Monogenic Fields Arising from Trinomials

RYAN IBARRA, HENRY LEMBECK, MOHAMMAD OZASLAN, HANSON SMITH,
AND KATHERINE E. STANGE

Abstract. We call a polynomial *monogenic* if a root θ has the property that $\mathbb{Z}[\theta]$ is the full ring of integers of $\mathbb{Q}(\theta)$. Consider the two families of trinomials x^n+ax+b and $x^n+cx^{n-1}+d$. For any $n>2$, we show that these families are monogenic infinitely often and give some positive densities in terms of the coefficients. When $n=5$ or 6 and when a certain factor of the discriminant is square-free, we use the Montes algorithm to establish necessary and sufficient conditions for monogeneity, illuminating more general criteria given by Jakhar, Khanduja, and Sangwan using other methods. Along the way we remark on the equivalence of certain aspects of the Montes algorithm and Dedekind's index criterion.

1. Introduction

Let K be a number field, and denote its ring of integers by $\mathcal{O}_K$. If $\mathcal{O}_K=\mathbb{Z}[\theta]$ for some $\theta\in\mathcal{O}_K$, we say that $\mathcal{O}_K$ admits a *power integral basis* or that K is *monogenic*. The classification of monogenic number fields is often known as Hasse's problem.

We use the term *monogenic* to refer to any polynomial $f(x)\in\mathbb{Z}[x]$ for which a root θ has the property that $\mathbb{Z}[\theta]$ is the full ring of integers in $\mathbb{Q}(\theta)$. Our work seeks to give sufficient conditions for certain polynomials to be monogenic. By elementary considerations, any polynomial having a square-free discriminant is automatically monogenic. Both Kedlaya [16] and Boyd, Martin, and Thom [2] find families of polynomials with square-free discriminant. We study families with discriminants that are not square-free.

Our main tool in approaching Hasse's problem is the Montes algorithm (for an overview, see [20]; for in-depth treatments, see [5] or [11]). We limit ourselves to irreducible trinomials of the form x^n+ax+b or $x^n+cx^{n-1}+d$, with $n=5$ and 6. Note that the discriminants of these polynomials are not square-free in general (see Theorem 2.1).

When a certain factor of the discriminant is square-free, we are able to provide necessary and sufficient conditions for the monogeneity of these families (Theorems 3.1, 3.2, 3.3, and 3.4). Using the Montes algorithm to treat the case $n=4$ has already been studied in [20]. Furthermore, we demonstrate infinite families of polynomials (Theorems 3.5 and 3.6) whose roots yield power integral bases for their associated rings of integers infinitely often, namely x^n+bx+b and $x^n+cx^{n-1}+cd$. The reader wishing to see the full statements of our results should proceed to Section 3.

The literature regarding monogenic fields is extensive. See [6] for an extensive and very recent survey of much of the literature; this work has a very in-depth perspective on index form techniques. A general survey can also be found in [17] as well as [4]. Much of the literature focuses on a given degree or Galois group. Classically, monogeneity is known for cyclotomic fields and the maximal real subfields thereof. Gras [10] shows that, with the exception of maximal real subfields of cyclotomic fields, abelian extensions of prime degree greater than or equal to 5 are not monogenic. Gras [9] also shows that almost all abelian extensions with degree coprime to 6 are not monogenic. Gassert [8] gives necessary and sufficient conditions for the monogeneity of extensions of the form x^n+a; when n is prime see [22]. In [7], Gassert investigates the monogeneity of extensions given by shifted Chebyshev polynomials. Jones and Phillips [14] investigate trinomials of the form $x^n+a(m,n)x+b(m,n)$ with m an indeterminate. They find infinitely many distinct monogenic fields and classify

Date: August 27, 2022.
1991 *Mathematics Subject Classification.* 11R04.
Key words and phrases. monogenic, power integral basis, ring of integers, trinomial.

the Galois groups, which are either S_n or A_n. Although there is overlap with our family x^n+ax+b, the methods we employ are distinct.

As this work was in final edits for release, the authors were made aware of an overlapping recent parallel research line. Jakhar, Khanduja, and Sangwan ([12] and [13]) established necessary and sufficient conditions for any trinomial to be monogenic. Their criteria are more general than ours, but our methods are distinct. The conditions in our theorems are also more succinct and this allows us to analyze the density of our families; such an analysis is not present in [12] or [13]. Concurrently but independent from our work, Jones and White [15] prove infinitude and analyze the density of certain families of monogenic trinomials. In particular, they provide a more complete density theorem than our Theorem 3.5 for trinomials of the form $x^n + bx + b$, but do not address the family in Theorem 3.6.

The outline of the paper is as follows. In Section 2 we establish our setup, quote some previous results we will need, and give a very brief overview of part of the Montes algorithm, our main tool in proving these trinomials yield monogenic fields. We will formally state our results in Section 3. With Section 4 we use the Montes algorithm to prove the roots of the trinomials we are considering yield power integral bases. Section 5 establishes the infinitude of some of our families. Finally, Section 6 contains some computational data for comparison to the densities of Theorems 3.5 and 3.6.

Acknowledgments

We would like to thank the Mathematics Department at the University of Colorado Boulder for hosting and supporting the summer 2018 REU that allowed us to conduct this research. We would like to thank the anonymous referee for the timely review and thoughtful report. We also want to thank Sebastian Bozlee for the help with the code for Section 6 and Lhoussain El Fadil for catching and kindly pointing out an error in an earlier version of the paper.

2. Notation, Definitions, and Lemmas

In Table 1 we outline some standard notation that will be in use throughout the paper.

Table 1. Notation

K	a finite extension of $\mathbb{Q}$
$\mathcal{O}_K$	the ring of integers of K
Δ_K	the absolute discriminant of K
f, g, ϕ	a monic polynomial in x
Δ_f	the discriminant of the polynomial f
θ	a root of a polynomial
$\deg f$	the degree of the polynomial f
$a, b, c, \ldots$	integer coefficients of a polynomial
p	a prime number
v_p	the p-adic valuation, normalized so $v_p(p) = 1$
$\overline{f}$	f as viewed in $(\mathbb{Z}/m\mathbb{Z})[x]$, when m is clear

We will need the following well-known result relating field discriminants and polynomial discriminants. Let f be a monic irreducible polynomial of degree $n > 1$ and let θ be a root. Then

$$\Delta_f = \Delta_K [\mathcal{O}_K : \mathbb{Z}[\theta]]^2. \tag{1}$$

We can see that it is essential to know the discriminant. For this it is nice to have the following formula; see [21, Theorem 2].

