the elliptic curve $E^D : y^2 = 4x^3 + D$ where $D = \mathrm{Disc}(K)$. The class of P_K in $E^D(\mathbb{Q})/3E^D(\mathbb{Q})$ depends only on K, and different cubic fields give rise to different classes. More generally, if K has no local obstruction to being monogenic, then C_K determines a class in the 3-Selmer group $\mathrm{Sel}_3(E^D)$, and different cubic fields yield distinct Selmer classes [27, §1].

The motivation and starting point for our proof is recent work of the second and third author and Elkies [7], where it was shown that there is a partition $\bigcup_{m\in\mathbb{Z}} T_m$ of $\mathbb{Z}$, with each T_m defined by congruence conditions, such that if S is any "large" subset of T_m, then the average size of $\mathrm{Sel}_3(E^D)$, as D varies over S, is at least $1 + 3^m$. Hence if $S \subset T_m$ is a set of cubic field discriminants with m large, then as D ranges over S, $\mathrm{Sel}_3(E^D)$ is very large on average.

This suggests that we may prove Theorem 1 by showing that:

(a) there are many cubic fields of discriminant D, for many discriminants $D \in S$, that have no local obstruction to being monogenic; and

(b) the ranks of many of the curves E^D for $D \in S$ are small.

Suitably strong and coordinated versions of (a) and (b) would imply Theorem 1: indeed, (a) would supply a large number of cubic fields across discriminants that have no local obstruction to being monogenic; on the other hand, these cubic fields could not all be monogenic—and thereby yield rational points on elliptic curves E^D—due to the ranks of many of these E^D being too small by (b).

Towards (b), we apply a recent result of the first author [3, Thm. 3.1.1]—extending a result of Ruth [26] and using a refinement of the circle method due to Heath-Brown [23]—which states that the average size of the 2-Selmer groups $\mathrm{Sel}_2(E^D)$, over any large set S of D defined by congruence conditions, is 3, irrespective of the congruence conditions. This gives an upper bound on the average size of $2^{\mathrm{rk}\, E^D}$ for D in any large set S defined by congruence conditions. This yields quite a strong version of (b).

Regarding (a), a first natural approach is to try and apply the asymptotic count of cubic fields due to Davenport–Heilbronn [11]. However, this does not yield a strong enough version of (a) to show, in conjunction with our version of (b), that many cubic fields (with no local obstruction to being monogenic) are not monogenic. Indeed, to obtain an upper bound on the globally soluble part of $\mathrm{Sel}_3(E^D)$, we would need an upper bound on the average size of $3^{\mathrm{rk}\, E^D}$. But $3 > 2$, so our upper bound on the average size of $2^{\mathrm{rk}\, E^D}$ does not suffice.

To remedy this, we construct explicit large subsets $S \subset T_m$, defined by congruence conditions, with the following two properties. First, each cubic field of discriminant $D \in S$

has no local obstruction to being monogenic. Second, there is a subset $S' \subset S$ of relative density $\mu \geq 1/2$ such that there are *at least* 2^{m-1} cubic fields of each discriminant $D \in S'$.

The construction of S involves two steps. First, we use a theorem of the second author and Varma [9] guaranteeing vanishing of the 3-parts of class groups of the fields $\mathbb{Q}(\sqrt{-3D})$ (when $D > 0$) or $\mathbb{Q}(\sqrt{D})$ (when $D < 0$) whenever $D \in S' \subset S$, where S' has relative density at least $1/2$ in S. We then use a higher composition law (when $D > 0$) and class field theory (when $D < 0$) to prove that there are *exactly* 2^{m-1} (resp. $3 \cdot 2^{m-1}$) cubic fields of discriminant D when $D \in S'$ and $D > 0$ (resp. $D < 0$). This yields our desired version of (a).

Now, were 100% of cubic fields of discriminant $D \in T_m$ monogenic, one would find that the ranks of $E^D(\mathbb{Q})$ for $D \in S'$ would all be at least $m \log_3 2$, since we produce at least $2 \cdot 2^{m-1}$ distinct elements $\pm P_K \in E^D(\mathbb{Q})/3E^D(\mathbb{Q})$ for each such D. This would force the average of $\#\mathrm{Sel}_2(E^D)$, for $D \in S$, to be at least $\mu \cdot 2^{m \log_3 2} \geq 2^{m \log_3 2 - 1}$, which for m sufficiently large is strictly larger than 3, contradicting the aforementioned [3, Thm. 3.1.1]. This proves Theorem 1.

In particular, the Hasse principle thus fails for many genus one curves of the form $z^3 = f_K(x, y)$ with $\mathrm{Disc}(K) \in S$, thereby proving Theorem 5. These curves represent elements of the Tate–Shafarevich group of $E^{\mathrm{Disc}(K)}$, so that once m is sufficiently large we also deduce Theorem 6.

This paper is organized as follows. In §2, we prove Theorem 4 by suitably applying the results of Davenport–Heilbronn [11] and their refinements in [8]. In §3.1 and §3.2, we recall from [3] and [7] the relevant definitions and results regarding 2- and 3-Selmer groups of the curves $E_k : y^2 = x^3 + k$, as k varies over suitable congruence families, and we describe their connections to monogenicity. In §3.3, we prove our formulas for the number of cubic fields of given discriminant in S', which we then use in §3.4 and §3.5 to compare 2- and 3-descent on E_k, thus deducing Theorems 1, 5, and 6.

Acknowledgments. The authors thank Arul Shankar for many helpful comments on earlier versions of this manuscript, and Michael Stoll for organizing Rational Points 2017 and 2019, which provided the pleasant environment where the authors first had the idea for this work. The first author also thanks David Harari, Emmanuel Peyre, and Alexei Skorobogatov for organizing the similarly invigorating Reinventing Rational Points program. The second author thanks Professor John Tate for posing this problem to him when he was in graduate school. The first author was supported by NSF grant DMS-2002109. The second author was supported by a Simons Investigator Grant and NSF grant DMS-1001828. The third author was supported by the Israel Science Foundation (grant No. 2301/20).

2. The proportion of cubic fields that are locally monogenic, and the proportion that have no local obstruction to being monogenic

Let $V(\mathbb{Z}) = \mathrm{Sym}^3 \mathbb{Z}^2$ be the space of binary cubic forms over $\mathbb{Z}$. Recall that there is a discriminant-preserving bijection between $\mathrm{GL}_2(\mathbb{Z})$-orbits on $V(\mathbb{Z})$ and isomorphism classes of cubic rings over $\mathbb{Z}$, i.e., rings that are free of rank 3 as $\mathbb{Z}$-modules, due to Levi [24], Delone–Faddeev [13], and Gan–Gross–Savin [20, §4]. Namely, a cubic ring R corresponds to the $\mathrm{GL}_2(\mathbb{Z})$-orbit of its index form $f_R\colon R/\mathbb{Z} \to \wedge^3 R$.

