Annales Mathematicae et Informaticae
55 (2022) pp. 93–113
DOI: https://doi.org/10.33039/ami.2022.09.001
URL: https://ami.uni-eszterhazy.hu

The monogenity of power-compositional Eisenstein polynomials

Lenny Jones

Shippensburg University
doctorlennyjones@gmail.com

Abstract. We construct infinite collections of monic Eisenstein polynomials $f(x) \in \mathbb{Z}[x]$ such that the power-compositional polynomials $f(x^{d^n})$ are monogenic for all integers $n \geq 0$ and any integer $d > 1$, where d has the property that $f(x)$ is Eisenstein with respect to every prime divisor of d. We also investigate extending these ideas to power-compositional Eisenstein polynomials $f(x^{s^n})$, where s has a prime divisor p such that $f(x)$ is not Eisenstein with respect to p.

Keywords: Eisenstein, irreducible, monogenic, power-compositional

AMS Subject Classification: Primary 11R04, Secondary 11R09, 12F05

1. Introduction

Let $f(x) \in \mathbb{Z}[x]$ be monic. We define $f(x)$ to be *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\{1, \theta, \theta^2, \ldots, \theta^{\deg(f)-1}\}$ is a basis for the ring of integers of $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. We say that $f(x)$ is *p-Eisenstein*, or simply *Eisenstein*, if there exists a prime p such that $f(x) \equiv x^{\deg(f)} \pmod{p}$, but $f(0) \not\equiv 0 \pmod{p^2}$. It is well known that Eisenstein polynomials are irreducible over $\mathbb{Q}$. Throughout this article, we use the following notation:

- $\mathcal{P}(z)$ is the set of all prime divisors of the integer $z > 1$,
- $\mathcal{E}_f$ is the set of all primes p for which $f(x)$ is p-Eisenstein,
- Π_f is the product of all primes in $\mathcal{E}_f$,
- Γ_f is the set of all integers $d > 1$ such that $\mathcal{P}(d) \subseteq \mathcal{E}_f$,
- Λ_f is the set of all integers $\lambda > 1$ such that the power-compositional polynomials $f(x^{\lambda^n})$ are monogenic for all integers $n \geq 0$.

Submitted: July 25, 2022
Accepted: September 1, 2022
Published online: September 13, 2022

The main purpose of this article is the construction of infinite collections of monic Eisenstein polynomials $f(x) \in \mathbb{Z}[x]$ such that the power-compositional polynomials $f(x^{d^n})$ are monogenic for all integers $n \geq 0$ and all integers $d \in \Gamma_f$. We divide the main investigation section (Section 3) into subsections according to trinomials, quadrinomials, quintinomials and sextinomials. Binomials, which are fully understood, are discussed briefly in Section 4. The approach we use for trinomials utilizes a result of Jakhar, Khanduja and Sangwan [11] that is tailored specifically for the determination of the monogenity of trinomials. For quadrinomials and beyond, we use a different approach that is based partly on ideas found in [12]. To facilitate our methods in these cases, we also prove a new result that establishes the fact that $\Gamma_f \subseteq \Lambda_f$ for any monogenic Eisenstein polynomial with $|f(0)| = \Pi_f$ (see Lemma 3.1). The following theorem, which is an excerpt taken from Theorem 3.9 in Section 3.2, represents a typical result from Section 3.

Theorem 1.1. *Let $N, \mathcal{K}, t, C \in \mathbb{Z}$ with $N \geq 3$, $\gcd(\mathcal{K}, N) = 1$ and $\mathcal{K}$ squarefree. Let*

$$f(x) = x^N + \mathcal{K}t\big((2CN - 2C + 1)x^2 + (2CN^2 - 4CN + N - 1)x + 1\big).$$

Then there exist infinitely many prime values of t such that $f(x^{d^n})$ is monogenic for all $d \in \Gamma_f$ and all integers $n \geq 0$.

Remark 1.2. We point out that infinite families of monogenic power-compositional trinomials were given in [8]. However, Eisenstein polynomials were not specifically addressed there.

2. Preliminaries

We first require some standard tools and notation. Let $\Delta(f(x))$, or simply $\Delta(f)$, and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of $f(x) \in \mathbb{Z}[x]$ and a number field K. If $f(x)$ is irreducible over $\mathbb{Q}$ with $f(\theta) = 0$, then [1]

$$\Delta(f) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \Delta(K). \tag{2.1}$$

Observe then, from (2.1), that $f(x)$ is monogenic if and only if $\Delta(f) = \Delta(K)$. We also see from (2.1) that if $\Delta(f)$ is squarefree, then $f(x)$ is monogenic. However, the converse is false in general, and when $\Delta(f)$ is not squarefree, it can be quite difficult to determine whether $f(x)$ is monogenic.

Definition 2.1. [1] Let $\mathcal{R}$ be an integral domain with quotient field K, and let $\overline{K}$ be an algebraic closure of K. Let $f(x), g(x) \in \mathcal{R}[x]$, and suppose that $f(x) = a\prod_{i=1}^{m}(x - \alpha_i) \in \overline{K}[x]$ and $g(x) = b\prod_{i=1}^{n}(x - \beta_i) \in \overline{K}[x]$. Then the *resultant* $R(f, g)$ of f and g is:

$$R(f, g) = a^n \prod_{i=1}^{m} g(\alpha_i) = (-1)^{mn} b^m \prod_{i=1}^{n} f(\beta_i).$$

The following theorem is a well-known result in algebraic number theory [2].

Theorem 2.2. *Let p be a prime and let $f(x) \in \mathbb{Z}[x]$ be a monic p-Eisenstien polynomial with $\deg(f) = N$. Let $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. Then*

1. *$p^{N-1} || \Delta(K)$ if $N \not\equiv 0 \pmod{p}$,*
2. *$p^N | \Delta(K)$ if $N \equiv 0 \pmod{p}$.*

Theorem 2.3. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Q}[x]$, with respective leading coefficients a and b, and respective degrees m and n. Then*

$$\Delta(f \circ g) = (-1)^{m^2 n(n-1)/2} \cdot a^{n-1} b^{m(mn-n-1)} \Delta(f)^n R(f \circ g, g').$$

Remark 2.4. As far as we can determine, Theorem 2.3 is originally due to John Cullinan [3]. A proof of Theorem 2.3 can be found in [7].

The following theorem, known as *Dedekind's Index Criterion*, or simply *Dedekind's Criterion* if the context is clear, is a standard tool used in determining the monogenity of a polynomial.

Theorem 2.5 (Dedekind [1])**.** *Let $K = \mathbb{Q}(\theta)$ be a number field, $T(x) \in \mathbb{Z}[x]$ the monic minimal polynomial of θ, and $\mathbb{Z}_K$ the ring of integers of K. Let q be a prime number and let $\overline{*}$ denote reduction of $*$ modulo q (in $\mathbb{Z}$, $\mathbb{Z}[x]$ or $\mathbb{Z}[\theta]$). Let*

$$\overline{T}(x) = \prod_{i=1}^{k} \overline{\tau_i}(x)^{e_i}$$

be the factorization of $T(x)$ modulo q in $\mathbb{F}_q[x]$, and set

$$g(x) = \prod_{i=1}^{k} \tau_i(x),$$

where the $\tau_i(x) \in \mathbb{Z}[x]$ are arbitrary monic lifts of the $\overline{\tau_i}(x)$. Let $h(x) \in \mathbb{Z}[x]$ be a monic lift of $\overline{T}(x)/\overline{g}(x)$ and set

$$F(x) = \frac{g(x)h(x) - T(x)}{q} \in \mathbb{Z}[x].$$

Then

$$[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q} \iff \gcd\left(\overline{F}, \overline{g}, \overline{h}\right) = 1 \text{ in } \mathbb{F}_q[x].$$

The following theorem appears as Theorem 1 in [12].