Theorem 2.1. *Consider the trinomial* $f(x) = x^n + ax^k + b$. *Write* N *for* $\dfrac{n}{\gcd(n,k)}$ *and* K *for* $\dfrac{k}{\gcd(n,k)}$. *The discriminant of the trinomial is*

$$\Delta_f = (-1)^{\frac{n^2-n}{2}} b^{k-1} \left(n^N b^{N-K} - (-1)^N (n-k)^{N-K} k^K a^N\right)^{\gcd(n,k)}.$$

We now outline the notation necessary for the Montes algorithm. In its full generality the Montes algorithm is a powerful p-adic factorization algorithm, but we do not need the full extent of the algorithm for our application to monogeneity. We require a theorem, originally due to Ore [18], that appears in an early step of the algorithm.

We extend the standard p-adic valuation by defining the p-adic valuation of $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ to be

$$v_p(f(x)) = \min_{0 \le i \le n} (v_p(a_i)).$$

If $\phi(x), f(x) \in \mathbb{Z}[x]$ are such that $\deg \phi \le \deg f$, then we can write

$$f(x) = \sum_{i=0}^{k} a_i(x) \phi(x)^i,$$

for some k, where each $a_i(x) \in \mathbb{Z}[x]$ has degree less than $\deg \phi$. We call the above expression the *ϕ-adic development* of $f(x)$. We associate to the ϕ-adic development of f a Newton polygon by taking the lower convex hull[1] of the integer lattice points $(i, v_p(a_i(x)))$. We call the sides of the Newton polygon with negative slope the *principal ϕ-polygon*. The number of integer lattice points (m, n), with $m, n > 0$, on or under the principal ϕ-polygon is called the *ϕ-index of f* and denoted $\operatorname{ind}_\phi(f)$. Associated to each side of the principal ϕ-polygon is a polynomial called the *residual polynomial*. To avoid technicality, we will not define the residual polynomial in general. For our purposes it suffices to note that residual polynomials attached to sides whose only integer lattice points are the initial vertex and terminal vertex are linear polynomials. Again, the interested reader is encouraged to consult [20] for a brief account of the Montes algorithm or [5] and [11] for in-depth descriptions and proofs.

Now we state a theorem of Ore [18] which will yield our main tool in proving monogeneity.

Theorem 2.2 (Ore's theorem of the index)**.** *Choose monic polynomials* $\phi_1, \ldots, \phi_k \in \mathbb{Z}[x]$ *whose reductions modulo* p *are exactly the distinct irreducible factors of* $\overline{f(x)}$. *Let* θ *be a root of* $f(x)$. *Then,*

$$v_p([\mathcal{O}_K : \mathbb{Z}[\theta]]) \ge \operatorname{ind}_{\phi_1}(f) + \cdots + \operatorname{ind}_{\phi_k}(f).$$

Further, equality holds if, for every ϕ_i, *each side of the principal* ϕ_i*-polygon has a separable residual polynomial.*

For our applications we will employ a clean equivalence derived from Theorem 2.2.

Corollary 2.3. *The prime* p *does not divide* $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ *if and only if* $\operatorname{ind}_{\phi_i}(f) = 0$ *for all* i. *In this case each principal* ϕ_i*-polygon is one-sided.*

[1] Loosely speaking, visualize the points $(i, v_p(a_i(x)))$ as nails in the xy-plane and pull a taut string upward from the negative y-axis to the positive y-axis. We consider the open polygon formed by the string intersecting the nails.

Proof. If $\text{ind}_{\phi_i}(f) > 0$, then Theorem 2.2 shows $v_p([\mathcal{O}_K : \mathbb{Z}[\theta]]) > 0$. Conversely, if each $\text{ind}_{\phi_i}(f) = 0$, then the associated residual polynomials will all be linear and hence separable. This is because if $\text{ind}_{\phi_i}(f) = 0$, then the only integer lattice points on each side of the principal ϕ_i-polygon are the initial and terminal vertices. Thus $v_p([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0$ in this case.

Notice that, since $f(x) \in \mathbb{Z}[x]$, if the principal ϕ_i-polygon has more than one side, then there is necessarily a vertex with positive integer coordinates. This vertex will contribute to $\text{ind}_{\phi_i}(f)$ and ensure that p divides $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. □

Before continuing we would like to compare Corollary 2.3 to another criterion used for studying monogeneity. Consider the following theorem of Dedekind [3].

Theorem 2.4 (Dedekind's index criterion)**.** *Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$ and let θ be a root of f. If p is a rational prime, we have*

$$f(x) \equiv \prod_{i=1}^{r} \phi_i(x)^{e_i} \bmod p,$$

where the $\phi_i(x)$ are monic lifts of the irreducible factors of $\overline{f(x)}$ to $\mathbb{Z}[x]$. Define

$$d(x) := \frac{f(x) - \prod_{i=1}^{r} \phi_i(x)^{e_i}}{p}.$$

Then p divides $\left[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]\right]$ if and only if $\gcd\left(\overline{\phi_i(x)}^{e_i - 1}, \overline{d(x)}\right) \neq 1$ for some i, where we are taking the greatest common divisor in $\mathbb{F}_p[x]$.

Remark 2.5. **(Equivalence of Polygons and Dedekind for Monogeneity)** Corollary 2.3 is equivalent to Dedekind's index criterion. To see this, we consider the ϕ-adic development,

$$f(x) = \phi(x)^k + a_{k-1}\phi(x)^{k-1} + \cdots + a_2\phi(x)^2 + a_1\phi(x) + a_0.$$

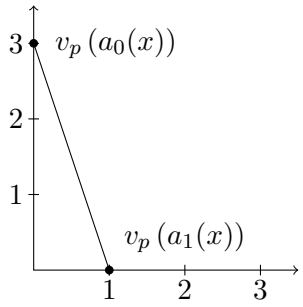
For ease of exposition, let $(*)$ denote the condition that either $v_p(a_0) = 1$ or $v_p(a_1) = 0$. Figure 1 shows examples of the principal $\phi(x)$-polygons corresponding to these two cases. Since $\phi(x)$ divides $f(x)$ in $\mathbb{F}_p[x]$, we have $v_p(a_0) > 0$. We notice that $\text{ind}_\phi(f) = 0$ if and only if condition $(*)$ holds. This is because the principal ϕ-polygon bounds or contains the point $(1, 1)$ if and only if $\text{ind}_\phi(f) > 0$. From the ϕ-adic development we can translate condition $(*)$: If $v_p(a_0) = 1$, then no root of $\phi(x)$ is a root of $f(x)$ modulo p^2. If $v_p(a_1) = 0$, then the exponent of $\phi(x)$ in the factorization of $f(x)$ modulo p is one. Combining these observations with some algebra, we obtain Dedekind's index criterion.