The number of $\mathrm{GL}_2(\mathbb{Z})$-classes of irreducible binary cubic forms having bounded absolute discriminant satisfying certain allowable sets of congruences was determined by Davenport and Heilbronn [11]:

Theorem 7 (Davenport–Heilbronn [11])**.** *Let S be a $\mathrm{GL}_2(\mathbb{Z})$-invariant set of integral binary cubic forms f defined by congruence conditions modulo bounded powers of primes p where, for sufficiently large p, the defining congruence conditions at p exclude only a set of forms f satisfying $p^2 \mid \mathrm{Disc}(f)$. Let $h(S;D)$ denote the number of classes of irreducible binary cubic forms that are contained in S and have discriminant D. Then:*

(a) $$\sum_{-X<D<0} h(S;D) \sim \frac{\pi^2}{24}\cdot X \cdot \prod_p \mu_p(S);$$

(b) $$\sum_{0<D<X} h(S;D) \sim \frac{\pi^2}{72}\cdot X \cdot \prod_p \mu_p(S),$$

where $\mu_p(S)$ denotes the p-adic density of S in the space of integral binary cubic forms.

To prove Theorem 4(a) (resp. Theorem 4(b)), we shall apply Theorem 7 with S the set of integral binary cubic forms that are index forms of a cubic field and, furthermore, represent a unit over $\mathbb{Z}_p$ for all p (resp. represent 1 over $\mathbb{Z}_p$ for all p). Note that a binary cubic form over a ring R represents 1 over R if and only if it represents -1.

2.1. **The density of index forms of cubic fields that locally represent a unit.** We follow the arguments of [8, §4], keeping track of those integral binary cubic forms that represent a unit. We use the following elementary lemma whose proof is immediate:

Lemma 8. *A binary cubic form f over $\mathbb{Z}_p$ represents a unit in $\mathbb{Z}_p$ if and only if f is primitive and furthermore, if $p=2$, then $f(x,y)\not\equiv xy(x+y) \pmod 2$.*

The condition of primitivity is automatically satisfied for index forms of cubic fields. Thus the only modification to the computations of [8, §4] that must be made to determine the density of index forms of cubic fields that locally represent a unit is the elimination of the splitting type (111) at the prime $p=2$. By [8, Lem. 19], the total local p-adic density $\mu_p(\mathcal{U})$ of the set of index forms is $(p^2-1)(p^3-1)/p^5$ (which is $21/32$ for $p=2$), while by the first line of [8, Lem. 18], the portion of this density corresponding to the splitting type (111) is $\frac{1}{6}(p-1)^2(p+1)/p^3$ (which is $2/32$ for $p=2$). Thus the Euler factor for $p=2$ in Theorem 7 changes from $21/32$ to $19/32$. We conclude that the proportion of index forms of cubic fields that locally represent a unit is $19/21$. We have proven Theorem 4(a).

2.2. **The density of index forms of cubic fields that locally represent 1.** We use the following lemma, which is a slight correction of [2, Lem. 4.1] at the prime $p=7$:

Lemma 9. *A primitive binary cubic form f over $\mathbb{Z}_2$ represents 1 if and only if $f(x,y)\not\equiv xy(x+y) \pmod 2$. If $p\equiv 1 \pmod 6$, then a primitive binary cubic form f over $\mathbb{Z}_p$ represents 1 if and only if $f(x,y)\not\equiv cL(x,y)^3 \pmod p$, where L is a linear form and c is a non-cube modulo p, and furthermore, if $p=7$, then $f(x,y)$ is not equivalent to $2xy(x+y)$ $\pmod 7$ under a linear change of variable. Finally, if $p\equiv 5 \pmod 6$, then every primitive binary cubic form f over $\mathbb{Z}_p$ represents 1.*

Proof. The proof of [2, Lem. 4.1] is correct except for a small oversight in the case $p \equiv 1 \pmod 6$ when $p = 7$. In that case, the Hasse-Weil bound shows that a smooth genus one curve $z^3 = f(x, y)$ has at least 3 points over $\mathbb{F}_7$, but these three points might all satisfy $z = 0$, so that $f(x, y)$ might *not* represent a unit cube, and therefore 1, over $\mathbb{F}_7$. Such a scenario can occur only if $f(x, y)$ splits completely over $\mathbb{F}_7$. All such forms over $\mathbb{F}_7$ are $\mathrm{GL}_2(\mathbb{F}_7)$-equivalent to $cxy(x + y)$, for some $c \in \mathbb{F}_7^\times$. Since c can be scaled by any unit cube by scaling x and y by a unit, we may assume that $c = 1$, 2, or 3, as ± 1 are the only cubes in $\mathbb{F}_7^\times$. Of these three possibilities, only $c = 2$ yields a binary cubic form over $\mathbb{F}_7$ that does not represent a unit cube. □

We also have the following analogue of Lemma 9 for index forms over $\mathbb{Z}_3$:

Lemma 10. *The index form f of a maximal cubic ring over $\mathbb{Z}_3$ represents 1 over $\mathbb{Z}_3$ if and only if f is not equivalent over $\mathbb{Z}/9\mathbb{Z}$ to $cxy(x+y)$, $2cx^3 - 3xy^2 + 3y^3$, or $2cx^3 - 3x^2y + 3y^3$ for $c = 1$ or 2.*

Proof. The cubes in $\mathbb{Z}_3^\times$ are $\pm 1 + 9\mathbb{Z}_3$, so it suffices to consider the index forms modulo 9. Forms of type (111) are equivalent to $cxy(x + y)$, which represents 1 only when $c \equiv \pm 4 \pmod 9$. Meanwhile, index forms of type (12), (3), and $(1^2 1)$ are equivalent to $x(x^2 + y^2)$, $x^3 - xy^2 + y^3$, and $x^2 y$, respectively, and these all represent $1 \pmod 9$.