Theorem 2.6. *Let N and k be integers with $N > k \geq 1$. Let*

$$f(x) = x^N + \mathcal{T} u(x), \text{ where } \mathcal{T} \in \mathbb{Z} \text{ and}$$

$$u(x) = a_k x^k + a_{k-1} x^{k-1} + a_{k-2} x^{k-2} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \text{ with } a_0, a_k \neq 0.$$

Suppose that $f(x)$ is irreducible over $\mathbb{Q}$, and let $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. Then

$$\Delta(f) = \frac{(-1)^{\frac{N(N+2k-1)}{2}} \mathcal{T}^{N-1} \mathcal{N}(\widehat{u}(\theta))}{a_0},$$

where

$$\widehat{u}(x) = a_k(N-k)x^k + a_{k-1}(N-(k-1))x^{k-1} + \cdots + a_1(N-1)x + a_0 N,$$

and $\mathcal{N} := \mathcal{N}_{K/Q}$ is the algebraic norm. Moreover, if

$$\widehat{u}(x) = \prod_{i=1}^{k} (A_i x + B_i),$$

where the $A_i x + B_i \in \mathbb{Z}[x]$ are not necessarily distinct, then

$$\mathcal{N}(\widehat{u}(\theta)) = \prod_{i=1}^{k} \left(\mathcal{T} \sum_{j=0}^{k} a_j A_i^{N-j} (-B_i)^j + (-B_i)^N \right).$$

The following corollary of Theorem 2.6 will be useful in this article.

Corollary 2.7. *Let $f(x)$, $u(x)$ and $\widehat{u}(x)$ be as defined in Theorem 2.6. Suppose that $f(x)$ is irreducible over $\mathbb{Q}$, $K = \mathbb{Q}(\theta)$ where $f(\theta) = 0$, and the content of $u(x)$ is 1. If $\mathcal{T}\mathcal{N}(\widehat{u}(\theta))/a_0$ is squarefree, then $\gcd(\mathcal{T}, N) = 1$ and $f(x)$ is monogenic.*

Proof. If $\mathcal{T} = 1$, the corollary is obviously true. If $|\mathcal{T}| \geq 2$, then $f(x)$ is Eisenstein with $\Pi_f = |\mathcal{T}|$, since the content of $u(x)$ is 1. Let p be a prime divisor of Π_f. If $p \mid N$, then $p^N \mid \Delta(K)$ by Theorem 2.2, which contradicts the fact that $\Pi_f \mathcal{N}(\widehat{u}(\theta))/a_0$ is squarefree. Hence, $p \nmid N$ and $p^{N-1} \mid\mid \Delta(K)$ by Theorem 2.2, which completes the proof. □

The next theorem follows from Corollary (2.10) in [14].

Theorem 2.8. *Let K and L be number fields with $K \subset L$. Then*

$$\Delta(K)^{[L:K]} \mid \Delta(L).$$

Theorem 2.9. *Let $G(t) \in \mathbb{Z}[t]$, and suppose that $G(t)$ factors into a product of distinct irreducibles, such that the degree of each irreducible is at most 3. Define*

$$N_G(X) = |\{p \leq X : p \text{ is prime and } G(p) \text{ is squarefree}\}|.$$

Then,

$$N_G(X) \sim C_G \frac{X}{\log(X)},$$

where

$$C_G = \prod_{\ell \text{ prime}} \left(1 - \frac{\rho_G(\ell^2)}{\ell(\ell-1)}\right)$$

and $\rho_G(\ell^2)$ is the number of $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$ such that $G(z) \equiv 0 \pmod{\ell^2}$.

Remark 2.10. Theorem 2.9 follows from work of Helfgott, Hooley and Pasten [9, 10, 15]. For more details, see [13].

Definition 2.11. In the context of Theorem 2.9, for $G(t) \in \mathbb{Z}[t]$ and a prime ℓ, if $G(z) \equiv 0 \pmod{\ell^2}$ for all $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$, we say that $G(t)$ has a *local obstruction* at ℓ.

The following immediate corollary of Theorem 2.9 is a tool used to establish the main results in this article.

Corollary 2.12. *Let $G(t) \in \mathbb{Z}[t]$, and suppose that $G(t)$ factors into a product of distinct irreducibles, such that the degree of each irreducible is at most 3. To avoid the situation when $C_G = 0$, we suppose further that $G(t)$ has no local obstructions. Then there exist infinitely many primes q such that $G(q)$ is squarefree.*

We make the following observation concerning $G(t)$ from Corollary 2.12 in the special case when each of the distinct irreducible factors of $G(t)$ is of the form $\alpha_i t + \beta_i \in \mathbb{Z}[t]$ with $\gcd(\alpha_i, \beta_i) = 1$. In this situation, it follows that the minimum number of distinct factors required in $G(t)$ so that $G(t)$ has a local obstruction at the prime ℓ is $2(\ell - 1)$. More precisely, in this minimum scenario, we have

$$G(t) = \prod_{i=1}^{2(\ell-1)} (\alpha_i t + \beta_i) \equiv C(t-1)^2(t-2)^2 \cdots (t-(\ell-1))^2 \pmod{\ell},$$

where $C \not\equiv 0 \pmod{\ell}$. Then each zero r of $G(t)$ modulo ℓ lifts to the ℓ distinct zeros

$$r, \quad r+\ell, \quad r+2\ell, \quad \ldots\ldots, \quad r+(\ell-1)\ell \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$$

of $G(t)$ modulo ℓ^2 [4, Theorem 4.11]. That is, $G(t)$ has exactly $\ell(\ell-1) = \phi(\ell^2)$ distinct zeros $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$. Therefore, if the number of factors k of $G(t)$ satisfies $k < 2(\ell-1)$, then there must exist $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$ for which $G(z) \not\equiv 0 \pmod{\ell^2}$, and we do not need to check such primes ℓ for a local obstruction. Consequently, only finitely many primes need to be checked for local obstructions. They are precisely the primes ℓ such that $\ell \leq (k+2)/2$.

3. The main results

This section is devoted to the construction of infinite collections of monic Eisenstein polynomials $f(x) \in \mathbb{Z}[x]$ with the property that the power-compositional polynomials $f(x^{d^n})$ are monogenic for all integers $n \geq 0$ and all integers $d \in \Gamma_f$. We begin with a new result that is key to our investigations in Sections 3.2, 3.3 and 3.4.

Lemma 3.1. *Let $f(x) \in \mathbb{Z}[x]$ be Eisenstein with $\deg(f) = N$. If $f(x)$ is monogenic and $|f(0)| = \Pi_f$, then $\Gamma_f \subseteq \Lambda_f$.*

Proof. Note first that we can write

$$f(x) = x^N + \Pi_f w(x), \text{ for some } w(x) \in \mathbb{Z}[x], \text{ with } |w(0)| = 1. \tag{3.1}$$

Let $d \in \Gamma_f$. For $n \geq 0$, define

$$\mathcal{F}_n(x) := f(x^{d^n}), \quad \theta_n := \theta^{1/d^n} \quad \text{and} \quad K_n := \mathbb{Q}(\theta_n),$$

where $f(\theta) = 0$. Then $\theta_0 = \theta$, $\mathcal{F}_0(x) = f(x)$ and, since $f(x)$ is monogenic, we have that $\Delta(f) = \Delta(\mathcal{F}_0) = \Delta(K_0)$. Additionally, for all $n \geq 0$,

$$\mathcal{F}_n(\theta_n) = 0, \quad [K_{n+1} : K_n] = d \quad \text{and} \quad \mathcal{F}_n(x) \text{ is Eisesntein with } |\mathcal{F}_n(0)| = \Pi_f.$$

We have that $\mathcal{F}_0(x)$ is monogenic by hypothesis, and we need to show that $\mathcal{F}_n(x)$ is monogenic for all integers $n \geq 1$. Assume that $\mathcal{F}_n(x)$ is monogenic, so that $\Delta(\mathcal{F}_n) = \Delta(K_n)$, and proceed by induction on n to show that $\mathcal{F}_{n+1}(x)$ is monogenic. Let $\mathbb{Z}_{K_n}$ denote the ring of integers of K_n. Consequently, by Theorem 2.8, it follows that

$$\Delta(\mathcal{F}_n)^d \text{ divides } \Delta(K_{n+1}) = \frac{\Delta(\mathcal{F}_{n+1})}{[\mathbb{Z}_{K_{n+1}} : \mathbb{Z}[\theta_{n+1}]]^2},$$

which implies that

$$[\mathbb{Z}_{K_{n+1}} : \mathbb{Z}[\theta_{n+1}]]^2 \text{ divides } \frac{\Delta(\mathcal{F}_{n+1})}{\Delta(\mathcal{F}_n)^d}.$$