We have seen that the Montes algorithm and Dedekind's index criterion are both equally able to answer the question of whether or not a given polynomial in $\mathbb{Z}[x]$ is monogenic. Moreover, Newton polygons give us another way of picturing Dedekind's index criterion. It bears noting again that a full application of the Montes algorithm computes the complete factorization of any prime p in $\mathbb{Q}(\theta)$ and a basis that is p-integral, so it is a much more general tool than Dedekind's index criterion.

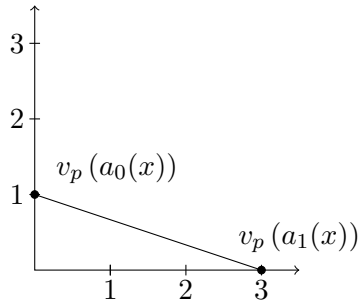
Lastly, in our paper 'density' refers to natural density. Let $A \subseteq \mathbb{N}$ and $a(x) := \#\{a \in A \mid a \leq x\}$. If

$$\lim_{x \to \infty} \frac{a(x)}{x} = \alpha,$$

we say that A has *natural density* α in $\mathbb{N}$.



(A) The exponent of $\phi(x)$ in $f(x)$ is one



(B) $\phi(x)$ is not a root modulo p^2

FIGURE 1. Examples of principal $\phi(x)$-polygons that could correspond to monogenic polynomials

3. Statements of Results

Consider the two families $f(x) = x^n + ax + b$ and $g(x) = x^n + cx^{n-1} + d$. The discriminants are

$$\Delta_f = (-1)^{\frac{n^2-n}{2}} \left(n^n b^{n-1} + (1-n)^{n-1} a^n\right)$$

and

$$\Delta_g = (-1)^{\frac{n^2-n}{2}} d^{n-2} \left(n^n d + (1-n)^{n-1} c^n\right).$$

We investigate the $n = 5$ and $n = 6$ cases in depth.

Theorem 3.1. *Let $f(x) = x^5 + ax + b \in \mathbb{Z}[x]$ be irreducible and let θ be a root. Suppose $\frac{2^8 a^5 + 5^5 b^4}{\gcd(2^8 a^5, 5^5 b^4)}$ is square-free. Then θ generates a power integral basis for the ring of integers of $\mathbb{Q}(\theta)$ if and only if for each prime $p \mid \gcd(2a, 5b)$ one of the following conditions holds:*

(1) $p \mid a$ and $p \mid b$, but $p^2 \nmid b$.
(2) $p = 2$, $2 \nmid a$, and $a + b \equiv 1 \pmod 4$.
(3) $p = 5$, $5 \nmid b$, and $b \not\equiv 1 + a, 7 + 2a, 18 + 3a, 24 + 4a \pmod{25}$.

Theorem 3.2. *Let $f(x) = x^6 + ax + b \in \mathbb{Z}[x]$ be irreducible and let θ be a root. Suppose $\frac{6^6 b^5 - 5^5 a^6}{\gcd(6^6 b^5, 5^5 a^6)}$ is square-free. Then θ generates a power integral basis for the ring of integers of $\mathbb{Q}(\theta)$ if and only if for each prime $p \mid \gcd(6b, 5a)$ one of the following conditions holds:*

(1) $p \mid a$ and $p \mid b$, but $p^2 \nmid b$.
(2) $p = 2$, $2 \nmid b$, and $a + b \equiv 1 \pmod 4$.
*(3) $p = 3$, $3 \nmid b$, and the image of (a, b) in $(\mathbb{Z}/9\mathbb{Z})^2$ is **not** in the set*

$$\{(0,1), (0,8), (3,2), (3,5), (6,2), (6,5)\}.$$

(4) $p = 5$, $5 \nmid a$, and $a \not\equiv 1 - 4b, 7 + 3b, 18 + 3b, 24 + 4b \pmod{25}$.

Theorem 3.3. *Let $g(x) = x^5 + cx^4 + d \in \mathbb{Z}[x]$ be irreducible and θ a root. Suppose $\frac{5^5 d + 2^8 c^5}{\gcd(5^5 d, 2^8 c^5)}$ is square-free. Then θ generates a power integral basis for the ring of integers of $\mathbb{Q}(\theta)$ if and only if d is square-free and if $5 \mid c$ but $5 \nmid d$, then $c + d \not\equiv 1, 7, 18, 24 \pmod{25}$.*

Theorem 3.4. *Let $g(x) = x^6 + cx^5 + d \in \mathbb{Z}[x]$ be irreducible and θ a root. Suppose $\frac{6^6 d - 5^5 c^6}{\gcd(6^6 d, 5^5 c^6)}$ is square-free. Then θ generates a power integral basis for the ring of integers of $\mathbb{Q}(\theta)$ if and only if for every $p \mid \gcd(6d, 5c)$ one of the following conditions hold:*

(1) d is square-free.
(2) If $2 \mid c$ and $2 \nmid d$, then $c + d \equiv 1 \pmod 4$.

(3) If $3 \mid c$ and $3 \nmid d$, then the image of (c,d) in $(\mathbb{Z}/9\mathbb{Z})^2$ is in the set

$$\{(0,2),(0,4),(0,5),(0,7),(3,1),(3,4),(3,7),(3,8),(6,1),(6,4),(6,7),(6,8)\}.$$

With sufficient conditions in hand, one can ask about the density of coefficients satisfying these conditions. Naturally, we would like to prove the infinitude of some of the families of monogenic fields.

Theorem 3.5. *Fix $n > 2$. Let θ be a root of $f(x) = x^n + bx + b \in \mathbb{Z}[x]$. Then there are infinitely many b such that f is irreducible and θ generates a power integral basis for the ring of integers of $\mathbb{Q}(\theta)$. In addition, the density of such b is at least*

$$\frac{6}{\pi^2} - \left(1 - \frac{6}{\pi^2} \prod_{p \mid (n-1)} \left(1 - \frac{1}{p^2}\right)^{-1}\right) > 21.58\%.$$

Theorem 3.6. *Fix $n > 2$. Let c be a nonzero integer such that $c \neq \pm 1$ and c is square-free. Suppose $g(x) = x^n + cx^{n-1} + cd \in \mathbb{Z}[x]$ is irreducible and let θ be a root. Consider the quantity*

$$B = \frac{6}{\pi^2} \prod_{p \mid c} \frac{p}{p+1} - \left(1 - \frac{6}{\pi^2} \prod_{p \mid n} \frac{p^2}{p^2-1}\right).$$

Then B gives a lower bound on the density of d such that θ generates a power integral basis for the ring of integers of $\mathbb{Q}(\theta)$. In particular, if c has exactly one prime factor or has exactly two prime factors and is coprime to 6, then $B > 0$ and there are infinitely many d yielding such monogenic fields.

Remark 3.7. The densities above are merely a byproduct of our proof methods, and appear weak compared to actual densities observed by computation. See Section 6 for these data.