Index forms of type (1^3) can naturally be subdivided into 3 subtypes based on the 3-adic valuations of their discriminants. Those with valuation 3 are equivalent to $c(x^3 + 3xy^2 + 3y^3)$ or $c(x^3 - 3xy^2 + 3y^3)$, and these forms represent 1 unless c is ± 2 or $\pm 4 \pmod 9$, respectively. Index forms f of valuation 4 come in two types. If $\mathrm{Gal}(f) \simeq S_3$, then, up to equivalence, $f(x, y) \equiv c(x^3 + 3x^2 y + 3y^3) \pmod 9$, which represents $1 \pmod 9$. If $\mathrm{Gal}(f) \simeq C_3$, then up to equivalence $f \equiv c(x^3 - 3x^2 y + 3y^3) \pmod 9$, which represents 1 if and only if $c \equiv \pm 1 \pmod 9$. Finally, those with valuation 3^5 are equivalent to $ax^3 + 3dy^3$, with a and d units, which all represent $1 \pmod 9$. □

To obtain the relative density at p of index forms that locally represent 1, we use Lemmas 9 and 10. At $p = 2$, we have already seen that the relative density is 19/21.

For primes $p \equiv 1 \pmod 6$ but $p \neq 7$, we use the fact that a relative density of 2/3 of index forms that have splitting type $(1^3) \pmod p$ do not represent 1 over $\mathbb{Z}_p$. By [8, Lem. 18], a density of $(p-1)^2(p+1)/p^5$ of binary cubic forms are index forms locally and have splitting type (1^3). Thus the desired relative density of index forms that represent 1 over $\mathbb{Z}_p$, for primes $p \pmod 6$ and $p \neq 7$, is

$$1 - \frac{2}{3} \cdot \frac{(p-1)^2(p+1)/p^5}{(p^2-1)(p^3-1)/p^5} = 1 - \frac{2}{3(p^2+p+1)}.$$

If $p = 7$, we must further subtract the relative density of index forms that split completely over $\mathbb{F}_7$ and do not represent 1 over $\mathbb{Z}_7$, which as we have seen is 1/3 of all forms that split completely over $\mathbb{F}_7$. The desired relative density of index forms that represent 1 over $\mathbb{Z}_7$ is thus

$$1 - \frac{2}{3(p^2+p+1)} - \frac{1}{3} \cdot \frac{(1/6)(p-1)^2(p+1)/p^3}{(p^2-1)(p^3-1)/p^5} = 1 - \frac{p^2+12}{18(p^2+p+1)} = \frac{965}{1026}$$

when $p = 7$.

If $p \equiv 5 \pmod 6$, then every index form represents 1 over $\mathbb{Z}_p$.

Finally, if $p = 3$, then 1/3 of forms of type (111) represent 1 over $\mathbb{Z}_3$ by Lemma 10. Among index forms of type (1^3), those with discriminant of valuation 5 have density 1/9 since they have a triple root modulo 9, not just modulo 3, and these all represent 1 over $\mathbb{Z}_3$. Among the remaining 8/9 of forms of type (1^3), we claim that a proportion of 2/3 represent 1 over $\mathbb{Z}_3$. This is true for those with discriminant of valuation 3 by Lemma 10. There are three cubic extensions of $\mathbb{Q}_3$ with discriminant of valuation 4 with Galois group C_3 and one with Galois group S_3. Thus, when weighted appropriately, there is the same proportion of each type. By the proof of Lemma 10, the proportion of these forms that represent 1 over $\mathbb{Z}_3$ is $\frac{1}{2}\left(\frac{1}{3}+1\right) = \frac{2}{3}$, as claimed. Thus the desired relative density of index forms f_K that represent 1 over $\mathbb{Z}_3$ is

$$1 - \frac{2}{3}\cdot\frac{(1/6)(p-1)^2(p+1)p^2}{(p^2-1)(p^3-1)} - \frac{1}{3}\cdot\frac{8}{9}\cdot\frac{(p-1)^2(p+1)}{(p^2-1)(p^3-1)} = \frac{316}{351}$$

when $p = 3$. We have proven Theorem 4(b).

2.3. **A cubic field that is locally monogenic but has a local obstruction to being monogenic.** The cubic field $K = \mathbb{Q}[X]/(X^3 - 7/5)$ has ring of integers $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\cdot 5\theta + \mathbb{Z}\cdot 5\theta^2$, where θ is the image of X. The index $f_K(x,y)$ of $x\cdot 5\theta + y\cdot 5\theta^2$ is given by $f_K(x,y) = 5x^3 - 7y^3$, which does not represent ± 1 over $\mathbb{F}_7$, let alone over $\mathbb{Z}_7$ or $\mathbb{Z}$. However, K is locally monogenic; for example, $\mathcal{O}_K \otimes \mathbb{Z}_7 = \mathbb{Z}_7[\theta]$. Thus K has a local obstruction to being monogenic, despite being locally monogenic.

On the other hand, consider $K' = \mathbb{Q}[X]/(X^3 - 21)$, which has a monogenic ring of integers $\mathcal{O}_{K'} = \mathbb{Z}[\sqrt[3]{21}]$. Then $f_{K'}(x,y) = x^3 - 21y^3$, which represents 1 over $\mathbb{Z}_7$ and indeed over $\mathbb{Z}$. Note that $\mathcal{O}_K \otimes \mathbb{Z}_7 \simeq \mathcal{O}_{K'} \otimes \mathbb{Z}_7$, but K has a local obstruction to being monogenic over $\mathbb{Z}_7$ while K' does not. Thus the property of having a local obstruction to being monogenic is not solely a property of the localization $K \otimes \mathbb{Q}_p$, but is also a property of the localization of the global index form.

Remark 11. Isomorphism classes of cubic rings over a principal ideal domain R (i.e., R-algebras that are free of rank 3 as modules over R) are parametrized by orbits of binary cubic forms over R under the "twisted" action of $\mathrm{GL}_2(R)$ rather than the "standard" action; see [21, Prop. 2.1]. The *standard* action of $\gamma \in \mathrm{GL}_2(R)$ on a binary cubic form f with coefficients in R (which we use in this paper throughout) is given by

$$\gamma \cdot f(x,y) := f((x,y)\gamma), \tag{2.1}$$

while the *twisted* action is given by

$$\gamma \star f(x,y) := \det(\gamma)^{-1} f((x,y)\gamma), \tag{2.2}$$

where we view (x,y) as a row vector.

