Math. J. Okayama Univ. **67** (2025), 53–65

THE IRREDUCIBILITY AND MONOGENICITY OF POWER-COMPOSITIONAL TRINOMIALS

Joshua Harrington and Lenny Jones

Abstract. A polynomial $f(x) \in \mathbb{Z}[x]$ of degree N is called *monogenic* if $f(x)$ is irreducible over $\mathbb{Q}$ and $\{1, \theta, \theta^2, \ldots, \theta^{N-1}\}$ is a basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta) = 0$. Define $\mathcal{F}(x) := x^m + Ax^{m-1} + B$. In this article, we determine sets of conditions on m, A, and B, such that the power-compositional trinomial $\mathcal{F}(x^{p^n})$ is monogenic for all integers $n \geq 0$ and a given prime p. Furthermore, we prove the actual existence of infinite families of such trinomials $\mathcal{F}(x)$.

1. Introduction

Unless stated otherwise, when we say that $f(x)$ is "irreducible", we mean irreducible over $\mathbb{Q}$. We let $\Delta(f(x))$, or simply $\Delta(f)$, and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of $f(x)$ and a number field K. If $f(x)$ is irreducible, with $f(\theta) = 0$ and $K = \mathbb{Q}(\theta)$, then [3]

$$\Delta(f) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \, \Delta(K), \tag{1.1}$$

where $\mathbb{Z}_K$ is the ring of integers of K. We define $f(x)$ to be *monogenic* if $f(x)$ is irreducible and $\mathbb{Z}_K = \mathbb{Z}[\theta]$, or equivalently from (1.1), that $\Delta(f) = \Delta(K)$. When $f(x)$ is monogenic, $\{1, \theta, \theta^2, \ldots, \theta^{\deg(f)-1}\}$ is a basis for $\mathbb{Z}_K$, commonly referred to as a *power basis*. The existence of a power basis facilitates computations in $\mathbb{Z}_K$, as in the case of the cyclotomic polynomials $\Phi_n(x)$ [26]. We see from (1.1) 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.

In this article, our focus is on trinomials of the form

$$\mathcal{F}(x) := \mathcal{F}_{m,A,B}(x) = x^m + Ax^{m-1} + B \in \mathbb{Z}[x]. \tag{1.2}$$

We determine sets of conditions on m, A and B so that the power-compositional trinomial $\mathcal{F}(x^{p^n})$ is monogenic (and hence irreducible) for all integers $n \geq 0$ and a given prime p. We then prove the actual existence of infinite families of such trinomials. Although much research has been conducted concerning the irreducibility and monogenicity of trinomials [2, 4, 7, 11–14, 16, 17, 20, 21, 23, 24], the approaches presented in this article are novel, and they allow us to construct new infinite families of monogenic trinomials in a manner unlike any methods previously used. Our main results are as follows.

Mathematics Subject Classification. Primary 11R04; Secondary 11R09, 12F05.

Key words and phrases. irreducible, monogenic, power-compositional, trinomial.

Theorem 1.1. *Let $\mathcal{F}(x)$ be as defined in* (1.2)*, and let $p \geq 3$ be a prime. Define*

$$\mathcal{D} := m^m B - (-1)^m (m-1)^{m-1} A^m. \tag{1.3}$$

(1) When $m = 2$, let $A = 4pu + p^2 + 2$ and $B = 2pt + 1$, where $u, t \in \mathbb{Z}$ are such that B, $B - 1$ and $\mathcal{D}$ are squarefree.
(2) When $m \in \{3, 4\}$, let $A = 4p^2u + 1$ and $B = 2pt + p$, where $u, t \in \mathbb{Z}$ are such that B and $\mathcal{D}$ are squarefree.
(3) When $m \geq 5$, let $A = 4p^2u + 1$ and $B = 2pt + p$, where $u, t \in \mathbb{Z}$ are such that B and $\mathcal{D}$ are squarefree; and assume that $\mathcal{F}(x)$ is irreducible.

Then, in any case above, $\mathcal{F}(x^{p^n})$ is monogenic for all $n \geq 0$.

Corollary 1.2. *Let $\mathcal{F}(x)$ be as defined in* (1.2)*, let $p \geq 3$ be a prime, and let $u \in \mathbb{Z}$. Let $\mathcal{D}$ be as defined in* (1.3)*. Then, in any case of Theorem 1.1, there exist infinitely many prime values of t such that $\mathcal{F}(x^{p^n})$ is monogenic for all $n \geq 0$.*

Remark 1. Note that in any case of Theorem 1.1, we have that $|B| \geq 2$.