4. Proofs

To warm up to Newton polygons, we will prove a well-known result, e.g. [17, Lemma 2.17], on the p-integrality of polynomials that are Eisenstein at p. Proving this here will also simplify the proofs below.

Lemma 4.1. *Suppose $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is Eisenstein at p (each a_i is divisible by p with p dividing a_0 exactly once), and let θ be a root of $f(x)$. Then p does not divide the index $[\mathcal{O}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]$.*

Proof. We have $f(x) \equiv x^n \bmod p$, so we consider only the x-adic development of $f(x)$. The x-adic development of $f(x)$ is just $f(x)$, so our principal x-polygon is one-sided with slope $-\frac{1}{n}$; see Figure 2. No positive integer lattice points lie on or below this polygon, thus the x-index is 0. Theorem 2.2 yields the result.

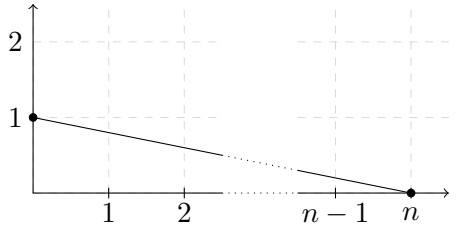


Figure 2. The principal x-polygon

□

We will be particularly deliberate with our proof of Theorem 3.1. The proofs of the other theorems are very similar, so we will only highlight aspects that are distinct from the proof of Theorem 3.1.

Proof of Theorem 3.1. Recall our set-up: $f(x) = x^5 + ax + b \in \mathbb{Z}[x]$ is irreducible, θ is a root, $K = \mathbb{Q}(\theta)$, and $\Delta_f = 5^5b^4 + 4^4a^5 = 3125b^4 + 256a^5$. By equation (1) and the hypothesis that $\frac{5^5b^4+2^8a^5}{\gcd(5^5b^4,2^8a^5)}$ is square-free, the only prime factors p of $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ are divisors of $\gcd(5b, 2a)$. Thus we need only consider the cases given in the theorem statement.

Case 1. Suppose p divides a and b. Employing the ideas at work in Lemma 4.1, we see $(1, 1)$ is on or under the principal x-polygon if and only if $p^2 \mid b$. Corollary 2.3 shows that in this case p divides the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ if and only if $p^2 \mid b$.

Case 2. Suppose that $p = 2$ and $2 \nmid a$. Since $2 \mid 5b$ and $\gcd(2, 5) = 1$, we see $2 \mid b$. As a result,

$$f(x) = x^5 + ax + b \equiv x^5 + ax \equiv x(x^4 + a) \pmod 2.$$

However, $2 \nmid a$ implies that $a \equiv 1 \pmod 2$. Hence

$$f(x) \equiv x(x^4 + 1) \equiv x(x^4 + 1^4) \equiv x(x + 1)^4 \pmod 2.$$

Since the exponent of x is one, it does not contribute to the index. Thus we only need to look at the $(x + 1)$-adic development of f, which is

$$f(x) = (x + 1)^5 - 5(x + 1)^4 + 10(x + 1)^3 - 10(x + 1)^2 + (a + 5)(x + 1) + b - a - 1.$$

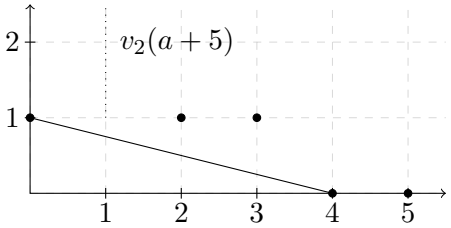
Note $a + 5 \equiv 1 + 5 \equiv 0 \pmod 2$, so $v_2(a + 5) \geq 1$. Thus $v_2(b - a - 1)$ is greater than 1 if and only if the point $(1, 1)$ is on or below the principal $(x + 1)$-polygon. Thus, applying Corollary 2.3, $2 \mid [\mathcal{O}_K : \mathbb{Z}[\theta]] \Leftrightarrow v_2(b - a - 1) > 1$. Hence we wish to ensure that $v_2(b - a - 1) = 1$. Since $a \equiv 1 \pmod 2$ and $b \equiv 0 \pmod 2$, we examine four possibilities for the image of a, b in $\mathbb{Z}/4\mathbb{Z}$. These can seen in Table 2.

a	b	$b - a - 1$
3	2	2
3	0	0
1	2	0
1	0	2

TABLE 2. a, b, and $b - a - 1$ modulo 4

To visualize Case 2, notice that when (a, b) is congruent to (3,2) or (1,0) modulo 4, i.e., $a+b \equiv 1 \pmod 4$, we have the principal $(x + 1)$-polygon in Figure 3. We can see that the integer lattice

FIGURE 3. The principal $(x + 1)$-polygon



point corresponding to $(1, v_2(a + 5))$ is on the dotted line above the principal $(x + 1)$-polygon.

Case 3. Now, suppose that $p = 5$ and $5 \nmid b$. Since $5 \mid 2a$, we see that $5 \mid a$. Thus

$$f(x) = x^5 + ax + b \equiv x^5 + b \equiv x^5 + b^5 \equiv (x+b)^5 \pmod 5.$$

The $(x+b)$-adic development is

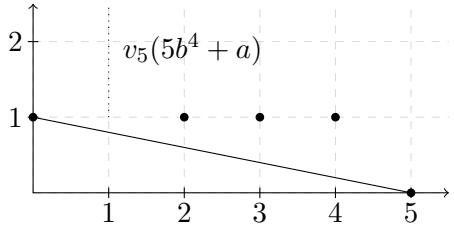
$$f(x) = (x+b)^5 - 5b(x+b)^4 + 10b^2(x+b)^3 - 10b^3(x+b)^2 + (5b^4+a)(x+b) - b^5 - ba + b.$$

We compute $v_5(-b^5 - ba + b) \geq 1$ and $v_5(5b^4 + a) \geq 1$. Thus the lattice point $(1, 1)$ will be on or under the principal $(x+b)$-polygon if and only if if $v_5(-b^5 - ba + b) > 1$. Hence, again with Corollary 2.3, 5 divides $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ if and only if 25 divides $-b^5 - ba + b$.

Note that $b_0 = 1, 2, 3, 4$ are solutions to $-x^5 - ax + x \equiv 0 \pmod 5$. We use Hensel's lemma to obtain solutions modulo 25, and we find that the solutions (a, b) are of the form $(a, 1+a), (a, 7+2a), (a, 18+3a)$, and $(a, 24+4a)$. Therefore $25 \mid \left(-b^5 - ba + b\right)$ if and only if (a, b) is one of these pairs. Corollary 2.3 finishes the argument.