For binary cubic forms over $R = \mathbb{Z}$, the standard and twisted $\mathrm{GL}_2(R)$-orbits are identical, but for $R = \mathbb{Z}_p$ they may not be. The property of whether or not a binary cubic form f represents 1 over $\mathbb{Z}_p$ is preserved under standard $\mathrm{GL}_2(\mathbb{Z}_p)$-equivalence but not necessarily under twisted $\mathrm{GL}_2(\mathbb{Z}_p)$-equivalence. This explains, in terms of binary cubic forms, why two cubic fields may have isomorphic completions at a prime p, and both may be locally monogenic at p, but only one may have a local obstruction to being monogenic at p.

The cubic fields K and K' above have this property; the corresponding binary cubic forms $5x^3 - 7y^3$ and $x^3 - 21y^3$, when viewed in $\mathbb{Z}_7[x, y]$, are not standard $\mathrm{GL}_2(\mathbb{Z}_7)$-equivalent, and indeed represent different cube classes in $\mathbb{Z}_7$, but they are twisted $\mathrm{GL}_2(\mathbb{Z}_7)$-equivalent, and thus correspond to the same cubic ring over $\mathbb{Z}_7$.

3. A positive proportion of cubic fields have no local obstruction to being monogenic but are not monogenic

3.1. 2-Selmer groups of the elliptic curves E^D.

Recall that the 2-Selmer group of an elliptic curve E over $\mathbb{Q}$ is defined by

$$\mathrm{Sel}_2(E) := \ker\Big(H^1(\mathbb{Q}, E[2]) \to \prod_{p\leq\infty} H^1(\mathbb{Q}_p, E)\Big)$$

and sits in an exact sequence

$$0 \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E) \to \text{Ш}(E)[2] \to 0.$$

In particular, we have $\#\mathrm{Sel}_2(E) \geq 2^{\mathrm{rk}\, E} \cdot \#E(\mathbb{Q})[2]$, where $\mathrm{rk}\, E$ is the rank of the finitely-generated abelian group $E(\mathbb{Q})$.

Recall the elliptic curve $E^D\colon y^2 = 4x^3 + D$. We require a bound on the average size of $\mathrm{Sel}_2(E^D)$ as D varies through certain sets $\Sigma \subset \mathbb{Z}$ defined by congruence conditions. We define the *average* $\mathrm{avg}_\Sigma(f)$ of a function f on Σ with respect to the natural density, i.e.,

$$\mathrm{avg}_\Sigma(f) = \lim_{X\to\infty} \frac{1}{\#\Sigma(X)} \sum_{D\in\Sigma(X)} f(D),$$

where $\Sigma(X) := \Sigma \cap [-X, X] \setminus \{0\}$.

Definition 12. A set $\Sigma \subset \mathbb{Z}$ is *defined by congruence conditions* if there is a set $\Sigma_\infty \in \{\mathbb{R}_{>0}, \mathbb{R}_{<0}, \mathbb{R}^\times\}$ and for each prime p there is an open and closed subset $\Sigma_p \subset \mathbb{Z}_p$ such that $\Sigma = \cap_p(\mathbb{Z} \cap \Sigma_p) \cap \Sigma_\infty$. If, moreover, $\Sigma \neq \emptyset$ and

$$\Sigma_p \supset \{D\colon v_p(D) \leq 1\}$$

for all sufficiently large p, then Σ is called *large*.

The following is a special case of a theorem of the first author [3, Thm. 3.1.1], which in turn is an extension of Ruth's Ph.D. thesis [26] who proved that $\mathrm{avg}_{\mathbb{Z}} \#\mathrm{Sel}_2(E^D) \leq 3$.

Theorem 13. *Let $\Sigma \subset \mathbb{Z}$ be a large set defined by congruence conditions. Then*

$$\mathrm{avg}_\Sigma \#\mathrm{Sel}_2(E^D) = 3.$$

Corollary 14. *The average rank of E^D, as D ranges over any large set Σ, is at most $3/2$.*

Proof. We have $\mathrm{avg}_\Sigma(2\,\mathrm{rk}\, E^D) \leq \mathrm{avg}_\Sigma(2^{\mathrm{rk}\, E^D}) \leq \mathrm{avg}_\Sigma\#\mathrm{Sel}_2(E^D) = 3.$ □

3.2. **3-isogeny Selmer groups of the elliptic curves E^D.** Let F be a field of characteristic not 2 or 3. For any nonzero $D \in F$, there is a degree-3 isogeny $\phi_D \colon E^D \to E^{-27D}$ whose kernel is generated by $(0, \pm\sqrt{D})$. More generally, if $f \in V(F)$ is a binary cubic form of discriminant D, then the plane cubic curve $C_f \colon z^3 = f(x,y)$ admits the degree 3 map $\phi_f \colon C_f \to E^{-27D}$ given by

$$[x\colon y\colon z] \mapsto \left(\frac{-h(x,y)}{z^2}, \frac{g(x,y)}{z^3}\right),$$

where $h(x,y) = \frac{1}{4}\left(f_{xx}f_{yy} - f_{xy}^2\right)$ is the Hessian of f and $g(x,y) = f_x h_y - f_y h_x$ is the Jacobian derivative of f and h (see [7, Rem. 31]). When $f(x,y) = x^2y - (D/4)y^3$, or more generally when f is in the unique $\mathrm{SL}_2(F)$-orbit of *reducible* forms of discriminant D, we have $C_f \simeq E^D$ and we define $\phi_D = \phi_f$. Since any f is reducible over the separable closure $\bar{F}$, we see that E^D is the Jacobian of C_f, and ϕ_f is a twist of ϕ_D. If K/F is a cubic extension and $f = f_K$ is the corresponding index form, we write $\phi_K = \phi_f$ and $C_K = C_f$.

Since $\mathrm{Aut}(\phi_D) = E^D[\phi_D]$, the twists of ϕ_D are parametrized by the $\mathbb{F}_3$-vector space $H^1(F, E^D[\phi_D])$. Thus, each cubic extension K/F with discriminant (in the square class of) D gives rise to a pair of nonzero classes $\pm\alpha_K \in H^1(F, E^D[\phi_D])$ corresponding to the class of ϕ_K. There are two classes because there are two $\mathrm{SL}_2(F)$-orbits of discriminant D in the $\mathrm{GL}_2(F)$-orbit of f. The genus one curves corresponding to α_K and $-\alpha_K$ are isomorphic, so we can unambiguously write C_K.