Since $|f(0)| = \Pi_f$, we see from Theorem 2.3 that

$$\begin{aligned} \left|\Delta(\mathcal{F}_n)^d\right| &= \left|\Delta(f)^{d^{n+1}} d^{nd^{n+1}N} (\Pi_f)^{d^{n+1}-d}\right| \quad \text{and} \\ |\Delta(\mathcal{F}_{n+1})| &= \left|\Delta(f)^{d^{n+1}} d^{(n+1)d^{n+1}N} (\Pi_f)^{d^{n+1}-1}\right|. \end{aligned}$$

Hence,

$$\left|\frac{\Delta(\mathcal{F}_{n+1})}{\Delta(\mathcal{F}_n)^d}\right| = d^{d^{n+1}N} (\Pi_f)^{d-1}.$$

Since $\mathcal{P}(d) \subseteq \mathcal{E}_f$, it is enough to show that $\gcd(\Pi_f, [\mathbb{Z}_{K_{n+1}} : \mathbb{Z}[\theta_{n+1}]]) = 1$. To establish this fact, we apply Theorem 2.5 to $T := \mathcal{F}_{n+1}(x)$, with q a prime divisor of Π_f. Then we see from (3.1) that $\overline{T}(x) = x^{d^{n+1}N}$, and so we can let $g(x) = x$ and $h(x) = x^{d^{n+1}N-1}$. Hence

$$F(x) = \frac{g(x)h(x) - T(x)}{q} = -\frac{\Pi_f}{q} w(x^{d^{n+1}}).$$

Since Π_f is squarefree, and $|w(0)| = 1$, we deduce that $\overline{F}(0) \neq 0$ and therefore, $\gcd(\overline{F}, \overline{g}) = 1$. Thus, by Theorem 2.5, we conclude that

$$[\mathbb{Z}_{K_{n+1}} : \mathbb{Z}[\theta_{n+1}]] \not\equiv 0 \pmod{q}$$

and, consequently, $\mathcal{F}_{n+1}(x)$ is monogenic, which completes the proof. □

We see from Lemma 3.1 that we only need to focus on finding infinite collections of monogenic Eisenstein polynomials $f(x)$ with $|f(0)| = \Pi_f$ to produce infinite collections of Eisenstein polynomials with the desired power-compositional properties. Lemma 3.1 will be used for quadrinomials and beyond, but a separate approach is used for trinomials.

3.1. Trinomials

The formula for the discriminant of an arbitrary monic trinomial, due to Swan [16], is given in the following theorem.

Theorem 3.2. *Let $f(x) = x^N + Ax^M + B \in \mathbb{Z}[x]$, where $0 < M < N$. Let $r = \gcd(N, M)$, $N_1 = N/r$ and $M_1 = M/r$. Then*

$$\Delta(f) = (-1)^{N(N-1)/2} B^{M-1} D^r,$$

where

$$D := N^{N_1} B^{N_1 - M_1} - (-1)^{N_1} M^{M_1} (N-M)^{N_1 - M_1} A^{N_1}.$$

Applying Theorem 3.2 to the power-compositional trinomial

$$\mathcal{F}_n(x) := f(x^{d^n}) = x^{d^n N} + Ax^{d^n M} + B \tag{3.2}$$

we get the following immediate corollary.

Corollary 3.3. *Let $f(x)$ and D be as given in Theorem 3.2, and let $\mathcal{F}_n(x)$ be as defined in (3.2). Let $d, n \in \mathbb{Z}$ with $d \geq 1$ and $n \geq 0$. Then*

$$\Delta(\mathcal{F}_n) = (-1)^{d^n N(d^n N - 1)/2} B^{d^n M - 1} d^{n d^n N} D^{d^n r}.$$

The next result is essentially an algorithmic adaptation of Dedekind's index criterion for trinomials.

Theorem 3.4. [11] *Let $N \geq 2$ be an integer. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in \mathbb{Z}_K$, the ring of integers of K, having minimal polynomial $f(x) = x^N + Ax^M + B$ over $\mathbb{Q}$, with $\gcd(M, N) = r$, $N_1 = N/r$ and $M_1 = M/r$. Let D be as defined in Theorem 3.2. A prime factor q of $\Delta(f)$ does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if q satisfies one of the following conditions:*

1. *when $q \mid A$ and $q \mid B$, then $q^2 \nmid B$;*
2. *when $q \mid A$ and $q \nmid B$, then*

$$\text{either} \quad q \mid A_2 \text{ and } q \nmid B_1 \quad \text{or} \quad q \nmid A_2 \Big((-B)^{M_1} A_2^{N_1} - (-B_1)^{N_1} \Big),$$

where $A_2 = A/q$ and $B_1 = \frac{B + (-B)^{q^e}}{q}$ with $q^e \mid\mid N$;

3. *when* $q \nmid A$ *and* $q \mid B$, *then*

   either $q \mid A_1$ *and* $q \nmid B_2$ *or* $q \nmid A_1 B_2^{M-1}\big((-A)^{M_1}A_1^{N_1-M_1} - (-B_2)^{N_1-M_1}\big)$,

   where $A_1 = \frac{A+(-A)^{q^j}}{q}$ *with* $q^j \mid\mid (N-M)$, *and* $B_2 = B/q$;

4. *when* $q \nmid AB$ *and* $q \mid M$ *with* $N = s'q^k$, $M = sq^k$, $q \nmid \gcd(s', s)$, *then the polynomials*

$$x^{s'} + Ax^s + B \quad \text{and} \quad \frac{Ax^{sq^k} + B + (-Ax^s - B)^{q^k}}{q}$$

   are coprime modulo q;

5. *when* $q \nmid ABM$, *then* $q^2 \nmid D/r^{N_1}$.

The following theorem lays the groundwork for the construction of infinite collections of monogenic power-compositional Eisenstein trinomials.

Theorem 3.5. *Suppose that* $f(x) = x^N + Ax^M + B \in \mathbb{Z}[x]$ *is Eisenstein with* $N > M > 0$ *and* B *squarefree. Suppose further that* $\Pi_f \equiv 0 \pmod{\kappa}$, *where* κ *is the squarefree kernel of* $r := \gcd(N, M)$. *Let*

$$\rho = \prod_{\substack{p \mid \Pi_f \\ p \text{ prime}}} p^{\nu_p(D)} \quad \text{and} \quad \mathfrak{D} = D/\rho,$$

where ν_p *is the* p*-adic valuation, and* D *is as defined in Theorem 3.2. If* $\mathfrak{D}$ *is squarefree and* $d \in \Gamma_f$, *then* $\mathcal{F}_n(x) := f(x^{d^n})$ *is monogenic for all integers* $n \geq 0$.

Proof. Note that $\mathcal{F}_n(x)$ is Eisenstein, and hence is irreducible over $\mathbb{Q}$. Suppose that $\mathcal{F}_n(\theta) = 0$, and let $\mathbb{Z}_K$ be the ring of integers of $K = \mathbb{Q}(\theta)$. To establish monogenity, we use Theorem 3.4 to show that $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$ for all primes q dividing $\Delta(\mathcal{F}_n)$ in Corollary 3.3. Since $\mathcal{P}(d) \subseteq \mathcal{P}(B)$, we only have to address primes dividing BD.