To see what is happening here, we note that if (a, b) is not of one of the forms above, then we obtain the principal $(x+b)$-polygon in Figure 4. The integer lattice point $(1, v_5(5b^4+a))$ lies above

FIGURE 4. The principal $(x+b)$-polygon



the principal $(x+b)$-polygon on the dotted line.

In conclusion, for all primes p that could possibly divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, we have established necessary and sufficient conditions for $v_p([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0$. □

Proof of Theorem 3.2. Recall our set-up: $f(x) = x^6 + ax + b \in \mathbb{Z}[x]$ is irreducible, θ is a root, $K = \mathbb{Q}(\theta)$, and $\Delta_f = 6^6b^5 - 5^5a^6 = 46656b^5 - 3125a^6$. We assume that $\frac{6^6b^5 - 5^5a^6}{\gcd(6^6b^5, 5^5a^6)}$ is square-free and consider primes p dividing $\gcd(6b, 5a)$. Our approach and Case 1 are exactly analogous to the proof of Theorem 3.1.

Case 2. Suppose $p = 2$ and $2 \nmid b$. We see $2 \mid a$ and as a result

$$f(x) = x^6 + ax + b = x^6 + b \equiv (x^3 + b)^2 \pmod 2.$$

Furthermore $b \equiv 1 \pmod 2$, so

$$f(x) \equiv (x^3+1)^2 \equiv \left[(x+1)(x^2+x+1)\right]^2 \pmod 2.$$

We have two irreducible factors to consider. For the irreducible factor $(x+1)$, the $(x+1)$-adic development of $f(x)$ is

$$(x+1)^6 - 6(x+1)^5 + 15(x+1)^4 - 20(x+1)^3 + 15(x+1)^2 + (a-6)(x+1) - a + b + 1.$$

We observe that $a_1(x) = a - 6 \equiv 0 \pmod 2$, so $v_2(a_1(x)) \geq 1$. We want to ensure $4 \nmid a_0(x) = -a + b + 1$. Thus (a, b) must be equivalent to $(2, 3)$ or $(0, 1)$ modulo 4.

We turn our attention to the other irreducible factor, x^2+x+1. The (x^2+x+1)-adic development of f is

$$(x^2+x+1)^3 - 3x(x^2+x+1)^2 + (2x-2)(x^2+x+1) + ax + b + 1.$$

It is clear that $a_1(x) = 2x - 2 \equiv 0 \pmod 2$, so $v_2(a_1(x)) \geq 1$. We need to ensure that $4 \nmid a_0(x) = ax + b + 1$. Thus we need either $v_2(a) = 1$ or $b \equiv 1 \pmod 4$.

Since the conditions coming from the irreducible factor $(x+1)$ are more restrictive, we conclude that $2 \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$ if and only if (a, b) is equivalent to either $(2, 3)$ or $(0, 1)$ modulo 4.

Case 3. Suppose $p = 3$ and $3 \nmid b$. Since $3 \mid a$, we have

$$f(x) = x^6 + ax + b \equiv x^6 + b \equiv (x^2 + b)^3 \pmod 3.$$

There are two subcases.

Subcase 3.1. Suppose $b \equiv 1$ modulo 3. Then, $x^2 + b \equiv x^2 + 1$, which is irreducible. Hence, $f(x) \equiv (x^2 + 1)^3 \pmod 3$. The $(x^2 + 1)$-adic development of f is

$$(x^2 + 1)^3 - 3(x^2 + 1)^2 + 3(x^2 + 1) + ax + b - 1.$$

Clearly, $v_3(a_1(x)) = 1$. In this subcase, $v_3([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0 \Leftrightarrow v_3(ax + b - 1) = 1$. Translating, either $a \not\equiv 0 \pmod 9$ or $b \not\equiv 1 \pmod 9$.

Subcase 3.2. Suppose $b \equiv 2$ modulo 3. Then, $x^2 + b \equiv x^2 + 2 \equiv (x + 1)(x + 2) \pmod 3$, and

$$f(x) \equiv ((x + 1)(x + 2))^3 \pmod 3.$$

First, we examine the factor $(x + 1)$. The $(x + 1)$-adic development of f is

$$\begin{aligned}(x + 1)^6 - 6(x + 1)^5 + 15(x + 1)^4 - 20(x + 1)^3 \\ + 15(x + 1)^2 + (a - 6)(x + 1) - a + b + 1.\end{aligned}$$

We observe that $v_3(a - 6) \geq 1$. To avoid $-a + b + 1 \equiv 0 \pmod 9$ is to require that $a \not\equiv b + 1 \pmod 9$.

Lastly, we look at the factor $(x + 2)$. The $(x + 2)$-adic development of f is

$$\begin{aligned}(x + 2)^6 - 12(x + 2)^5 + 60(x + 2)^4 - 160(x + 2)^3 \\ + 240(x + 2)^2 + (a - 192)(x + 2) - 2a + b + 64.\end{aligned}$$

Since $v_3(a-192) \geq 1$, we want $-2a+b+64 \not\equiv 0 \pmod 9$. This happens exactly when $b \not\equiv 2a-64 \equiv 2a - 1 \pmod 9$.

Therefore, in this subcase, we see $v_3([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0$ if and only if the reduction of (a, b) modulo 9 is not a member of the set

$$\{(0, 1), (0, 8), (3, 2), (3, 5), (6, 2), (6, 5)\}.$$

Case 4. Finally, assume that $p = 5$ and $5 \nmid a$. Since $5 \mid b$, we have

$$f(x) \equiv x^6 + ax \equiv x(x + a)^5.$$

The only irreducible factor that concerns us is $x + a$. The $(x + a)$-adic development of $f(x)$ is

$$\begin{aligned}(x + a)^6 - 6a(x + a)^5 + 15a^2(x + a)^4 - 20a^3(x + a)^3 \\ + 15a^4(x + a)^2 + (-6a^5 + a)(x + a) + a^6 - a^2 + b.\end{aligned}$$

Proceeding in the same manner as in the proof of Theorem 3.1, $v_5([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0$ if and only if a is not of the form $1 - 4b, 7 + 3b, 18 + 3b,$ or $24 + 4b \pmod{25}$.

For all primes p which could possible divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, we have shown the necessity and sufficiency of our conditions. □

Proof of Theorem 3.3. Recall that we are considering the irreducible polynomial $g(x) = x^5 + cx^4 + d \in \mathbb{Z}[x]$. One computes $\Delta_g = d^3\left(5^5 d + 4^4 c^5\right) = d^3\left(3125d + 256c^5\right)$. We assume that $\dfrac{5^5 d + 2^8 c^5}{\gcd\left(5^5 d, 2^8 c^5\right)}$ is square-free. The possible prime divisors of the index are primes dividing d or $\gcd(5d, 2c)$. The only prime we may have to consider that is not necessarily a divisor of d is 5.