Lemma 15. *If K and K' are non-isomorphic cubic extensions of F of the same discriminant D, then α_K and $\alpha_{K'}$ are linearly independent in $H^1(F, E^D[\phi_D])$.*

Proof. Recall that $K \simeq F[x]/(f_K(x,1))$. Thus f_K is reducible over K, while $f_{K'}$ stays irreducible over K. Since the reducible orbit corresponds to the trivial class, this means α_K is in the kernel of $H^1(F, E^D[\phi_D]) \to H^1(K, E^D[\phi_D])$, while $\alpha_{K'}$ is not. □

Finally, we remark that the natural map $H^1(F, E^D[\phi_D]) \to H^1(F, E^D)$ sends the class of ϕ_f to the class of the twist C_f of E^D.

Now take $F = \mathbb{Q}$. The ϕ_D-Selmer group is defined by

$$\mathrm{Sel}_{\phi_D}(E^D) := \ker\Big(H^1(\mathbb{Q}, E^D[\phi_D]) \to \prod_p H^1(\mathbb{Q}_p, E^D)\Big).$$

The classes $\pm\alpha_K$ lie in $\mathrm{Sel}_{\phi_D}(E^D)$ if and only if $C_K(\mathbb{Q}_p) \neq \emptyset$ for all primes p.

The inclusion $E^D[\phi_D] \subset E^D[3]$ induces a map $\mathrm{Sel}_{\phi_D}(E^D) \to \mathrm{Sel}_3(E^D)$, which is injective if $\ker(\hat{\phi}_D)(\mathbb{Q}) = 0$, i.e., if $-27D$ is not a perfect square [7, Eq. (22)]. From the exact sequence

$$0 \to E^D(\mathbb{Q})/3E^D(\mathbb{Q}) \to \mathrm{Sel}_3(E^D) \to \text{Ш}(E^D)[3] \to 0,$$

we see that any class in $\mathrm{Sel}_{\phi_D}(E^D)$ such that $C_f(\mathbb{Q}) \neq \emptyset$ lies in the subgroup $E^D(\mathbb{Q})/3E^D(\mathbb{Q})$. In particular, if $-27D$ is not a perfect square and K is a monogenic cubic field of discriminant D, then E^D has rank at least 1.

Remark 16. If $D = -27n^2$, then the kernel of $\mathrm{Sel}_{\phi^D}(E^D) \to \mathrm{Sel}_3(E^D)$ has size 3, generated by the class of ϕ_f with $f(x,y) = x^3 + ny^3$. Its Hessian h is $9nxy$, and hence $\phi_f(1\colon 0\colon 1)$ is the rational 3-torsion point $(0, 27n)$ on $E^{-27D} = E^{3^6 n^2}$. In this special case, E^D can have rank 0 despite there being a monogenic cubic field of discriminant D; this occurs, for example, when $n = 5$.

For any large subset $\Sigma \subset \mathbb{Z}$, the second and third authors and Elkies computed the average size of $\mathrm{Sel}_{\phi_D}(E^D)$ for $D \in \Sigma$ in [7]. Unlike Theorem 13 for the 2-Selmer group, this average size is sensitive to the congruence conditions defining Σ. However, one can partition $\mathbb{Z}$ into sets T_m ($m \in \mathbb{Z}$) such that each T_m has positive density and, for any large subset $\Sigma \subset T_m$, the average size $\mathrm{avg}_\Sigma \#\mathrm{Sel}_{\phi_D}(E^D)$ is independent of Σ.

Theorem 17 ([7])**.** *Fix $m \in \mathbb{Z}$ and let $\Sigma \subset \mathbb{Z}$ be a large set contained in T_m. Then*

$$\mathrm{avg}_\Sigma \#\mathrm{Sel}_{\phi_D}(E^D) = 1 + 3^m.$$

The sets T_m are defined by infinitely many congruence conditions; we refer to [7] for the exact definition. The key point is that in order for D to lie in T_m, it must be divisible by n^2 for some n divisible by at least $|m| - 1$ primes $p \equiv 2 \pmod 3$.

This suggests that, to prove the existence of many non-monogenic cubic fields, one might focus on cubic fields of discriminant $D = dn^2$, with n divisible by many primes $p \equiv 2 \pmod 3$.

3.3. **Construction of cubic fields ramified at a fixed set of primes with no local obstruction to being monogenic.** To prove Theorem 1, we construct a subset $\Sigma \subset \mathbb{Z}$ for which we can guarantee the following:

(i) a cubic field K with $\mathrm{Disc}(K) \in \Sigma$ has no local obstruction to being monogenic; and
(ii) for a positive proportion of $D \in \Sigma$, there are "many" cubic fields of discriminant D.

To construct such Σ, we choose t distinct primes $p_1, \ldots, p_t$ each congruent to $2 \pmod 3$, and set $n = 3 \cdot \prod_{i=1}^t p_i$. It will be convenient to assume $p_1 = 2$, and we do so. For Theorem 1 we will simply take $t = 2$ and $n = 2 \cdot 3 \cdot 5 = 30$, but for Theorem 6 we will take t to be arbitrarily large.

Define the set of integers

$$\Sigma_n = \left\{ -27dn^2 \in \mathbb{Z} \colon d \text{ fundamental}, \left(\frac{d}{7}\right) \neq 1, \text{ and } \left(\frac{d}{p}\right) = 1 \text{ for all } p \mid n \right\},$$

where $\left(\frac{d}{p}\right)$ denotes the Kronecker symbol. Note that Σ_n has positive natural density.

Lemma 18. *If K is a cubic field and $\mathrm{Disc}(K) \in \Sigma_n$, then f_K represents 1 over $\mathbb{Z}_p$ for all p, i.e., K has no local obstruction to being monogenic.*

Proof. This follows from Lemmas 9 and 10. For $p \equiv 5 \pmod 6$ there is nothing to check. If $p \equiv 1 \pmod 3$ then $p^2 \nmid \mathrm{Disc}(f_K)$, and so f_K represents 1 over $\mathbb{Z}_p$ for all such $p > 7$. The 3-adic and 7-adic conditions imposed on d guarantee that f represents 1 over $\mathbb{Z}_3$ and $\mathbb{Z}_7$. Finally, f_K represents 1 over $\mathbb{Z}_2$ since it is primitive and $2 \mid \mathrm{Disc}(f_K)$. ☐

Let $\Sigma_n^\pm$ be the subset of $D \in \Sigma_n$ such that $\pm D > 0$. The next proposition shows that there are many cubic fields per discriminant in $\Sigma_n^\pm$, on average.