Suppose first that $q \mid B$. If $q \mid A$, then condition (1) of Theorem 3.4 is satisfied since B is squarefree. Suppose then that $q \nmid A$, and we examine condition (3). Note that $q \nmid \Pi_f$. If $q \nmid A_1$, then $q^j \mid\mid (d^n N - d^n M)$ for some integer $j \geq 1$. Thus, since $q \nmid d$, we conclude that

$$N - M = q^j c, \tag{3.3}$$

for some integer $c \geq 1$. If $N_1 - M_1 > 1$, then

$$q^2 \mid B^{N_1 - M_1} \quad \text{and} \quad q^2 \mid (N-M)^{N_1-M_1}.$$

Thus, $q^2 \mid D$, which implies that $q^2 \mid \mathfrak{D}$ since $q \nmid \Pi_f$, contradicting the fact that $\mathfrak{D}$ is squarefree. Therefore, $N_1 - M_1 = 1$ and we deduce from (3.3) that

$$1 = N_1 - M_1 = (N-M)/r = q^j c/r,$$

which contradicts the fact that $q \nmid r$. Hence, $q \mid A_1$, and since B is squarefree, condition (3) of Theorem 3.4 is satisfied.

Suppose next that $q \mid D$ and $q \nmid B$. If $q \mid A$, then $q \mid N$ so that

$$q^2 \mid N^{N_1} \quad \text{and} \quad q^2 \mid A^{N_1}.$$

Then $q^2 \mid D$, which implies that $q^2 \mid \mathfrak{D}$ since $q \nmid \Pi_f$, contradicting the fact that $\mathfrak{D}$ is squarefree. If $q \nmid AB$ and $q \mid M$, then $q \mid N$. We then conclude that

$$q^2 \mid N^{N_1} \quad \text{and} \quad q^2 \mid M^{M_1}(N-M)^{N_1-M_1}.$$

Then, as before, $q^2 \mid D$, which implies that $q^2 \mid \mathfrak{D}$ since $q \nmid \Pi_f$, contradicting the fact that $\mathfrak{D}$ is squarefree. Finally, suppose that $q \nmid ABM$. Thus, $q^2 \nmid D/r^{N_1}$ since $q \nmid \Pi_f$ and $\mathfrak{D}$ is squarefree, so that condition (5) is satisfied. □

The following corollary illustrates how Theorem 3.5 can be used to construct infinite collections of monic Eisenstein trinomials with the desired power-compositional properties.

Corollary 3.6. *Let $N, C, t \in \mathbb{Z}$ be such that $N \geq 2$ and Ct is squarefree. Then, in each of the following situations, there exist infinitely many prime values of t such that $f(x^{d^n})$ is monogenic for any $d \in \Gamma_f$ and all integers $n \geq 0$:*

1. *$f(x) = x^N + Ctx + Ct$, where $|Ct| \geq 2$ and $\gcd(Ct, N) = 1$,*
2. *$f(x) = x^N + Cx^{N-1} + Ct$, where $|C| \geq 2$ and $\gcd(C, Nt) = 1$,*
3. *$f(x) = x^p + px^{p-1} + pt$, where p is prime.*

Proof. Observe that $f(x)$ is Eisenstein for all situations. For (1), in the setting of Theorem 3.5, we have

$$A = B = Ct, \quad \Pi_f = |Ct|, \quad r = \kappa = 1 \quad \text{and}$$

$$D = (-1)^{N-1}(Ct)^{N-1}\big((N-1)^{N-1}Ct - (-1)^N N^N\big),$$

so that $\Pi_f \equiv 0 \pmod{\kappa}$ and

$$\mathfrak{D} = (1-N)^{N-1}Ct + N^N,$$

since $\gcd(Ct, N) = 1$. Thinking of t as an indeterminate, let $G(t) = \mathfrak{D}$. Since $G(t)$ has no local obstructions, we conclude from Corollary 2.12 that there exist infinitely many primes q such that $G(q)$ is squarefree. Since Ct is also squarefree for any such prime $t = q > C$, part (1) follows from Theorem 3.5.

For (2), in the setting of Theorem 3.5, we have

$$A = C, \quad B = Ct, \quad \Pi_f = |C|, \quad r = \kappa = 1 \quad \text{and}$$

$$D = C\big(N^N t - (-1)^N (N-1)^{N-1} C^{N-1}\big),$$

so that $\Pi_f \equiv 0 \pmod{\kappa}$ and

$$\mathfrak{D} = N^N t - (-1)^N (N-1)^{N-1} C^{N-1}.$$

The remainder of the proof for this part is identical to part (1), and we omit the details.

Finally, for (3), we have that

$$N = p, \quad M = p-1, \quad A = p, \quad B = pt, \quad \Pi_f = p, \quad r = \kappa = 1 \quad \text{and}$$

$$D = p^p(pt - (-1)^p(p-1)^{p-1}) = p^p \mathfrak{D}.$$

Again, the remainder of the proof for this part is identical to part (1), and we omit the details. □

Note that part (3) of Corollary 3.6 is similar to part (2), except that we have lifted the restriction $\gcd(C, Nt) = 1$. Indeed, this restriction is really unnecessary in part (2). However, we have added it there to make the computation of $\mathfrak{D}$ more transparent. Similarly, the restriction $\gcd(Ct, N) = 1$ can be lifted from part (1) as well.

3.2. Quadrinomials

The following lemma contains two special cases of Theorem 2.6.

Lemma 3.7. *Let $N, \mathcal{T}, C \in \mathbb{Z}$ with $N \geq 3$.*

1. *Suppose that*

$$f(x) = x^N + \mathcal{T}\big((2CN - 2C + 1)x^2 + (2CN^2 - 4CN + N - 1)x + 1\big)$$

is irreducible over $\mathbb{Q}$. Then $|\Delta(f)| = \big|\mathcal{T}^{N-1} T_1 T_2\big|$, where

$$T_1 = (2CN^2 + N + 1)\mathcal{T} + (-N)^N \text{ and}$$
$$T_2 = -(N-2)^{N-2}(2CN - 2C + 1)^{N-1}(2CN^2 - 8CN + N + 8C - 3)\mathcal{T} + (-1)^N.$$

2. *Suppose that*

$$f(x) = x^N + \mathcal{T}((CN - C + 1)x^2 + (CN + 2)x + 1)$$

is irreducible over $\mathbb{Q}$. Then $|\Delta(f)| = \big|\mathcal{T}^{N-1} T_1 T_2\big|$, where

$$T_1 = (N-2)^{N-2}(CN^2 + 4)\mathcal{T} + (-N)^N \text{ and}$$
$$T_2 = -C(CN - C + 1)^{N-1}\mathcal{T} + (-1)^N.$$

Proof. We give details only for *(1)* since the details for *(2)* are similar. For *(1)*, we have in the setting of Theorem 2.6 that

$$u(x) = (2CN - 2C + 1)x^2 + (2CN^2 - 4CN + N - 1)x + 1 \text{ and}$$
$$\widehat{u}(x) = \big(x + N\big)\big((N-2)(2CN - 2C + 1)x + 1\big),$$

so that

$$a_2 = 2CN - 2C + 1, \quad a_1 = 2CN^2 - 4CN + N - 1, \quad a_0 = 1,$$
$$A_1 = 1, \quad B_1 = N, \quad A_2 = (N-2)(2CN - 2C + 1) \quad \text{and} \quad B_2 = 1.$$

Then $|\Delta(f)|$ in *(1)* can be calculated easily using Theorem 2.6. □

Remark 3.8. Both cases of Lemma 3.7 provide generalizations of the example $v(x) := x^N + \mathcal{T}(x^2 + (N-1)x + 1)$ given in [12, Corollary 1] for the construction of infinite families of monogenic quadrinomials. For example, $f(x)$ in *(1)* of Lemma 3.7 specializes to $v(x)$ at $C = 0$.

The following theorem uses Lemma 3.1 and Lemma 3.7 to construct monogenic power-compositional Eisenstein quadrinomials.