For primes $p \mid d$ we have

$$g(x) \equiv x^5 + cx^4 \equiv x^4(x+c) \pmod{p}.$$

As the exponent is one, the factor $x+c$ contributes nothing to the index. The x-adic development is again $g(x)$. By the standard argument, $v_p([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0$ if and only if d is square-free.

$p = 5$: Suppose now that $5 \mid c$ and $5 \nmid d$. We have

$$f(x) = x^5 + cx^4 + d \equiv x^5 + d \equiv x^5 + d^5 \equiv (x+d)^5 \pmod{5}.$$

The $(x+d)$-adic development of $f(x)$ is given by

$$\begin{aligned}(x+d)^5 + (c-5d)(x+d)^4 + (10d^2 - 4cd)(x+d)^3 \\ + (6cd^2 - 10d^3)(x+d)^2 + (5d^4 - 4cd^3)(x+d) + cd^4 + d - d^5.\end{aligned}$$

As we expect, $5 \mid [\mathcal{O}_K : \mathbb{Z}[\theta]] \Leftrightarrow 25 \mid \left(cd^4 + d - d^5\right)$. One computes that 25 divides $cd^4 + d - d^5$ if and only if $c + d \equiv 1, 7, 18$, or $24 \pmod{25}$. □

Proof of Theorem 3.4. We remind ourselves that we are considering $g(x) = x^6 + cx^5 + d$. We have $\Delta_g = -d^4(6^6 d - 5^5 c^6)$ and by hypothesis $\frac{6^6 d - 5^5 c^6}{\gcd(6^6 d, 5^5 c^6)}$ is square-free. We consider primes p dividing d or $\gcd(6d, 5c)$. The only primes we may have to consider that are not divisors of d are 2 and 3.

Our routine argument shows that prime divisors of d divide the index if and only if their square divides d.

$p = 2$: Suppose $2 \mid c$ and $2 \nmid d$. Reducing yields

$$g(x) = x^6 + cx^5 + d \equiv (x+1)^2(x^2+x+1)^2 \pmod{2}.$$

The $(x+1)$-adic development is

$$\begin{aligned}g(x) = (x+1)^6 + (-6+c)(x+1)^5 + (15-5c)(x+1)^4 + (-20+10c)(x+1)^3 \\ + (15-10c)(x+1)^2 + (-6+5c)(x+1) - c + d + 1.\end{aligned}$$

This factor not contributing to the index is equivalent to (c, d) reducing to either $(0,1)$ or $(2,3)$ in $(\mathbb{Z}/4\mathbb{Z})^2$.

Continuing, the (x^2+x+1)-adic development is

$$\begin{aligned}g(x) = (x^2+x+1)^3 + (-3x + cx - 2c)(x^2+x+1)^2 \\ + (2x + cx + 3c - 2)(x^2+x+1) - cx - c + d + 1.\end{aligned}$$

We are concerned with $v_2(-cx - c + d + 1) = \min(v_2(-c), v_2(-c+d+1))$. For this factor not to contribute to the index it is necessary and sufficient that $c \equiv 2 \pmod 4$ or $d \equiv 1 \pmod 4$. The $(x+1)$-adic development is more restrictive, so $v_2([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0$ if and only if (c, d) reduces to either $(0,1)$ or $(2,3)$ in $(\mathbb{Z}/4\mathbb{Z})^2$.

$p = 3$: Suppose $3 \mid c$ and $3 \nmid d$. If $d \equiv 1 \pmod 3$, then $g(x) \equiv (x^2+1)^3 \pmod 3$. The (x^2+1)-adic development is

$$g(x) = (x^2+1)^3 + (cx - 3)(x^2+1)^2 + (3 - 2cx)(x^2+1) + cx + d - 1.$$

Thus $v_3([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0$ if and only if either $c \equiv 3, 6 \pmod 9$ or $d \equiv 4, 7 \pmod 9$.

If $d \equiv 2$ modulo 3, then $g(x) \equiv (x+1)^3(x-1)^3$ modulo 3. The $(x+1)$-adic development is above. The $(x-1)$-adic development is

$$\begin{aligned}g(x) = (x-1)^6 + (6+c)(x-1)^5 + (15+5c)(x-1)^4 + (20+10c)(x-1)^3 \\ (15+10c)(x-1)^2 + (6+5c)(x-1) + c + d + 1.\end{aligned}$$

Combining this with the conditions coming from the $(x+1)$-adic development it is necessary and sufficient that $v_3(d-c+1) = v_3(d+c+1) = 1$. Therefore $v_3([\mathcal{O}_K : \mathbb{Z}[\theta]]) = 0$ if and only if the image of (c,d) in $(\mathbb{Z}/9\mathbb{Z})^2$ is in $\{(0,2),(0,5),(3,8),(6,8)\}$. □

5. Infinitude of the Families

In this section we will let $n \geq 2$, but restrict the coefficients of our families and find that they are monogenic infinitely often. To do this, we will actually prove that the coefficients yielding monogenic fields have positive density in $\mathbb{Z}$. This requires considering the density of square-free values of parts of the discriminant.

In general, showing a polynomial takes on infinitely many square-free values can be difficult: for example, it is not known whether there is a single irreducible quartic polynomial that is square-free infinitely often [1]. In our case, we only require some results on linear polynomials. The first is a result from Prachar [19] about the density of square-free integers congruent to m modulo k. Let $S(x;m,k)$ denote the number of square-free integers not exceeding x that are congruent to m modulo k.

Theorem 5.1. *If* $\gcd(m,k) = 1$ *and* $k \leq x^{\frac{2}{3}-\epsilon}$, *then*

$$S(x;m,k) \sim \frac{6x}{\pi^2 k} \prod_{p|k} \left(1 - \frac{1}{p^2}\right)^{-1} \qquad (x \to \infty).$$

We will also need to know the number of integers not exceeding x that are square-free and coprime to k. Denote this quantity by $T(x;k)$. The following is a straightforward corollary of Theorem 5.1 if one notes there are $\phi(k) = k\prod_{p|k} \frac{p-1}{p}$ distinct congruence classes modulo k that are relatively prime to k.