Proposition 19. *Let $\Sigma_n^\pm(X) = \Sigma_n^\pm \cap [-X, X]$, and let $N(\Sigma_n^\pm, X)$ be the number of cubic fields with discriminant in $\Sigma_n^\pm(X)$. Then*

$$\lim_{X\to\infty} \frac{N(\Sigma_n^\pm, X)}{\#\Sigma_n^\pm(X)} = (2 \mp 1)2^t,$$

Proposition 19 may be deduced from [8, Thm. 8]; we omit the details, as it is only suggestive of how to proceed but will not be used directly in what follows.

As explained in the introduction, average results such as Proposition 19 are not strong enough for our purposes. In the next two propositions, we provide exact formulas for the number of cubic fields of discriminant $D \in \Sigma_n$ for specific values of D, namely those D for which the 3-torsion in the class group of $\mathbb{Q}(\sqrt{D^*})$ is trivial, where $D^* = D$ or $-3D$ depending on whether $D < 0$ or $D > 0$. Moreover, we prove that the average values in Proposition 19 are actually attained on the nose for these individual discriminants.

Proposition 20. *Let $D \in \Sigma_n^+$ and write $F = \mathbb{Q}(\sqrt{-3D})$. If $\mathrm{Cl}(F)[3] = 0$, then there are exactly 2^t cubic fields of discriminant D.*

Proof. Let K be a cubic field of discriminant $D = -27dn^2 \in \Sigma_n^+$. Since $3^5 \mid \mathrm{Disc}(f_K)$, f_K has a triple root over $\mathbb{F}_3$, and hence its central coefficients are divisible by 3. Let S be the quadratic ring $\mathcal{O}_{dn^2}$ of discriminant dn^2, and let (S, I, δ) be the triple corresponding to f_K under the bijection of [6, Thm. 13]. Thus I is an S-ideal such that $I^3 \subset \delta S$ and $\mathrm{Nm}_S(I)^3 = \mathrm{Nm}(\delta)$.

The condition that f_K corresponds to a maximal cubic order is equivalent to the condition that I is also an ideal for the maximal order $\mathcal{O}_d = \mathcal{O}_F$. To see this, note that the latter is equivalent to the condition that the primitive part of the Hessian h of f_K has discriminant d; see [6, Eq. (24)]. Then note that $\mathrm{Disc}(h) = dn^2$ and h is a scalar multiple of n if and only if f_K has a triple root modulo each $p \mid n$.

The conditions $I^3 \subset \delta S$ and $\mathrm{Nm}_S(I)^3 = \mathrm{Nm}(\delta)$ are equivalent to the single condition $I^3 = nJ(\delta)$, for some $\mathcal{O}_d$-ideal J of norm n. Indeed, $\mathrm{Nm}_S(I)^3 = \mathrm{Nm}(I)^3/n^3$, so $\mathfrak{a} := I^3\delta^{-1}$ is an $\mathcal{O}_d$-ideal of norm n^3 contained in S. By the defining conditions of Σ_n^+, all primes $p \mid n$ split as $\mathfrak{p}\bar{\mathfrak{p}}$ in $\mathcal{O}_d$. Since $\mathfrak{p} \otimes \mathbb{Z}_p \neq S \otimes \mathbb{Z}_\mathfrak{p} \neq \bar{\mathfrak{p}} \otimes \mathbb{Z}_p$, the ideal $\mathfrak{a}$ must be divisible by n. Thus $I^3(n\delta)^{-1}$ is an $\mathcal{O}_d$-ideal of norm n. Thus each cubic field K of discriminant D gives rise to an $\mathcal{O}_d$-ideal J of norm n, together with a class $[I] \in \mathrm{Cl}(\mathcal{O}_d)$ which cubes to $[J]$.

Conversely, given a pair $(J, [I])$, where J is an $\mathcal{O}_d$-ideal of norm n and $[I]$ is an ideal class such that $[I]^3 = [J]$, we may write $I^3 = nJ(\delta)$, for some δ. Since $S^\times = \{\pm 1\}$, this δ is uniquely determined up to sign. Then the equivalence class of (S, I, δ) corresponds to a $\mathrm{GL}_2(\mathbb{Z})$-orbit of cubic forms, which itself corresponds to a maximal cubic order of discriminant $D = -27dn^2$. Thus, the bijection of [6, Thm. 13] induces a bijection:

$$\{\text{cubic fields } K\colon \mathrm{Disc}(K) = -27dn^2\}$$
$$\updownarrow$$
$$\{(J, [I])\colon J \text{ is an } \mathcal{O}_d\text{-ideal of norm } n \text{ and } [I]^3 = [J]\}/\sim,$$

where $\sim$ denotes $\mathrm{Gal}(\mathcal{O}_d/\mathbb{Z})$-conjugation. When $\mathrm{Cl}(F)[3] = 0$, every ideal class has a unique cube root, hence the data of $[I]$ is unnecessary. Since each $p \mid n$ splits in $\mathcal{O}_d$, there are

$\frac{1}{2}\cdot 2^{\omega(n)} = 2^t$ equivalence classes of ideals J of norm n, and hence 2^t cubic fields of discriminant $D = -27dn^2$. □

Proposition 21. *Let $D \in \Sigma_n^-$ and write $F = \mathbb{Q}(\sqrt{D})$. If $\mathrm{Cl}(F)[3] = 0$, then there are exactly $3 \cdot 2^t$ cubic fields of discriminant D.*

Proof. Write $D = -27dn^2$. By class field theory, the number of cubic fields with discriminant of the form $-3dm^2$, for some $m \mid 3n$, is the number of index 3 subgroups in the ring class group $\mathrm{Cl}(\mathcal{O}_D)$ of discriminant D [9, §5.1]. Since $\mathrm{Cl}(F)[3] = \mathrm{Cl}(\mathcal{O}_{-3D})[3] = 0$ and $D < 0$, the group $\mathrm{Cl}(\mathcal{O}_D)[3]$ is isomorphic to the 3-torsion subgroup of

$$\frac{(\mathcal{O}_F/3n)^\times}{(\mathbb{Z}/3n)^\times} \simeq \frac{(\mathcal{O}_F/9)^\times}{(\mathbb{Z}/9)^\times} \times \prod_{i=1}^{t} \frac{(\mathcal{O}_F/p_i)^\times}{(\mathbb{Z}/p_i)^\times}.$$

Note that each p_i is inert in F, by definition of Σ_n, whereas 3 ramifies. The 3-torsion subgroup of the right hand side is therefore isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^t$, since $p_i \equiv 2 \pmod 3$. Thus, $\mathrm{Cl}(\mathcal{O}_D)$ has $\frac{1}{2}(3^{t+2} - 1)$ index 3 subgroups, and there are that many cubic fields with discriminant of the form $-3dm^2$ for some $m \mid 3n$. By Möbius inversion, the number of cubic fields of discriminant $D = -27dn^2$ is $3 \cdot 2^t$, as claimed. □

Remark 22. One can also prove Proposition 21 using [6], but the proof is more involved since one must grapple with units in $\mathbb{Q}(\sqrt{-3D})$. Similarly, one can also prove Proposition 20 using class field theory, but again the proof is more involved since one must now deal with units in $\mathbb{Q}(\sqrt{D})$; see [10, Thm. 2.5]. In fact, the method we use to prove Proposition 20 can be used to give an alternative expression for the generating series Φ_d of [10], namely, as a finite sum of what are essentially Epstein zeta functions.