2. Preliminaries

The formula for the discriminant of an arbitrary monic trinomial, due to Swan [25, Theorem 2], is given in the following theorem.

Theorem 2.1. *Let $f(x) = x^n + Ax^m + B \in \mathbb{Q}[x]$, where $0 < m < n$, and let $d = \gcd(n, m)$. Then $\Delta(f) =$*

$$(-1)^{n(n-1)/2} B^{m-1} \left(n^{n/d} B^{(n-m)/d} - (-1)^{n/d} (n-m)^{(n-m)/d} m^{m/d} A^{n/d} \right)^d.$$

The following immediate corollary of Theorem 2.1 is of pertinence to us here.

Corollary 2.2. *Let $\mathcal{F}(x)$ be as defined in* (1.2)*, and let p be a prime. Then, for any integer $n \geq 0$, we have*

$$\Delta(\mathcal{F}(x^{p^n})) = (-1)^{mp^n(mp^n-1)/2} B^{(m-1)p^n - 1} p^{mnp^n} \mathcal{D}^{p^n}, \tag{2.1}$$

where $\mathcal{D}$ is as defined in (1.3)*.*

The next two theorems are due to Capelli [22].

Theorem 2.3. [22, Theorem 22] *Let $f(x)$ and $h(x)$ be polynomials in $\mathbb{Q}[x]$ with $f(x)$ irreducible. Suppose that $f(\alpha) = 0$. Then $f(h(x))$ is reducible over $\mathbb{Q}$ if and only if $h(x) - \alpha$ is reducible over $\mathbb{Q}(\alpha)$.*

Theorem 2.4. [22, Theorem 19] *Let $c \in \mathbb{Z}$ with $c \geq 2$, and let $\alpha \in \mathbb{C}$ be algebraic. Then $x^c - \alpha$ is reducible over $\mathbb{Q}(\alpha)$ if and only if either there is a prime p dividing c such that $\alpha = \beta^p$ for some $\beta \in \mathbb{Q}(\alpha)$ or $4 \mid c$ and $\alpha = -4\beta^4$ for some $\beta \in \mathbb{Q}(\alpha)$.*

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 monogenicity of a polynomial.

Theorem 2.5 (Dedekind [3])**.** *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 next result is essentially a "streamlined" version of Dedekind's index criterion for trinomials.

Theorem 2.6. [10] *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 $\gcd(M, N) = d_0$, $M = M_1 d_0$ and $N = N_1 d_0$. A prime factor q of $\Delta(f)$ does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if all of the following statements are true:*

(1) *if $q \mid A$ and $q \mid B$, then $q^2 \nmid B$;*
(2) *if $q \mid A$ and $q \nmid B$, then*

either $q \mid A_2$ *and* $q \nmid B_1$ *or* $q \nmid A_2 \left((-B)^{M_1} A_2^{N_1} - (-B_1)^{N_1}\right)$,

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

(3) *if* $q \nmid A$ *and* $q \mid B$, *then*

$$\text{either} \quad q \mid A_1 \text{ and } q \nmid B_2 \quad \text{or} \quad q \nmid A_1 B_2^{M-1} \left((-A)^{M_1} A_1^{N_1 - M_1} - (-B_2)^{N_1 - M_1} \right),$$

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

(4) *if* $q \nmid AB$ *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) *if* $q \nmid ABM$, *then*

$$q^2 \nmid \left(B^{N_1 - M_1} N_1^{N_1} - (-1)^{M_1} A^{N_1} M_1^{M_1} (M_1 - N_1)^{N_1 - M_1} \right).$$

Remark 2. We will find both Theorem 2.5 and Theorem 2.6 useful in our investigations.

The next theorem follows from Corollary (2.10) in [18].

Theorem 2.7. *Let* K *and* L *be number fields with* $K \subset L$. *Then*

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

Theorem 2.8. *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,

$$N_G(X) \sim C_G \frac{X}{\log(X)}, \tag{2.2}$$

where

$$C_G = \prod_{\ell \text{ prime}} \left(1 - \frac{\rho_G(\ell^2)}{\ell(\ell - 1)} \right) \tag{2.3}$$

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

Remark 3. Theorem 2.8 follows from work of Helfgott, Hooley and Pasten [8, 9, 19]. For more details, see the discussion following [14, Theorem 2.11].