Corollary 5.2. *With the notation as above*

$$T(x;k) \sim \frac{6x}{\pi^2} \prod_{p|k} \frac{p}{p+1} \qquad (x \to \infty).$$

Proof of Theorem 3.5. We are considering the polynomial $f(x) = x^n + bx + b$. First note that if b is square-free, then f is irreducible by Eisenstein's Criterion. Recall that the density of square-free b is $\frac{6}{\pi^2}$. We have computed $\Delta_f = \pm b^{n-1}(n^n + (1-n)^{n-1}b)$, and Lemma 4.1 tells us that if $n^n + (1-n)^{n-1}b$ is square-free in addition to b, the number field generated by $f(x)$ is monogenic. Notice that choices of $b \in \mathbb{Z}$ are in bijection with integers congruent to n^n modulo $(n-1)^{n-1}$. We take $S(x; n^n, (n-1)^{n-1})$. By Theorem 5.1, the density of b such that $n^n + (1-n)^{n-1}b$ is square-free is

$$\frac{6}{\pi^2} \prod_{p|(n-1)} \left(1 - \frac{1}{p^2}\right)^{-1} > \frac{6}{\pi^2}.$$

Note that we do not have a factor of $(n-1)^{n-1}$ in the denominator of $\frac{6}{\pi^2}$ because we are considering the density of square-free integers congruent to n^n among all integers congruent to n^n. For the purposes of a lower bound on the density of

$$\left\{b \in \mathbb{Z} : b \text{ and } n^n + (1-n)^{n-1}b \text{ are square-free}\right\},$$

the worst case scenario is that every value of $n^n + (1-n)^{n-1}b$ that is not square-free occurs when b is square-free. Thus the density of square-free b with $n^n + (1-n)^{n-1}b$ also square-free is at least

$$\frac{6}{\pi^2} - \left(1 - \frac{6}{\pi^2} \prod_{p|(n-1)} \left(1 - \frac{1}{p^2}\right)^{-1}\right) > \frac{6}{\pi^2} - \left(1 - \frac{6}{\pi^2}\right) \approx 21.58\%.$$

□

Proof of Theorem 3.6. Consider $g(x) = x^n + cx^{n-1} + cd$ with n and c fixed such that c is square-free, $c \neq \pm 1$, and $\gcd(c, n) = 1$. Since $c \neq \pm 1$, Eisenstein's criterion shows g is irreducible when $\gcd(c, d) = 1$.

We wish to analyze the density of d for which g is monogenic. First, for g to be monogenic it is necessary that $\gcd(c, d) = 1$. We have computed $\Delta_g = \pm(cd)^{n-2}\left(n^n(cd) + (1-n)^{n-1}c^n\right)$. If $\gcd(c, d) = 1$, the product cd is square-free if d is square-free. If d and $cdn^n + (1-n)^{n-1}c^n$ are square-free, then Lemma 4.1 shows that g is monogenic. The factor of c is extraneous, so we will investigate when $dn^n + (1-n)^{n-1}c^{n-1}$ is square-free.

From Corollary 5.2, the proportion of square-free d that are coprime to c is given by

$$\frac{6}{\pi^2}\prod_{p|c}\frac{p}{p+1}.$$

In addition, Theorem 5.1 tells us the density of square-free integers among all integers congruent to $(1-n)^{n-1}c^{n-1}$ modulo n^n is

$$\frac{6}{\pi^2}\prod_{p|n}\frac{p^2}{p^2-1}.$$

Thus (much as in the last proof) a lower bound on the density of square-free d coprime to c such that $(1-n)^{n-1}c^{n-1} + dn^n$ is square-free is,

$$B = \frac{6}{\pi^2}\prod_{p|c}\frac{p}{p+1} - \left(1 - \frac{6}{\pi^2}\prod_{p|n}\frac{p^2}{p^2-1}\right) = \frac{6}{\pi^2}\left(\prod_{p|c}\frac{p}{p+1} + \prod_{p|n}\frac{p^2}{p^2-1}\right) - 1.$$

This is non-trivial if this value is positive.

If c has exactly one prime factor, then

$$\frac{6}{\pi^2}\prod_{p|c}\frac{p}{p+1} \geq \frac{6\cdot 2}{\pi^2\cdot 3}.$$

Hence

$$B > \frac{6\cdot 2}{\pi^2\cdot 3} - \left(1 - \frac{6}{\pi^2}\right) \approx 0.013.$$

On the other hand, if c has at most two prime factors and is coprime to 6, then we have

$$\frac{6}{\pi^2}\prod_{p|c}\frac{p}{p+1} \geq \frac{6\cdot 5\cdot 7}{\pi^2\cdot 6\cdot 8}.$$

Hence

$$B > \frac{6\cdot 5\cdot 7}{\pi^2\cdot 6\cdot 8} - \left(1 - \frac{6}{\pi^2}\right) \approx 0.051.$$

□

In both proofs, the densities would be improved if we could assume that the square-freeness of the two relevant quantities is independent. If this was the case, then we would expect a lower bound for the family of Theorem 3.5 of at least

$$B_1 := \frac{36^2}{\pi^4}\prod_{p|(n-1)}\left(1 - \frac{1}{p^2}\right)^{-1}$$

and for the family of Theorem 3.6 of at least

$$B_2 := \frac{6^2}{\pi^4}\prod_{p|c}\frac{p}{p+1}\prod_{p|n}\frac{p^2}{p^2-1}.$$

Note that, using $\prod_p \left(1-\frac{1}{p^2}\right)^{-1} = \zeta(2)$,

$$0.28 \approx \frac{27}{\pi^4} \leq B_1 \leq \frac{6}{\pi^2} \approx 0.61.$$

Similarly, we have

$$0 \leq B_2 \leq \frac{6^2}{\pi^4} \prod_p \left(1+\frac{1}{p^2-1}\right) \leq \frac{72}{\pi^4} \approx 0.74.$$

6. Computational Data

Table 3 is for comparison to Theorems 3.5 and 3.6. We can see it is rare that one of our trinomials yields a monogenic field for which it is not a generator. It is also noteworthy that our theorems on the monogeneity of the trinomials f and g do not capture all instances in which f and g yield monogenic fields. Specifically, there are instances when the relevant factors of Δ_f and Δ_g are not square-free, but those square factors do not contribute to the index. It does not appear the machinery we use is adequate to understand when and why these square factors do not contribute to the index.

References

[1] A. R. Booker and T. D. Browning. Square-free values of reducible polynomials. *Discrete Anal.*, Paper No. 8, 16, 2016. ISSN 2397-3129. doi: 10.19086/da.732. URL https://doi.org/10.19086/da.732.

[2] D. W. Boyd, G. Martin, and M. Thom. Squarefree values of trinomial discriminants. *LMS J. Comput. Math.*, 18(1):148–169, 2015. ISSN 1461-1570. doi: 10.1112/S1461157014000436. URL https://doi.org/10.1112/S1461157014000436.

[3] R. Dedekind. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Gött. Abhandlungen*, 23:3–38, 1878.

[4] J.-H. Evertse and K. Győry. *Discriminant equations in Diophantine number theory*, volume 32 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, 2017. ISBN 978-1-107-09761-2. doi: 10.1017/CBO9781316160763. URL https://doi.org/10.1017/CBO9781316160763.

[5] L. E. Fadil, J. Montes, and E. Nart. Newton polygons and p-integral bases of quartic number fields. *Journal of Algebra and Its Applications*, 11(04):1250073, 2012. doi: 10.1142/S0219498812500739. URL https://www.worldscientific.com/doi/abs/10.1142/S0219498812500739.