3.4. **Proof of Theorem 1.** We prove the stronger statement that a positive proportion of totally real (resp. complex) cubic fields are not monogenic, despite having no local obstruction to being so. Fix n as in the previous section and note that both Σ_n^+ and Σ_n^- have positive natural density and are large in the terminology of Section 3.1.

If $D \in \Sigma_n^\pm$ and K is a cubic field with $\mathrm{Disc}(K) = D$, then the class α_K defined in Section 3.2 lies in $\mathrm{Sel}_{\phi_D}(E^D)$ by Lemma 18. Since $-27D$ is not a perfect square, we have $E^D[\hat{\phi}_D](\mathbb{Q}) = 0$ and hence an injection $\mathrm{Sel}_{\phi_D}(E^D) \hookrightarrow \mathrm{Sel}_3(E^D)$. We may therefore view α_K as an element of $\mathrm{Sel}_3(E^D) \subset H^1(\mathbb{Q}, E^D[3])$. The image of α_K in $\text{Ш}(E^D)[3]$ vanishes if and only if $C_K(\mathbb{Q}) \neq \emptyset$. In particular, $C_K(\mathbb{Q}) \neq \emptyset$ if K is monogenic, since $f_K(x, y) = 1$ has a solution over $\mathbb{Z}$ and thus over $\mathbb{Q}$. Therefore, when K is a monogenic cubic field of discriminant D, the classes $\pm\alpha_K$ lie in the subgroup $E^D(\mathbb{Q})/3E^D(\mathbb{Q})$ of $\mathrm{Sel}_3(E^D)$.

Let U_n^+ (resp. U_n^-) be the subset of integers $D \in \Sigma_n^+$ (resp. Σ_n^-) such that the 3-torsion in the class group of $\mathbb{Q}(\sqrt{-3D})$ (resp. $\mathbb{Q}(\sqrt{D})$) is trivial. The lower natural density $\mu_{n,\pm}$ of $U_n^\pm$ within $\Sigma_n^\pm$ is at least 1/2 by [9, Thm. 4]. By Lemma 15 and Propositions 20 and 21, there are $(2 \mp 1)2^{t+1}$ distinct non-zero classes $\pm\alpha_K \in \mathrm{Sel}_3(E^D)$ for each $D \in U_n^\pm$. Write m_D for the number of monogenic cubic fields of discriminant D. Thus $0 \leq m_D \leq (2 \mp 1)2^{t+1}$ for $D \in U_n^\pm$, and $1 + 2m_D \leq 3^{\mathrm{rk}\, E^D(\mathbb{Q})}$.

Switching to 2-descent, this implies that

$$(1 + 2m_D)^{\log_3 2} \leq 2^{\mathrm{rk}\, E^D(\mathbb{Q})} \leq \#\mathrm{Sel}_2(E^D).$$

By the above inequality and Theorem 13,

$$\mu_{n,\pm}\cdot \mathrm{avg}_{D\in U_n^\pm}(1+2m_D)^{\log_3 2} + (1-\mu_{n,\pm})\cdot 1 \;\le\; \mathrm{avg}_{D\in\Sigma_n^\pm}\#\mathrm{Sel}_2(E^D) \;=\; 3.$$

Therefore,

$$\mathrm{avg}_{D\in U_n^\pm}(1+2m_D)^{\log_3 2} \le 1+2\mu_{n,\pm}^{-1} \le 5.$$

The function $f(x) := x^{\log_2 3}$ is strictly convex on $\mathbb{R}_{>0}$. Thus, given the two constraints (a) $m_D \in [0,(2\mp 1)2^t]$ for all $D\in U_n^\pm$, and (b) $\mathrm{avg}_{D\in U_n^\pm}(1+2m_D)^{\log_3 2}\le 5$, the average $\mathrm{avg}_{D\in U_n^\pm}(1+2m_D)$ is maximized when m_D takes all its values at the endpoints of $[0,(2\mp1)2^t]$. Once $t\ge 3$, this occurs when m_D attains its maximum value $(2\mp 1)2^t$ for a density of $4/((1+(2\mp 1)2^{t+1})^{\log_3 2}-1) = O(2^{-t\log_3 2})$ of $D\in U_n^\pm$, and $m_D=0$ otherwise. It follows that a (positive) lower density of at least $1-O(2^{-t\log_3 2})$ of cubic fields K with $\mathrm{Disc}(K)$ in $U_n^\pm$ are non-monogenic.

Since the relative lower density $\mu_{n,\pm}$ of $U_n^\pm$ in $\Sigma_n^\pm$ is at least $1/2$, we have produced $c\cdot X + o(X)$ (for an explicit constant $c>0$) cubic fields K with $\mathrm{Disc}(K)\in\Sigma_n^\pm$ and $|\mathrm{Disc}(K)|<X$ that are not monogenic and have no local obstruction to being monogenic. By the asymptotic count of all cubic fields due to Davenport and Heilbronn [11], this proves Theorem 1 for both positive and negative discriminants. □

Remark 23. For negative discriminants, we can even take $t=1$ in the argument above. In that case, we have $\dim_{\mathbb{F}_2}\mathrm{Sel}_2(E^D)\equiv\dim_{\mathbb{F}_3}\mathrm{Sel}_3(E^D)\equiv 1 \pmod 2$ for all $D\in\Sigma_n^-$ by the computation of the parity of the 3-Selmer rank in [7, Prop. 34, 49(b)] and the p-parity theorem [14]. Thus $\#\mathrm{Sel}_2(E^D)\ge 8$ when $m_D\ge 2$ and $\#\mathrm{Sel}_2(E^D)\ge 2$ always. Reasoning as in the proof of Theorem 1, it then follows that at least $\frac{5}{9}$ of cubic fields with discriminant in U_n^- are non-monogenic. If $n=2\cdot 3$, we find that there are at least

$$6\cdot\frac{5}{9}\cdot\mu_{n,-}\cdot\mu(\Sigma_n^-)\cdot X \ge 6\cdot\frac{5}{9}\cdot\frac{1}{2}\cdot\frac{1}{2^4}\cdot\frac{1}{3^6}\cdot\frac{27}{7^2}\cdot\prod_{p\nmid 42}(1-p^{-2})\cdot X$$

such fields, where $\mu(\Sigma_n^-)$ denotes the natural density of Σ_n^-. Dividing by the total number $\frac{1}{4}\cdot\zeta(3)^{-1}\cdot(.7599\ldots)\cdot X$ of unobstructed complex cubic fields (Theorem 4), we conclude that the proportion of unobstructed complex cubic fields that are non-monogenic is at least .000463.