Definition 1. In the context of Theorem 2.8, for $G(t) \in \mathbb{Z}[t]$ and a prime ℓ, if $G(z) \equiv 0 \pmod{\ell^2}$ for all $z \in (\mathbb{Z}/\ell^2\mathbb{Z})^*$, we say that $G(t)$ has a *local obstruction* at ℓ. A polynomial $G(t) \in \mathbb{Z}[t]$ is said to have *no local obstructions*, if for every prime ℓ there exists some $z \in (\mathbb{Z}/\ell^2\mathbb{Z})^*$ such that $G(z) \not\equiv 0 \pmod{\ell^2}$.

Note that $C_G > 0$ in (2.3) if and only if $G(t)$ has no local obstructions. Consequently, it follows that $N_G(X) \to \infty$ as $X \to \infty$ in (2.2), when $G(t)$ has no local obstructions. Hence, we have the following immediate corollary of Theorem 2.8 which is used to establish Corollary 1.2.

Corollary 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. To avoid the situation when $C_G = 0$, we suppose further that $G(t)$ has no local obstructions. Then there exist infinitely many primes ρ such that $G(\rho)$ is squarefree.*

We make the following observation concerning $G(t)$ from Corollary 2.9 in the special case when each of the distinct irreducible factors of $G(t)$ is of the form $a_i t + b_i$ with $\gcd(a_i, b_i) = 1$. 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

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

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 [5, 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 $\ell \le (k+2)/2$.

3. The Proof of Theorem 1.1

Before we begin the proof of Theorem 1.1, we require the following.

Lemma 3.1. *Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible, and let p be a prime. If $|f(0)| \ge 2$ and $f(0)$ is squarefree, then $f(x^{p^n})$ is irreducible for all $n \ge 0$.*

Proof. Suppose that $f(\alpha) = 0$. Let $n \ge 1$ and assume, by way of contradiction, that $f(g(x))$ is reducible, where $g(x) = x^{p^n}$. If $p \ge 3$, we deduce from Theorems 2.3 and 2.4 that $\alpha = \beta^p$ for some $\beta \in \mathbb{Q}(\alpha)$. Then, by taking the norm $\mathcal{N} := \mathcal{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}$, we have that

$$\mathcal{N}(\beta)^p = \mathcal{N}(\alpha) = (-1)^{\deg(f)} f(0),$$

which contradicts the fact that $f(0)$ is squarefree since $\mathcal{N}(\beta) \in \mathbb{Z}$ and $|f(0)| \geq 2$. The argument is similar when $p = 2$, and we omit the details. □

Note that the conditions in part (3) of Theorem 1.1 contain the assumption that $\mathcal{F}(x)$ is irreducible. Under this assumption, we obtain the following immediate corollary of Lemma 3.1.

Corollary 3.2. *Let $m \in \mathbb{Z}$ with $m \geq 3$ and let p be a prime with $p \geq 3$. Let $\mathcal{F}(x)$ be as defined in* (1.2)*, and let $\mathcal{D}$ be as defined in* (1.3)*. Suppose that $A = 4p^2u + 1$ and $B = 2pt + p$, where $u, t \in \mathbb{Z}$ are such that B and $\mathcal{D}$ are squarefree. If $\mathcal{F}(x)$ is irreducible, then $\mathcal{F}(x^{p^n})$ is irreducible for all $n \geq 0$.*

Computer evidence suggests the following, which, if true, implies the conclusion of Corollary 3.2 by Lemma 3.1, since $|B| > 2$ in Corollary 3.2.

Conjecture 3.3. *Let $m \geq 3$, and let $\mathcal{F}(x)$ be as defined in* (1.2)*. If $A \equiv 1 \pmod 4$ and $B \equiv 1 \pmod 2$, with B squarefree and $|B| > 2$, then $\mathcal{F}(x)$ is irreducible.*

The next lemma is similar in nature to Lemma 3.1 in [15]. We let $\mathcal{T}$ be the set of the 12 possible ordered pairs (a, b), where $0 \leq a \leq 3$ and $1 \leq b \leq 3$, corresponding respectively to the possible congruence classes modulo 4 of A and B (excluding $b = 0$ since B is squarefree). For any integer z, we let $\widehat{z} \in \{0, 1, 2, 3\}$ be the reduction of z modulo 4.