[6] I. Gaál. *Diophantine equations and power integral bases.* Birkhäuser/Springer, Cham, 2019. ISBN 978-3-030-23864-3; 978-3-030-23865-0. doi: 10.1007/978-3-030-23865-0. URL https://doi.org/10.1007/978-3-030-23865-0. Theory and algorithms, Second edition of [MR1896601].

[7] T. A. Gassert. Discriminants of Chebyshev radical extensions. *J. Théor. Nombres Bordeaux*, 26(3):607–634, 2014. ISSN 1246-7405. URL http://jtnb.cedram.org/item?id=JTNB_2014__26_2_607_0.

[8] T. A. Gassert. A note on the monogeneity of power maps. *Albanian J. Math.*, 11(1):3–12, 2017. ISSN 1930-1235.

[9] M.-N. Gras. Condition nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de $\mathbf{Q}$. In *Séminaire de théorie des nombres, Paris 1984–85*, volume 63 of *Progr. Math.*, pages 97–107. Birkhäuser Boston, Boston, MA, 1986.

[10] M.-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbf{Q}$ de degré premier $l \geq 5$. *J. Number Theory*, 23(3):347–353, 1986. ISSN 0022-314X. doi: 10.1016/0022-314X(86)90079-X. URL https://doi.org/10.1016/0022-314X(86)90079-X.

TABLE 3. Monogenic Percentages for Degrees 5 and 6

Family	% monogenic	% with θ a generator	% satisfying hypotheses of relevant Theorem
x^5+bx+b	52.46	50.50	50.50
x^6+bx+b	58.49	57.71	57.71
x^5+cx^4+c	44.84	43.10	35.92
x^6+cx^5+c	58.68	58.00	29.00
x^5+ax+b	61.17	60.86	60.86
x^6+ax+b	61.10	60.90	60.90
x^5+cx^4+d	55.78	51.80	51.80
x^6+cx^5+d	45.43	44.66	26.00
x^5+2x^4+2d	36.88	33.67	33.67
x^5+3x^4+3d	43.96	43.29	43.29
x^5+4x^4+4d	65.97	0.00	0.00
x^5+5x^4+5d	42.19	42.08	42.08
x^5+6x^4+6d	32.05	28.85	28.85
x^5+7x^4+7d	45.18	45.13	45.13
x^5+8x^4+8d	13.08	0.00	0.00
x^6+2x^5+2d	40.29	38.48	38.48
x^6+3x^5+3d	43.53	43.28	14.43
x^6+4x^5+4d	2.50	0.00	0.00
x^6+5x^5+5d	48.11	48.09	16.03
x^6+6x^5+6d	30.38	28.86	28.84
x^6+7x^5+7d	51.57	51.57	17.19
x^6+8x^5+8d	4.91	0.00	0.00

For families with a single parameter a, b, c, or d, the values tested were $[-500000, 500000]$. For families with two parameters the values tested were $[-500, 500]$. The percentages are rounded to the nearest hundredth.

[11] J. Guàrdia, J. Montes, and E. Nart. Higher newton polygons and integral bases. *Journal of Number Theory*, 147:549 – 589, 2015. ISSN 0022-314X. doi: https://doi.org/10.1016/j.jnt.2014.07.027. URL http://www.sciencedirect.com/science/article/pii/S0022314X14002777.

[12] A. Jakhar, S. K. Khanduja, and N. Sangwan. On prime divisors of the index of an algebraic integer. *J. Number Theory*, 166:47–61, 2016. ISSN 0022-314X. doi: 10.1016/j.jnt.2016.02.021. URL https://doi.org/10.1016/j.jnt.2016.02.021.

[13] A. Jakhar, S. K. Khanduja, and N. Sangwan. Characterization of primes dividing the index of a trinomial. *Int. J. Number Theory*, 13(10):2505–2514, 2017. ISSN 1793-0421. doi: 10.1142/S1793042117501391. URL https://doi.org/10.1142/S1793042117501391.

[14] L. Jones and T. Phillips. Infinite families of monogenic trinomials and their Galois groups. *Internat. J. Math.*, 29(5):1850039, 11, 2018. ISSN 0129-167X. doi: 10.1142/S0129167X18500398. URL https://doi.org/10.1142/S0129167X18500398.

[15] L. Jones and D. White. Monogenic trinomials with non-squarefree discriminant. *arXiv e-prints*, art. arXiv:1908.07947, Aug 2019. To appear in *The International Journal of Mathematics*.

[16] K. S. Kedlaya. A construction of polynomials with squarefree discriminants. *Proc. Amer. Math. Soc.*, 140(9):3025–3033, 2012. ISSN 0002-9939. doi: 10.1090/S0002-9939-2012-11231-6. URL https://doi.org/10.1090/S0002-9939-2012-11231-6.

[17] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004. ISBN 3-540-21902-1. doi: 10.1007/978-3-662-07001-7. URL https://doi.org/10.1007/978-3-662-07001-7.

[18] Ø. Ore. Newtonsche Polygone in der Theorie der algebraischen Körper. *Math. Ann.*, 99(1): 84–117, 1928. ISSN 0025-5831. doi: 10.1007/BF01459087. URL https://doi.org/10.1007/BF01459087.

[19] K. Prachar. Über die kleinste quadratfreie zahl einer arithmetischen reihe. *Monatshefte für Mathematik*, 62:173–176, 1958. URL http://eudml.org/doc/177039.

[20] H. Smith. Two families of monogenic S_4 quartic number fields. *Acta Arith.*, 186(3):257–271, 2018. ISSN 0065-1036. doi: 10.4064/aa180423-24-8. URL https://doi.org/10.4064/aa180423-24-8.

[21] R. G. Swan. Factorization of polynomials over finite fields. *Pacific J. Math.*, 12:1099–1106, 1962. ISSN 0030-8730. URL http://projecteuclid.org/euclid.pjm/1103036322.

[22] J. Westlund. On the fundamental number of the algebraic number-field $k(\sqrt[p]{m})$. *Trans. Amer. Math. Soc.*, 11(4):388–392, 1910. ISSN 0002-9947. doi: 10.2307/1988640. URL https://doi.org/10.2307/1988640.

Email address: Henry.Lembeck@colorado.edu
Email address: Mohammad.Ozaslan@colorado.edu
Email address: Ryan.Ibarra@colorado.edu
Email address: hanson.smith@uconn.edu
Email address: kstange@math.colorado.edu

Department of Mathematics, University of Colorado, Campus Box 395, Boulder, Colorado 80309-0395 USA

Department of Mathematics, University of Connecticut, 341 Mansfield Road U1009 Storrs, CT 06269-1009 USA