For positive discriminants, we may similarly take $t=2$ and $n=2\cdot 3\cdot 5$ by parity considerations, and find that a proportion of at least .0000139 of unobstructed totally real cubic fields are not monogenic. Of course, we have not tried to optimize these lower bounds.

3.5. **Proofs of Theorems 5 and 6.** The proof of Theorem 1 immediately implies Theorem 5: we have produced a positive proportion of (both totally real and complex) cubic fields K such that the curves $C_K\colon z^3 = f_K(x,y)$ all have local solutions but not global solutions.

Choosing t large enough in the proof of Theorem 1 also immediately yields Theorem 6. More generally, if $\Sigma\subset\mathbb{Z}$ is a set of integers that are cubefree and satisfy a further finite set of congruence conditions, then, for a positive proportion of $k\in\Sigma$, we have $\dim_{\mathbb{F}_3}\text{Ш}(E_k)[3]\ge r$. Indeed, for any m, the set $T_m\cap\Sigma$ has positive density, and $\dim_{\mathbb{F}_3}\mathrm{Sel}_{\phi_k}(E_k)\ge m$ for *all* $k\in T_m$, by [7, Thm. 4(ii)]. On the other hand, by Corollary 14, the average rank of E_k is at most $3/2$. Thus, for $m\ge r+2$, it cannot be the case that, for 100% of $k\in T_m\cap\Sigma$, the image of $\mathrm{Sel}_{\phi_k}(E_k)$ in $\text{Ш}(E_k)[3]$ is less than r-dimensional. □

References

[1] S. Akhtari. Cubic Thue equations. *Publ. Math. Debrecen*, 75(3-4):459–483, 2009.

[2] S. Akhtari and M. Bhargava. A positive proportion of Thue equations fail the integral Hasse principle. *Amer. J. Math.*, 141(2):283–307, 2019.

[3] L. Alpöge. Points on Curves. *Princeton University Ph.D. thesis*, 2020.

[4] M. A. Bennett. On the representation of unity by binary cubic forms. *Trans. Amer. Math. Soc.*, 353(4):1507–1534, 2001.

[5] A. Bérczes. On the number of solutions of index form equations. *Publ. Math. Debrecen*, 56(3-4):251–262, 2000.

[6] M. Bhargava. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Ann. of Math. (2)*, 159(1):217–250, 2004.

[7] M. Bhargava, N. Elkies, and A. Shnidman. The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$. *Journal of the London Mathematical Society*, 101(1):299–327, 2020.

[8] M. Bhargava, A. Shankar, and J. Tsimerman. On the Davenport-Heilbronn theorems and second order terms. *Invent. Math.*, 193(2):439–499, 2013.

[9] M. Bhargava and I. Varma. The mean number of 3-torsion elements in the class groups and ideal groups of quadratic orders. *Proc. Lond. Math. Soc. (3)*, 112(2):235–266, 2016.

[10] H. Cohen and F. Thorne. Dirichlet series associated to cubic fields with given quadratic resolvent. *The Michigan Mathematical Journal*, 63(2):253–273, 2014.

[11] H. Davenport and H. Heilbronn. On the density of discriminants of cubic fields. II. *Proc. Roy. Soc. London Ser. A*, 322(1551):405–420, 1971.

[12] R. Dedekind. Uber den zusammenhang zwischen der theorie der ideale und der theorie der hoheren kongruenzen. *Abh.der Konig.Gesell.der Wiss.zu Gottingen*, 23:3–38, 1878.

[13] B. N. Delone and D. K. Faddeev. *The theory of irrationalities of the third degree*. Translations of Mathematical Monographs, Vol. 10. American Mathematical Society, Providence, R.I., 1964.

[14] T. Dokchitser and V. Dokchitser. Root numbers and parity of ranks of elliptic curves. *J. Reine Angew. Math.*, 658:39–64, 2011.

[15] J.-H. Evertse. On the representation of integers by binary cubic forms of positive discriminant. *Invent. Math.*, 73(1):117–138, 1983.

[16] J.-H. Evertse. A survey on monogenic orders. *Publ. Math. Debrecen*, 79(3-4):411–422, 2011.

[17] J.-H. Evertse and K. Győry. On unit equations and decomposable form equations. *J. Reine Angew. Math.*, 358:6–19, 1985.

[18] J.-H. Evertse and K. Győry. *Discriminant equations in Diophantine number theory*, volume 32 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2017.

[19] I. Gaál. *Diophantine equations and power integral bases*. Birkhäuser Boston, Inc., Boston, MA, 2002.

[20] W. T. Gan, B. Gross, and G. Savin. Fourier coefficients of modular forms on G_2. *Duke Math. J.*, 115(1):105–169, 2002.

[21] B. H. Gross and M. W. Lucianovic. On cubic rings and quaternion rings. *J. Number Theory*, 129(6):1468–1478, 2009.

[22] K. Győry. Sur les polynômes à coefficients entiers et de discriminant donné. III. *Publ. Math. Debrecen*, 23(1-2):141–165, 1976.

[23] D. R. Heath-Brown. A new form of the circle method, and its application to quadratic forms. *J. Reine Angew. Math.*, 481:149–206, 1996.

[24] F. Levi. Kubische Zahlkörper und binäre kubische Formenklassen. *Leipz. Ber.*, 66:26–37, 1914.

[25] R. Okazaki. Geometry of a cubic Thue equation. *Publ. Math. Debrecen*, 61(3-4):267–314, 2002.

[26] S. Ruth. A bound on the average rank of j-invariant 0 elliptic curves. *Princeton University Ph.D. thesis*, 2013.

[27] P. Satgé. Groupes de Selmer et corps cubiques. *J. Number Theory*, 23(3):294–317, 1986.