Lemma 3.4. *Let $\mathcal{F}(x)$ be as defined in* (1.2) *with $m \in \{2, 3, 4\}$, and let p be a prime. Suppose that B is squarefree with $|B| \geq 2$. Then $\mathcal{F}(x^{p^n})$ is irreducible for all $n \geq 0$ if $(\widehat{A}, \widehat{B}) \in \Gamma_m$, where*

$$\Gamma_m = \begin{cases} \{(0,1),(0,2),(1,1),(1,3),(2,2),(2,3),(3,1),(3,3)\} & \text{if } m \in \{2,4\} \\ \{(0,2),(1,1),(1,3),(2,2),(3,1),(3,3)\} & \text{if } m = 3. \end{cases}$$

Moreover, for each $m \in \{2, 3, 4\}$, and each $(a, b) \in \mathcal{T} \setminus \Gamma_m$, there exist integers A and B with $(\widehat{A}, \widehat{B}) = (a, b)$ such that $\mathcal{F}(x^{p^n})$ is reducible for all $n \geq 0$.

Proof. We begin by showing, for each $m \in \{2, 3, 4\}$ and each $(\widehat{A}, \widehat{B}) \in \Gamma_m$, that $\mathcal{F}(x)$ is irreducible. It is easy to check that $\mathcal{F}(x)$ has no zeros modulo 4, which verifies that $\mathcal{F}(x)$ is irreducible when $m \in \{2, 3\}$. When $m = 4$, we also need to show that $\mathcal{F}(x)$ cannot be written as the product of two irreducible quadratics. Suppose then that

$$\mathcal{F}(x) = x^4 + Ax^3 + B = (x^2 + c_1x + c_0)(x^2 + d_1x + d_0),$$

for some $c_i, d_i \in \mathbb{Z}$. Expanding this factorization and equating coefficients yields the system of equations:

$$\begin{aligned} \text{constant term}: &\quad c_0 d_0 = B \\ x: &\quad c_0 d_1 + c_1 d_0 = 0 \\ x^2: &\quad c_0 + d_0 + c_1 d_1 = 0 \\ x^3: &\quad c_1 + d_1 = A. \end{aligned} \tag{3.1}$$

It turns out that for each $(\widehat{A}, \widehat{B}) \in \Gamma_4$, the system (3.1) is impossible modulo 4. For example, if $(\widehat{A}, \widehat{B}) = (3, 1)$, then

$$\text{either} \quad c_0 \equiv d_0 \equiv 1 \pmod 4 \quad \text{or} \quad c_0 \equiv d_0 \equiv 3 \pmod 4.$$

In either of these cases, we see in (3.1) that the congruence corresponding to the coefficient on x contradicts the congruence corresponding to the coefficient on x^3. Similar contradictions are easily seen to occur for each $(\widehat{A}, \widehat{B}) \in \Gamma_4$, and we omit the details. It follows that $\mathcal{F}(x^{p^n})$ is irreducible for all $n \geq 0$ by Lemma 3.1.

To complete the proof, for each $m \in \{2, 3, 4\}$ we give, respectively, in Tables 1, 2 and 3, an example of each $(\widehat{A}, \widehat{B}) \in \mathcal{T} \setminus \Gamma_m$ such that $\mathcal{F}(x^{p^n})$ is reducible for all $n \geq 0$. We also give the factorization of $\mathcal{F}(x^{p^n})$. □

$(\widehat{A}, \widehat{B}) \in \mathcal{T} \setminus \Gamma_2$	(A, B)	Factorization of $\mathcal{F}(x^{p^n})$
$(0, 3)$	$(4, 3)$	$(x^{p^n} + 1)(x^{p^n} + 3)$
$(1, 2)$	$(5, 6)$	$(x^{p^n} + 2)(x^{p^n} + 3)$
$(2, 1)$	$(2, 1)$	$(x^{p^n} + 1)^2$
$(3, 2)$	$(3, 2)$	$(x^{p^n} + 1)(x^{p^n} + 2)$

TABLE 1. Examples for $(\widehat{A}, \widehat{B}) \in \mathcal{T} \setminus \Gamma_2$ and their factorizations

Computer evidence suggests the following extension of Lemma 3.4.