Theorem 3.9. *Let $N, \mathcal{K}, t, C \in \mathbb{Z}$, where $N \geq 3$, $\gcd(\mathcal{K}, N) = 1$ and $\mathcal{K}$ is squarefree. With $\mathcal{T} = \mathcal{K}t$, let $f(x)$ be as given in either (1) or (2) of Lemma 3.7. Then there exist infinitely many prime values of t such that $f(x^{d^n})$ is monogenic for any $d \in \Gamma_f$ and all integers $n \geq 0$, for any $N \geq 3$ in (1), and any $N \equiv 1 \pmod 2$ in (2).*

Proof. Since the two cases are handled in a similar manner, we give details only for *(1)* of Lemma 3.7. Thinking of t as an indeterminate, let $G(t) := T_1 T_2$. We claim that there exist infinitely many primes q such that $G(q)$ is squarefree. To see this, we apply Corollary 2.12 to $G(t)$. Observe that $T_1 \neq T_2$, and that each T_i is of the form $\alpha_i t + \beta_i \in \mathbb{Z}[t]$, with $\gcd(\alpha_i, \beta_i) = 1$. We need to check for local obstructions. According to the discussion following Corollary 2.12, we only need to check the prime $\ell = 2$. An easy computer calculation reveals that either $G(1) \not\equiv 0 \pmod 4$ or $G(3) \not\equiv 0 \pmod 4$ for every one of the 48 possible combinations of $[N \pmod 4, C \pmod 4, \mathcal{K} \pmod 4]$, noting that $\mathcal{K} \not\equiv 0 \pmod 4$ since $\mathcal{K}$ is squarefree. Thus, $G(t)$ has no local obstructions, and we conclude from Corollary 2.12 that there exist infinitely many primes q such that $G(q)$ is squarefree, and the claim is verified. Then, for such a prime q with $t = q > \mathcal{K}N$, it follows that $\mathcal{K}qG(q)$ is squarefree. Thus, since $f(x)$ is Eisenstien with $|f(0)| = \Pi_f = |\mathcal{K}t|$, we deduce that $f(x)$ is monogenic by Corollary 2.7. Hence, by Lemma 3.1, we have that $f(x^{d^n})$ is monogenic for any $d \in \Gamma_f$ and all integers $n \geq 0$. □

3.3. Quintinomials

In this section, we use Theorem 2.6 with $\mathcal{T} = \mathcal{K}t$, where $\mathcal{K}, t \in \mathbb{Z}$ with $\mathcal{K}t \equiv 1 \pmod 2$, $\mathcal{K}t$ squarefree and $|\mathcal{K}t| \geq 3$. Then, a strategy similar to [12] is employed

to construct infinite collections of monogenic Eisenstein quintinomials. For an integer $N \geq 4$, suppose that $\gcd(N, \mathcal{K}) = 1$, and let

$$f(x) = x^N + \mathcal{T}u(x) = x^N + \mathcal{K}t(a_3x^3 + a_2x^2 + a_1x + a_0),$$

where $a_i \in \mathbb{Z}$ with $a_0 = 1$. Thus, $f(x)$ is Eisenstein. In the context of Theorem 2.6, we have that

$$\widehat{u}(x) = a_3(N-3)x^3 + a_2(N-2)x^2 + a_1(N-1)x + N. \tag{3.4}$$

Suppose that $\widehat{u}(x)$ factors as

$$\widehat{u}(x) = (a_3x + 1)(x + N)((N-3)x + 1). \tag{3.5}$$

Then, in Theorem 2.6, we have

$$\begin{array}{ll} A_1 = a_3, & B_1 = 1 \\ A_2 = 1, & B_2 = N \\ A_3 = N-3, & B_3 = 1, \end{array}$$

so that $|\Delta(f)| = \left|(\mathcal{K}t)^{N-1}T_1T_2T_3\right|$, where

$$\begin{aligned} T_1 &= a_3^{N-3}(a_3^3 - a_1a_3^2 + a_2a_3 - a_3)\mathcal{K}t + (-1)^N, \\ T_2 &= (1 - a_1N + a_2N^2 - a_3N^3)\mathcal{K}t + (-N)^N, \\ T_3 &= (N-3)^{N-3}\big((N-3)^3 - a_1(N-3)^2 + a_2(N-3) - a_3\big)\mathcal{K}t + (-1)^N. \end{aligned} \tag{3.6}$$

Thinking of t as an indeterminate, we define $G(t) := T_1T_2T_3$. Note that each T_i is of the form $\alpha_it + \beta_i$, where $\gcd(\alpha_i, \beta_i) = 1$. To show that there exist infinitely many primes q such that $G(q)$ is squarefree, we use Corollary 2.12. However, we must first show that $G(t)$ has no obstruction at the prime $\ell = 2$. Expanding $\widehat{u}(x)$ in (3.5) gives

$$\widehat{u}(x) = a_3(N-3)x^3 + (a_3(N^2-3N+1)+N-3)x^2 + (a_3N+N^2-3N+1)x + N. \tag{3.7}$$

Equating coefficients in (3.4) and (3.7) then yields the system of linear Diophantine equations

$$\begin{aligned} (N-1)a_1 - Na_3 &= N^2 - 3N + 1 \\ (N-2)a_2 - (N^2 - 3N + 1)a_3 &= N - 3, \end{aligned} \tag{3.8}$$

which has infinitely many solutions since

$$\gcd(N-1, N) = \gcd(N-2, N^2 - 3N + 1) = 1.$$

Using a parity argument on (3.8), we conclude that:

$$a_1 \equiv a_3 \equiv 1 \pmod 2 \quad \text{when } N \equiv 0 \pmod 2,$$

$$a_2 \equiv a_3 \equiv 1 \pmod 2 \quad \text{when } N \equiv 1 \pmod 2.$$

Upon closer inspection of (3.6), we see that if $a_2 \equiv 0 \pmod 2$ when $N \equiv 0 \pmod 2$, then $T_1 \equiv T_3 \equiv t+1 \pmod 2$ and $T_2 \equiv t \pmod 2$. Thus, $G(1) \equiv G(3) \equiv 0 \pmod 4$ so that $G(t)$ has a local obstruction at $\ell = 2$. Similarly, if $a_1 \equiv 0 \pmod 2$ when $N \equiv 1 \pmod 2$, then $G(t)$ has a local obstruction at $\ell = 2$. However, if $a_1 \equiv a_2 \equiv a_3 \equiv 1 \pmod 2$, then it is easy to verify that $G(t)$ has no local obstruction at $\ell = 2$. To isolate such solutions of (3.8), we let $a_i = 2b_i + 1$ for each $i \in \{1, 2, 3\}$ and substitute into (3.8) to get

$$\begin{aligned} (N-1)b_1 - Nb_3 &= \frac{N^2 - 3N + 2}{2} \\ (N-2)b_2 - (N^2 - 3N + 1)b_3 &= \frac{N^2 - 3N}{2}. \end{aligned} \tag{3.9}$$

Unimodular row reduction produces the following parametric solutions of (3.9):

$$\begin{aligned} b_1 &= -\left(\frac{N^4 - 7N^3 + 15N^2 - 9N + 2}{2}\right) - (N^2 - 2N)z, \\ b_2 &= -(N-2)\left(\frac{N^4 - 7N^3 + 15N^2 - 9N + 2}{2}\right) - (N^3 - 4N^2 + 4N - 1)z, \\ b_3 &= \frac{-N^4 + 8N^3 - 22N^2 + 23N - 8}{2} - (N^2 - 3N + 1)z, \end{aligned} \tag{3.10}$$

where $z \in \mathbb{Z}$. Thus, for any (a_1, a_2, a_3), where $a_i = 2b_i + 1$ and (b_1, b_2, b_3) is a solution to (3.10), it follows that there exist infinitely many primes q such that $G(q)$ is squarefree. Consequently, Corollary 2.7 implies the following theorem.

Theorem 3.10. *Let $N, \mathcal{K}, t \in \mathbb{Z}$ with $N \geq 4$, $\mathcal{K}t \equiv 1 \pmod 2$, $\mathcal{K}t$ squarefree, $|\mathcal{K}t| \geq 3$ and $\gcd(\mathcal{K}, N) = 1$. Then, for each (a_1, a_2, a_3), where $a_i = 2b_i + 1$ with (b_1, b_2, b_3) a solution to (3.10), there exist infinitely many prime values of t such that*

$$f(x) = x^N + \mathcal{K}t(a_3x^3 + a_2x^2 + a_1x + a_0)$$

is monogenic.

Then, the following corollary, which is immediate from Lemma 3.1, gives us our desired collections of quintinomials.