Conjecture 3.5. *Let $\mathcal{F}(x)$ be as defined in (1.2), and let p be a prime. Suppose that B is squarefree with $|B| \geq 2$. Then $\mathcal{F}(x^{p^n})$ is irreducible for all $n \geq 0$ if $(\widehat{A}, \widehat{B}) \in \Gamma_m$, where*

$$\Gamma_m = \begin{cases} \{(0,1), (0,2), (1,1), (1,3), \\ \qquad (2,2), (2,3), (3,1), (3,3)\} & \text{if } m \equiv 0 \pmod 2 \\ \{(0,2), (1,1), (1,3), (2,2), (3,1), (3,3)\} & \text{if } m \equiv 1 \pmod 2. \end{cases}$$

Remark 4. Note that the truth of Conjecture 3.5 also implies the conclusion of Corollary 3.2.

$(\widehat{A}, \widehat{B}) \in \mathcal{T} \setminus \Gamma_3$	(A, B)	Factorization of $\mathcal{F}(x^{p^n})$
$(0, 1)$	$(-4, 5)$	$(x^{p^n}+1)(x^{2p^n}-5x^{p^n}+5)$
$(0, 3)$	$(-4, 3)$	$(x^{p^n}-1)(x^{2p^n}-3x^{p^n}-3)$
$(1, 2)$	$(-3, 2)$	$(x^{p^n}-1)(x^{2p^n}-2x^{p^n}-2)$
$(2, 1)$	$(-2, 1)$	$(x^{p^n}-1)(x^{2p^n}-x^{p^n}-1)$
$(2, 3)$	$(-2, 3)$	$(x^{p^n}+1)(x^{2p^n}-3x^{p^n}+3)$
$(3, 2)$	$(-1, 2)$	$(x^{p^n}+1)(x^{2p^n}-2x^{p^n}+2)$

TABLE 2. Examples for $(\widehat{A}, \widehat{B}) \in \mathcal{T} \setminus \Gamma_3$ and their factorizations

$(\widehat{A}, \widehat{B}) \in \mathcal{T} \setminus \Gamma_4$	(A, B)	Factorization of $\mathcal{F}(x^{p^n})$
$(0, 3)$	$(4, 3)$	$(x^{p^n}+1)(x^{3p^n}+3x^{2p^n}-3x^{p^n}+3)$
$(1, 2)$	$(-3, 2)$	$(x^{p^n}-1)(x^{3p^n}-2x^{2p^n}-2x^{p^n}-2)$
$(2, 1)$	$(2, 1)$	$(x^{p^n}+1)(x^{3p^n}+x^{2p^n}-x^{p^n}+1)$
$(3, 2)$	$(3, 2)$	$(x^{p^n}+1)(x^{3p^n}+2x^{2p^n}-2x^{p^n}+2)$

TABLE 3. Examples for $(\widehat{A}, \widehat{B}) \in \mathcal{T} \setminus \Gamma_4$ and their factorizations

Lemma 3.6. *Let $\mathcal{F}(x)$ be as defined in* (1.2)*. Suppose that B is squarefree with $|B| \geq 2$, and that $\mathcal{D}$, as defined in* (1.3)*, is squarefree. If $\mathcal{F}(x)$ is irreducible, then $\mathcal{F}(x)$ is monogenic.*

Proof. We have by Corollary 2.2 that

$$\begin{aligned}\Delta(\mathcal{F}(x)) &= (-1)^{m(m-1)/2}B^{m-2}\left(m^m B - (-1)^m(m-1)^{m-1}A^m\right)\\ &= (-1)^{m(m-1)/2}B^{m-2}\mathcal{D}.\end{aligned}$$

Let $K = \mathbb{Q}(\theta)$, where $\mathcal{F}(\theta) = \theta^m + A\theta^{m-1} + B = 0$, and let $\mathbb{Z}_K$ denote the ring of integers of K. We check that all statements in Theorem 2.6 are true with $N := m$ and $M := m-1$, and all primes q dividing $\Delta(\mathcal{F}(x))$. Note that statements (1) and (5) are always true for any value of q since, respectively, B and $\mathcal{D}$ are squarefree.

Suppose first that $q \mid B$. We see immediately that statements (2) and (4) are trivially true. For statement (3), we have $\ell = 0$ so that $A_1 = 0$. Hence, $q \mid A_1$, and $q \nmid B_2$ since B is squarefree. Thus, statement (3) is true and $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$.

Suppose now that q is a prime such that $q \mid \mathcal{D}$. Observe that if $q \mid A$ and $q \nmid B$, then $q \mid m$, which contradicts the fact that $\mathcal{D}$ is squarefree. Hence, statement (2) is trivially true. If $q \nmid A$ and $q \mid B$, then $\ell = 0$ so

that $A_1 = 0$. Hence, $q \mid A_1$, and $q \nmid B_2$ since B is squarefree. Therefore, statement (3) is true. Suppose next that $q \nmid AB$ and $q \mid (m-1)$. Then $q \mid m$ since $q \mid \mathcal{D}$, which is impossible, and so statement (4) is trivially true. Thus, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$, and consequently, $\mathcal{F}(x)$ is monogenic, which completes the proof of the lemma. □

While Lemma 3.6 is new and of some interest in its own right, we note that in light of Remark 1, Lemma 3.6 can be applied to $\mathcal{F}(x)$, and is crucial to establish the monogenicity of $\mathcal{F}(x)$ for the base case of the induction argument in the proof of Theorem 1.1.

Proof of Theorem 1.1. For part (1), we see that

$$(\widehat{A}, \widehat{B}) \in \{(3,1),(3,3)\} \subset \Gamma_2.$$

Thus, $\mathcal{F}(x^{p^n})$ is irreducible for all $n \geq 0$ by Lemma 3.4, and $\mathcal{F}(x)$ is monogenic by Lemma 3.6. By Corollary 2.2, we have that

$$\Delta(\mathcal{F}(x^{p^n})) = (-1)^{p^n(2p^n-1)} B^{p^n-1} p^{2np^n} \mathcal{D}^{p^n}, \tag{3.2}$$

where $\mathcal{D} = 4B - A^2$. Define

$$\theta_n := \theta^{1/p^n} \quad \text{and} \quad K_n := \mathbb{Q}(\theta_n) \quad \text{for } n \geq 0,$$

noting that $\theta_0 = \theta$ and $K_0 = K$ from the proof of Lemma 3.6. Furthermore, observe that $\mathcal{F}((\theta_n)^{p^n}) = 0$ and $[K_{n+1} : K_n] = p$ for all $n \geq 0$. We assume that $\mathcal{F}(x^{p^n})$ is monogenic and proceed by induction on n. Then $\Delta\left(\mathcal{F}(x^{p^n})\right) = \Delta(K_n)$, and we deduce from Theorem 2.7 that

$$\Delta\left(\mathcal{F}(x^{p^n})\right)^p \mid \Delta(K_{n+1}).$$

By (3.2), we have that

$$\Delta(\mathcal{F}(x^{p^{n+1}}))/\Delta(\mathcal{F}(x^{p^n}))^p = B^{p-1} p^{2p^{n+1}}.$$

Hence, to show that $\mathcal{F}(x^{p^{n+1}})$ is monogenic, we only have to show that

$$\left[\mathbb{Z}_{K_{n+1}} : \mathbb{Z}[\theta_{n+1}]\right] \not\equiv 0 \pmod{q} \tag{3.3}$$

for all primes q dividing Bp. We check that all statements in Theorem 2.6 are true for such primes, when applied to $\mathcal{F}(x^{p^{n+1}}) = x^{2p^{n+1}} + Ax^{p^{n+1}} + B$.

Suppose first that $q = p$. We use Theorem 2.5 with $T(x) := \mathcal{F}(x^{p^{n+1}})$. Since $A \equiv 2 \pmod{p}$ and $B \equiv 1 \pmod{p}$, we get that $\overline{T}(x) = (x+1)^{2p^{n+1}}$. Thus, we can let $g(x) = x + 1$ and $h(x) = (x+1)^{2p^{n+1}-1}$, so that

$$\begin{aligned} F(x) &= \frac{g(x)h(x) - T(x)}{p} \\ &= \frac{(x+1)^{2p^{n+1}} - x^{2p^{n+1}} - Ax^{p^{n+1}} - B}{p} \end{aligned}$$

$$= \sum_{\substack{j=1 \\ j\neq p^{n+1}}}^{2p^{n+1}-1} \frac{\binom{2p^{n+1}}{j}}{p} x^j + \frac{\binom{2p^{n+1}}{p^{n+1}} - A}{p} x^{p^{n+1}} + \frac{1-B}{p}. \tag{3.4}$$