Corollary 3.11. *As described in Theorem 3.10, let $t = q$ be a prime such that $f(x)$ is monogenic. Then $\Pi_f = |\mathcal{K}q|$ and $f(x^{d^n})$ is monogenic for all $d \in \Gamma_f$ and integers $n \geq 0$.*

3.4. Sextinomials

In this section, we show how techniques similar to previous sections can be used to construct sextinomials with the desired properties. Let m be an integer with $m \notin \{-1, 0\}$, and let

$$N = 9m^2 + 9m + 2 = (3m+1)(3m+2),$$

so that $N \geq 20$. Let

$$f(x) = x^N + tu(x) = x^N + t(a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0) \in \mathbb{Z}[x],$$

where $|t| > 1$ is squarefree, $a_i \neq 0$ and $a_0 = 1$. Note that $f(x)$ is Eisenstein. We use Theorem 2.6 and assume that

$$\widehat{u}(x) = (a_4x + 1)(x + 3m + 1)(x + 3m + 2)((N - 4)x + 1) \tag{3.11}$$
$$= a_4(N - 4)x^4 + a_3(N - 3)x^3 + a_2(N - 2)x^2 + a_1(N - 1) + N. \tag{3.12}$$

Equating coefficients in (3.11) and (3.12) yields the linear Diophantine system

$$\begin{aligned} (C + 1)a_1 - (C + 2)a_4 &= C^2 + 6m - 1 \\ Ca_2 - (C^2 + 6m - 1)a_4 &= (6m + 3)C - 12m - 5 \\ (C - 1)a_3 - ((6m + 3)C - 12m - 5)a_4 &= C - 2, \end{aligned} \tag{3.13}$$

where $C = 9m^2 + 9m$. Straightforward gcd arguments reveal that

$$\begin{aligned} \gcd(C + 1, C + 2) &= 1 \\ \gcd(C, C^2 + 6m - 1) &= \begin{cases} 7 & \text{if } m \equiv 6 \pmod 7 \\ 1 & \text{otherwise} \end{cases} \\ \gcd(C - 1, (6m + 3)C - 12m - 5) &= 1. \end{aligned}$$

Since $(6m + 3)C - 12m - 5 \equiv 0 \pmod 7$ when $m \equiv 6 \pmod 7$, it follows that the system (3.13) has infinitely many solutions. We give the following example to illustrate how to complete the process of constructing infinite collections of Eisenstein sextinomials $f(x)$ of degree 20, such that $f(x^{d^n})$ is monogenic for all integers $n \geq 0$ and any $d \in \Gamma_f$.

Example 3.12. Let $m = -2$. Then the solutions to (3.13) are given by

$$\begin{aligned} a_1 &= 1729 + 6120z, \\ a_2 &= 28103 + 100453z, \\ a_3 &= -13685 - 48906z, \\ a_4 &= 1627 + 5814z, \end{aligned}$$

where z is any integer. Suppose that $z = -1$. Then

$$f(x) = x^{20} + t(-4187x^4 + 35221x^3 - 72350x^2 - 4391x + 1),$$

and $\Delta(f) = -t^{19}T_1T_2T_3T_4$, where

$$\begin{aligned} T_1 &= 7109t + 1099511627776, \\ T_2 &= 44954t - 95367431640625, \\ T_3 &= 191523504812730156748636 16t - 1, \end{aligned}$$

$$T_4 = st - 1,$$

with

$$s = 144908492743671980251811132224257097263134126277964322808069004613234102.$$

Let $G(t) := T_1T_2T_3T_4$. Since $G(1) \equiv 1 \pmod 4$, we see that $G(t)$ has no local obstruction at the prime $\ell = 2$. We may apply Corollary 2.12 to $G(t)$ to deduce that there exist infinitely many primes q such that $G(q)$ is squarefree, and using the same arguments as before, we conclude that $f(x)$ is monogenic when $t = q$ for each of these primes q.

4. Extending results beyond Γ_f

Up to this point, all results in this article have dealt with power-compositional Eisesntein polynomials $f(x^{d^n})$, where $d \in \Gamma_f$. What drives this situation is that the exponent d^n in this case does not contribute any new prime factors to the discriminant. Indeed, Lemma 3.1 is predicated upon this very fact. It then seems natural to ask if we can improve Lemma 3.1. That is, do there exist monogenic Eisenstein polynomials $f(x)$ such that Γ_f is a proper subset of Λ_f? In particular, can we find monogenic Eisenstein polynomials $f(x)$ such that the polynomials $f(x^{s^n})$ are monogenic for all integers $n \geq 0$ and all integers $s \in \mathcal{S}$, where $\Gamma_f \subset \mathcal{S} \subseteq \Lambda_f$? In general, this is tricky business since new prime factors p would be introduced in the discriminants $\Delta(f(x^{s^n}))$, where $f(x)$ is not p-Eisenstein. However, we are able to present some results that provide an affirmative answer to the questions posed here.

For an integer $a \geq 2$, we say a prime p is a *base-a Wieferich prime* if $a^{p-1} \equiv 1 \pmod{p^2}$. When $a = 2$, such primes are usually referred to simply as Wieferich primes. Although it is conjectured that the number of base-a Wieferich primes is infinite, the only Wieferich primes up to 6.7×10^{15} are 1093 and 3511 [5]. It is easy to show that p is a base-a Wieferich prime if and only if $a^{p^k} \equiv a \pmod{p^2}$ for any $k \geq 1$.

Our first theorem gives simple examples of binomials $f(x)$ to show that Γ_f can be a proper subset of Λ_f. Moreover, the set Λ_f is completely determined.

Theorem 4.1. *Let $a, s \in \mathbb{Z}$ with $a \geq 2$ and $s \geq 2$. Suppose that a is squarefree, and let $f(x) = x - a$. Then $f(x^{s^n})$ is monogenic for all integers $n \geq 0$ if and only if s has no prime divisors that are base-a Wieferich primes. That is, $\Lambda_f = \mathcal{S}$, where*

$$\mathcal{S} = \{s \in \mathbb{Z} : s \geq 2 \text{ and no prime divisor of } s \text{ is a base-}a \text{ Wieferich prime}\}.$$

Remark 4.2. We do not provide a proof of Theorem 4.1 for two reasons: the first reason is that it can be deduced from results in [6], and the second reason is that the methods used in the proof are similar to, but less complicated than, the methods used to establish the main result of this section (see Theorem 4.5).

We can then use Lemma 3.1 and Theorem 4.1 to construct an infinite collection of binomials with the desired power-compositional properties in the following immediate corollary, whose proof is omitted.

Corollary 4.3. *Let $f(x) = x - a \in \mathbb{Z}[x]$. Then there exist infinitely many prime values of a such that $f(x^{a^n})$ is monogenic for all integers $n \geq 0$.*

The main result of this section (Theorem 4.5) is an attempt to extend the ideas of Theorem 4.1 to monogenic trinomials of the form $f(x) = x^2 + ax + a \in \mathbb{Z}[x]$, where $a \geq 2$ is squarefree. For the sake of completeness, we begin with a basic proposition which gives a simple condition to determine when such trinomials are monogenic.

Proposition 4.4. *Let $f(x) = x^2 + ax + a \in \mathbb{Z}[x]$, with $a \geq 2$ and squarefree. Then $f(x)$ is monogenic if and only if $a - 4$ is squarefree.*

Proof. Note that $f(x)$ is irreducible since $f(x)$ is Eisenstein. Let $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. We use Theorem 2.5 with $T(x) := f(x)$, and p a prime divisor of $\Delta(f) = a(a-4)$.

Suppose first that $p \mid a$. Then $\overline{T}(x) = x^2$, and we may let $g(x) = h(x) = x$, so that

$$F(x) = \frac{g(x)h(x) - T(x)}{a} = -x - 1.$$

Hence, $\gcd(\overline{g}, \overline{F}) = 1$ and therefore, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{p}$ by Theorem 2.5.