To show that $\gcd(\overline{g}, \overline{F}) = 1$, it is enough to show that $F(-1) \not\equiv 0 \pmod{p}$. Since

$$\sum_{\substack{j=1 \\ j\neq p^{n+1}}}^{2p^{n+1}-1} \binom{2p^{n+1}}{j} x^j = (x+1)^{2p^{n+1}} - x^{2p^{n+1}} - 1 - \binom{2p^{n+1}}{p^{n+1}} x^{p^{n+1}},$$

it follows that

$$\sum_{\substack{j=1 \\ j\neq p^{n+1}}}^{2p^{n+1}-1} \binom{2p^{n+1}}{j} (-1)^j = -2 + \binom{2p^{n+1}}{p^{n+1}} \equiv 0 \pmod{p^2} \quad [1,6].$$

Hence, since $A \equiv 2 \pmod{p}$ and $B-1$ is squarefree, we see from (3.4) that

$$F(-1) \equiv \frac{\overline{1-B}}{p} \not\equiv 0 \pmod{p}.$$

Thus, we conclude from Theorem 2.5 that (3.3) is true for $q = p$.

Suppose next that $q \mid B$. Note that $q \neq p$. Here we use Theorem 2.6, and we want to show that all statements are true for $\mathcal{F}(x^{p^{n+1}})$ with $N = 2p^{n+1}$ and $M = p^{n+1}$. Statement (1) is true since B is squarefree. We see that statements (2), (4) and (5) are trivially true. For statement (3), we have that $\ell = 0$, since $q \neq p$ and $N - M = p^{n+1}$, and hence, $A_1 = 0$. Thus, $q \mid A_1$ and $q \mid B_2$ since B is squarefree. Therefore, (3.3) is true. Consequently, $\mathcal{F}(x^{p^n})$ is monogenic for all $n \geq 0$ by induction.

For parts (2) and (3), we give details only for the case $m = 3$ since the other cases are handled in an identical manner. In particular, for part (3) (cases of $m \geq 5$), we use Corollary 3.2 and proceed as in the case of $m = 3$.

For the case of $m = 3$, we see that

$$(\widehat{A}, \widehat{B}) \in \{(1,1), (1,3)\} \subset \Gamma_3.$$

Thus, $\mathcal{F}(x^{p^n})$ is irreducible for all $n \geq 0$ by Lemma 3.4, and $\mathcal{F}(x)$ is monogenic by Lemma 3.6. By Corollary 2.2, we have that

$$\Delta(\mathcal{F}(x^{p^n})) = (-1)^{3p^n(3p^n-1)/2} B^{2p^n-1} p^{3np^n} \mathcal{D}^{p^n}, \tag{3.5}$$

where $\mathcal{D} = 27B + 4A^3$. Using (3.5) and Theorem 2.7 for

$$\mathcal{F}(x^{p^{n+1}}) = x^{3p^{n+1}} + Ax^{2p^{n+1}} + B,$$

and arguing as in part (1) with θ_n and K_n defined accordingly, we deduce that we only have to check primes dividing B, since $B \equiv 0 \pmod{p}$ in this case.

Suppose first that $q = p$. We use Theorem 2.5 with $T(x) := \mathcal{F}(x^{p^{n+1}})$. Since $A \equiv 1 \pmod{p}$ and $B \equiv 0 \pmod{p}$, we get that

$$\overline{T}(x) = x^{2p^{n+1}}(x+1)^{p^{n+1}}.$$

Thus, we may let $g(x) = x(x+1)$ and $h(x) = x^{2p^{n+1}-1}(x+1)^{p^{n+1}-1}$, so that

$$\begin{aligned} F(x) &= \frac{g(x)h(x) - T(x)}{p} \\ &= \frac{x^{2p^{n+1}}(x+1)^{p^{n+1}} - x^{3p^{n+1}} - Ax^{2p^{n+1}} - B}{p} \\ &= \sum_{j=1}^{p^{n+1}-1} \frac{\binom{p^{n+1}}{j}}{p} x^{j+2p^{n+1}} + \left(\frac{1-A}{p}\right) x^{2p^{n+1}} - \frac{B}{p}. \end{aligned} \tag{3.6}$$

To show that $\gcd(\overline{g}, \overline{F}) = 1$, it is enough to show that $F(c) \not\equiv 0 \pmod{p}$, where $c \in \{-1, 0\}$. Note first that since $A \equiv 1 \pmod{p^2}$, the middle term in (3.6) disappears in $\overline{F}$. Observe next that the sum in (3.6) is zero when $x = -1$. Hence,

$$F(c) \equiv -\frac{\overline{B}}{p} \not\equiv 0 \pmod{p},$$

since B is squarefree. Thus, we deduce from Theorem 2.5 that (3.3) is true for $q = p$.