Now suppose that $a \equiv 4 \pmod{p}$. Then

$$\overline{T}(x) = x^2 + 4x + 4 = (x+2)^2,$$

and we may let $g(x) = h(x) = x + 2$. Thus,

$$F(x) = \frac{g(x)h(x) - T(x)}{p} = \left(\frac{4-a}{p}\right)(x+1).$$

It follows that

$$\overline{F}(-2) = -\overline{\left(\frac{4-a}{p}\right)} = 0 \text{ if and only if } a \equiv 4 \pmod{p^2},$$

which completes the proof. □

Theorem 4.5. *Let $f(x) = x^2 + ax + a$ with $a \in \{2, 3\}$, and let $s \in \mathbb{Z}$ with $s \geq 2$. Then $f(x^{s^n})$ is monogenic for all integers $n \geq 0$ if and only if s has no prime divisors that are base-a Wieferich primes. That is, $\Lambda_f = \mathcal{S}$, where*

$$\mathcal{S} = \{s \in \mathbb{Z} : s \geq 2 \text{ and no prime divisor of } s \text{ is a base-}a \text{ Wieferich prime}\}.$$

Proof. For $a \in \{2, 3\}$, define

$$\mathcal{F}_n(x) := f(x^{s^n}) = x^{2s^n} + ax^{s^n} + a.$$

Thus, $\mathcal{F}_n(x)$ is irreducible, and

$$\Delta(\mathcal{F}_n) = (-1)^{s^n(2s^n-1)}a^{2s^n-1}(4-a)^{s^n}s^{2ns^n}$$

by Corollary 3.3. Let $n \in \mathbb{Z}$ with $n \geq 1$, and let $K = \mathbb{Q}(\theta)$, where $\mathcal{F}_n(\theta) = 0$. To show that $\mathcal{F}_n(x)$ is monogenic, we use Theorem 2.5 with $T(x) := \mathcal{F}_n(x)$, and q equal to a prime divisor of $\Delta(\mathcal{F}_n)$. That is, we need to examine the prime $q = a$ and the prime divisors q of s.

When $q = a$, we have that $\overline{T}(x) = x^{2s^n}$. So, we can let $g(x) = x$ and $h(x) = x^{2s^n-1}$. Thus,

$$F(x) = \frac{g(x)h(x) - T(x)}{q} = -x^{s^n} - 1,$$

so that $\overline{F}(0) = -1$. Hence, $\gcd(\overline{g}, \overline{F}) = 1$ and, therefore, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$ by Theorem 2.5.

Next, let $q = p$ be a prime divisor of s, where $p \neq a$ and $p^m \mid\mid s$ with $m \geq 1$. Let

$$\overline{\tau}(x) = x^{2s^n/p^{mn}} + \overline{a}x^{s^n/p^{mn}} + \overline{a} = \prod_{i=1}^{k} \overline{\tau_i}(x)^{e_i},$$

where the $\overline{\tau_i}(x)$ are irreducible. Then $\overline{T}(x) = \prod_{i=1}^{k} \overline{\tau_i}(x)^{p^{mn}e_i}$. Thus, we can let

$$g(x) = \prod_{i=1}^{k} \tau_i(x) \quad \text{and} \quad h(x) = \prod_{i=1}^{k} \tau_i(x)^{p^{mn}e_i-1},$$

where the $\tau_i(x)$ are monic lifts of the $\overline{\tau_i}(x)$. Note also that

$$\prod_{i=1}^{k} \tau_i(x)^{e_i} = \overline{\tau}(x) + pr(x),$$

for some $r(x) \in \mathbb{Z}[x]$. Suppose that $\overline{\tau}(\alpha) = 0$.

We treat the case $a = 2$ first. Note that $p \geq 3$. Then

$$\big(\beta - (-1 + \sqrt{-1})\big)\big(\beta - (-1 - \sqrt{-1})\big) = 0,$$

where $\beta = \alpha^{s^n/p^{mn}}$. With $\beta = -1 + \sqrt{-1}$ or $\beta = -1 - \sqrt{-1}$, straightforward induction arguments reveal that

$$\alpha^{s^n} = \beta^{p^{mn}} = 2^{(p^{mn}-1)/2}\big(\epsilon_1 + \epsilon_2\sqrt{-1}\big) \tag{4.1}$$

for some $\epsilon_i \in \{-1, 1\}$. Then, the remainder when $T(x) = \mathcal{F}_n(x)$ is divided by $x - \alpha$ is

$$\begin{aligned} T(\alpha) &= 2\Big(2^{(p^{mn}-1)/2}\epsilon_1 + 1\Big) + 2^{(p^{mn}+1)/2}\epsilon_2\Big(2^{(p^{mn}-1)/2}\epsilon_1 + 1\Big)\sqrt{-1} \\ &= 2\Big(2^{(p^{mn}-1)/2}\epsilon_1 + 1\Big)\Big(2^{(p^{mn}-1)/2}\epsilon_2\sqrt{-1} + 1\Big) \equiv 0 \pmod{p}. \end{aligned}$$

Since $pF(x) = (\overline{\tau}(x) + pr(x))^{p^{mn}} - T(x)$, it follows that

$$F(\alpha) = p^{p^{mn}-1} r(\alpha)^{p^{mn}} - \frac{T(\alpha)}{p}.$$

Hence,

$$\overline{F}(\alpha) = -\frac{T(\alpha)}{p} = -\frac{2\big(2^{(p^{mn}-1)/2}\epsilon_1 + 1\big)\big(2^{(p^{mn}-1)/2}\epsilon_2\sqrt{-1} + 1\big)}{p}.$$

If $2^{(p^{mn}-1)/2}\epsilon_2\sqrt{-1}+1 \equiv 0 \pmod{p}$, then $-2^{p^{mn}} \equiv 2 \pmod{p}$, which implies that $p = 2$, a contradiction. Consequently,

$$\begin{aligned}
[\mathbb{Z}_K : \mathbb{Z}[\theta]] \equiv 0 \pmod{p} &\iff \gcd(\overline{F}, \overline{g}) \neq 1 \\
&\iff \overline{F}(\alpha) = 0 \\
&\iff 2^{(p^{mn}-1)/2}\epsilon_1 + 1 \equiv 0 \pmod{p^2} \\
&\iff 2^{(p^{mn}-1)} \equiv 1 \pmod{p^2} \\
&\iff p \text{ is a Wieferich prime,}
\end{aligned}$$

which completes the proof when $a = 2$.

Suppose now that $a = 3$. Since $p \neq 3$, we have two possibilities: $p = 2$ and $p \geq 5$. We first handle the situation when $p = 2$. Then $\beta^3 = 1$, where $\beta = \alpha^{s^n/2^{mn}} \neq 1$. Thus,

$$\alpha^{s^n} = \beta^{2^{mn}} = \begin{cases} \beta & \text{if } 2^{mn} \equiv 1 \pmod 3 \\ \beta^2 & \text{if } 2^{mn} \equiv 2 \pmod 3). \end{cases}$$

Hence, the remainder when $T(x) = \mathcal{F}_n(x)$ is divided by $x - \alpha$ is

$$T(\alpha) = \beta^{2^{mn}+1} + 3\beta^{2^{mn}} + 3 = \begin{cases} 2\beta + 2 & \text{if } 2^{mn} \equiv 1 \pmod 3), \\ 2\beta^2 + 2 & \text{if } 2^{mn} \equiv 2 \pmod 3). \end{cases}$$

Since $2F(x) = (\overline{\tau}(x) + pr(x))^{2^{mn}} - T(x)$, it follows that

$$F(\alpha) = 2^{2^{mn}-1} r(\alpha)^{2^{mn}} - \frac{T(\alpha)}{2}.$$

Therefore,

$$\overline{F}(\alpha) = -\frac{T(\alpha)}{2} = -\begin{cases} \beta + 1 \not\equiv 0 \pmod 2 & \text{if } 2^{mn} \equiv 1 \pmod 3), \\ \beta^2 + 1 \not\equiv 0 \pmod 2 & \text{if } 2^{mn} \equiv 2 \pmod 3). \end{cases}$$

Thus, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod 2$.

We now address the situation when $p \geq 5$. In this case, we have

$$\left(\beta - \left(\frac{-3 + \sqrt{-3}}{2}\right)\right)\left(\beta - \left(\frac{-3 - \sqrt{-3}}{2}\right)\right) = 0,$$

where $\beta = \alpha^{s^n/p^{mn}}$. With $\beta = (-3+\sqrt{-3})/2$ or $\beta = (-3-\sqrt{-3})/2$, straightforward induction arguments reveal that

$$\alpha^{s^n} = \beta^{p^{mn}} = 3^{(p^{mn}-1)/2}\left(\frac{3\epsilon_1 + \epsilon_2\sqrt{-3}}{2}\right) \tag{4.2}$$

for some $\epsilon_i \in \{-1, 1\}$. Then, the remainder when $T(x) = \mathcal{F}_n(x)$ is divided by $x-\alpha$ is

$$\begin{aligned} T(\alpha) &= \frac{3^{p^{mn}} + 3^{(p^{mn}+3)/2}\epsilon_1 + 6}{2} + \left(\frac{3^{p^{mn}}\epsilon_1\epsilon_2 + 3^{(p^{mn}+1)/2}\epsilon_2}{2}\right)\sqrt{-3} \\ &= \left(\frac{3^{(p^{mn}-1)/2} + \epsilon_1}{2}\right)(A+B), \end{aligned}$$

where

$$A = 3^{(p^{mn}+1)/2} + 6\epsilon_1 \quad \text{and} \quad B = \epsilon_1\epsilon_2 3^{(p^{mn}+1)/2}\sqrt{-3}.$$

Then

$$A^2 \equiv 45 \pm 36 \pmod{p} \quad \text{and} \quad B^2 \equiv -27 \pmod{p}.$$

Hence,

$$A^2 - B^2 \pmod{p} \in \{108, 36\}. \tag{4.3}$$

If $A + B \equiv 0 \pmod{p}$, then $A^2 - B^2 \equiv 0 \pmod{p}$, and we deduce from (4.3) that $p \in \{2, 3\}$, contradicting the fact that $p \geq 5$. Consequently, $A + B \not\equiv 0 \pmod{p}$ so that

$$\overline{F}(\alpha) = -\frac{T(\alpha)}{p} = \left(\frac{3^{(p^{mn}-1)/2} + \epsilon_1}{2p}\right)(A+B) = 0$$

if and only if 3 is a base-a Wieferich prime, which completes the proof of the theorem. □

Remark 4.6. Although the precise values of ϵ_1 and ϵ_2 in (4.1) are not essential for the proof of Theorem 4.5, it can be shown for $a = 2$ and odd $N = p^{mn}$ that

$$\beta^N = 2^{(N-1)/2}(\epsilon_1 + \epsilon_2\sqrt{-1}),$$

where $\beta = -1 + \sqrt{-1}$ and

$$(\epsilon_1, \epsilon_2) = \begin{cases} (-1, 1) & \text{if } N \equiv 1 \pmod 8 \\ (1, 1) & \text{if } N \equiv 3 \pmod 8 \\ (1, -1) & \text{if } N \equiv 5 \pmod 8 \\ (-1, -1) & \text{if } N \equiv 7 \pmod 8. \end{cases}$$

A similar result holds for (ϵ_1, ϵ_2) in (4.2) when $a = 3$ and N is in the respective congruence classes 1,5,7,11 modulo 12.

At first encounter, Theorem 4.5 seems a bit curious, and it also raises some questions. For one, is it true that Λ_f can never contain any integers $s \geq 2$ with prime factors that are base-a Wieferich primes, where $f(x) = x^2 + ax + a$ with squarefree $a \geq 2$? The example $f(x) = x^2 + 7x + 7$ provides a negative answer to this question, since $p = 5$ is a base-7 Wieferich prime but $f(x^{5^n})$ is monogenic for all integers $n \geq 0$.

A second related question that arises is whether Λ_f must contain all primes that are not base-a Wieferich primes. The example $f(x) = x^2 + 7x + 7$ also provides a negative answer to this question since 37 is not a base-7 Wieferich prime, but $f(x^{37})$ is not monogenic.

A third question then is why is it that Theorem 4.5 cannot be extended to $a = 7$? When $a \in \{2, 3\}$, the elements $\beta^{p^{mn}}$ are well-behaved and well-understood, where $f(\beta) = 0$. This stability and clarity seem to disappear when $a \geq 5$. Could it be a result of the loss of a one-to-one correspondence between the set of possibilities for (e_1, e_2) and the congruence classes of $(\mathbb{Z}/4a\mathbb{Z})^*$? That is, we have that $\phi(4a) = 4$ if and only if $a \in \{2, 3\}$. Or could it simply be explained by the fact that $\beta \notin \mathbb{R}$ when $a \in \{2, 3\}$ and $\beta \in \mathbb{R}$ when $a \geq 5$?

A final question is how large can Λ_f be for monogenic $f(x) = x^2 + ax + a$, where $a \geq 2$ is squarefree. In particular, could Λ_f equal the set of all positive integers larger than one? We do not know the answer to this question, but we suspect the answer is negative.

One avenue of future research is to establish results for monogenic trinomials $f(x) = x^2 + ax + a$, with squarefree $a \geq 2$, that are analogous to Theorem 4.1 and Corollary 4.3. In other words, can we explicitly determine Λ_f for these trinomials in terms of conditions on a? And then, can we use this information to construct infinite collections of such trinomials $f(x)$ for which $f(x^{s^n})$ is monogenic for all integers $n \geq 0$ and $s \in \mathcal{S} \subseteq \Lambda_f$, where $\Gamma_f \subset \mathcal{S}$?

Acknowledgements. The author thanks the referee for the careful reading of the manuscript.

References

[1] H. Cohen: *A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics, 138*, Berlin: Springer-Verlag, 1993.

[2] K. Conrad, url: www.math.uconn.edu/~kconrad/blurbs/gradnumthy/totram.pdf.

[3] J. Cullinan, url: https://studylib.net/doc/8187082/the-discriminant-of-a-composition-of-two.

[4] J. B. Dence, T. P. Dence: *Elements of the Theory of Numbers*, San Diego, CA: Harcourt/Academic Press, 1999.

[5] F. G. Dorais, D. Klyve: *A Wieferich prime search up to* 6.7×10^{15}, J. Integer Seq. 14.9, Article 11.9.2 (2011).

[6] T. A. Gassert: *A note on the monogeneity of power maps*, Albanian J. Math. 11.1 (2017), pp. 3–12.

[7] J. Harrington, L. Jones: *Monogenic cyclotomic compositions*, Kodai Math. J. 44.1 (2021), pp. 115–125, doi: https://doi.org/10.11650/tjm/200201.

[8] J. Harrington, L. Jones: *The irreducibility and monogenicity of power-compositional trinomials*, arXiv:2204.07784v1.

[9] H. A. Helfgott: *Square-free values of $f(p)$, f cubic*, Acta Math. 213.1 (2014), pp. 107–135, doi: https://doi.org/10.1007/s11511-014-0117-2.

[10] C. Hooley: *Applications of sieve methods to the theory of numbers. Cambridge Tracts in Mathematics, No. 70*, Cambridge-New York-Melbourne: Cambridge University Press, 1976.

[11] A. Jakhar, S. K. Khanduja, N. Sangwan: *Characterization of primes dividing the index of a trinomial*, Int. J. Number Theory 13.10 (2017), pp. 2505–2514, doi: https://doi.org/10.1142/s1793042117501391.

[12] L. Jones: *Generating infinite families of monogenic polynomials using a new discriminant formula*, Albanian J. Math. 14.1 (2020), pp. 37–45, doi: https://doi.org/10.51286/albjm/1608313765.

[13] L. Jones: *Infinite families of reciprocal monogenic polynomials and their Galois groups*, New York J. Math. 27 (2021), pp. 1465–1493.

[14] J. Neukirch: *Algebraic Number Theory*, Berlin: Springer-Verlag, 1999.

[15] H. Pasten: *The ABC conjecture, arithmetic progressions of primes and squarefree values of polynomials at prime arguments*, Int. J. Number Theory 13.7 (2017), pp. 1881–1894, doi: https://doi.org/10.1142/s1793042115500396.

[16] R. G. Swan: *Factorization of polynomials over finite fields*, Pacific J. Math. 12.7 (1962), pp. 1099–1106.