Suppose next that $q \mid B$ with $q \neq p$. Here we use Theorem 2.6, and we want to show that all statements are true for $\mathcal{F}(x^{p^{n+1}})$ with $N = 3p^{n+1}$ and $M = 2p^{n+1}$. Statement (1) is true since B is squarefree. We see that statements (2), (4) and (5) are trivially true. For statement (3), we have that $\ell = 0$, since $q \neq p$ and $N - M = p^{n+1}$, and hence, $A_1 = 0$. Thus, $q \mid A_1$ and $q \mid B_2$ since B is squarefree. Therefore, (3.3) is true. Consequently, $\mathcal{F}(x^{p^n})$ is monogenic for all $n \geq 0$ by induction. □

4. Proof of Corollary 1.2

Proof. For all cases of m in Theorem 1.1, we define $G(t) := B\mathcal{D}$. We wish to apply Corollary 2.9, and so we must check for local obstructions. In light of the discussion following Corollary 2.9, since B and $\mathcal{D}$ are both linear in t, we only have to check for a local obstruction at the prime $\ell = 2$.

Specifically, for part (1) of Theorem 1.1 (when $m = 2$), we get that

$$G(t) = p(2pt+1)(8t - 16pu^2 - 8p^2u - 16u - 4p - p^3).$$

Since $G(1) \equiv 1 \pmod 4$, there is no local obstruction at $\ell = 2$. Thus, by Corollary 2.9, there exist infinitely many primes ρ such that $G(\rho)$ is squarefree. Therefore, we see that $|B| \geq 2$, and both B and $\mathcal{D}$, individually, are squarefree for such primes ρ. Note also that $B - 1 = 2pt$ is squarefree when $t = \rho > p$. Consequently, for each $t = \rho > p$, $\mathcal{F}(x^{p^n})$ is monogenic for all integers $n \geq 0$ by Theorem 1.1.

When $m \geq 3$, we get generically that

$$G(t) = p(2t+1)(m^m(2pt+p) - (-1)^m(m-1)^{m-1}(4p^2u+1)^m),$$

from which it follows easily for $m \geq 3$ that

$$G(1) \equiv \begin{cases} 3p \pmod 4 & \text{if } m \equiv 0 \pmod 4 \\ 1 \pmod 4 & \text{if } m \equiv 1 \pmod 4 \\ p \pmod 4 & \text{if } m \equiv 2 \pmod 4 \\ 3 \pmod 4 & \text{if } m \equiv 3 \pmod 4. \end{cases}$$

Therefore, in each of these cases, we conclude from Corollary 2.9 that there exist infinitely many primes ρ such that $G(\rho)$ is squarefree. Consequently, for each $t = \rho$, $\mathcal{F}(x^{p^n})$ is monogenic for all integers $n \geq 0$ by Theorem 1.1. □

Acknowledgement

The authors thank the anonymous referee for the helpful suggestions.

References

[1] D. F. Bailey, Some binomial coefficient congruences, *Appl. Math. Lett.* **4** (1991), no. 4, 1–5.
[2] D. W. Boyd, G. Martin and M. Thom, *Squarefree values of trinomial discriminants*, LMS J. Comput. Math. **18** (2015), no. 1, 148–169.
[3] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, 2000.
[4] C. T. Davis and B. K. Spearman, *The index of a quartic field defined by a trinomial* $x^4 + ax + b$, J. Algebra Appl. **17** (2018), no. 10, 1850197, 18 pp.
[5] J. Dence and T. Dence, *Elements of the theory of numbers*, Harcourt/Academic Press, San Diego, CA, 1999.
[6] D. Grinberg, *The Lucas and Babbage congruences*, `http://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf`
[7] J. Harrington, On the factorization of the trinomials $x^n + cx^{n-1} + d$, *Int. J. Number Theory* **8** (2012), no. 6, 1513–1518.
[8] H. A. Helfgott, *Square-free values of $f(p)$, f cubic*, Acta Math. **213** (2014), no. 1, 107–135.
[9] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Mathematics, No. 70. Cambridge University Press, Cambridge-New York-Melbourne, (1976). xiv+122 pp.
[10] A. Jakhar, S. Khanduja and N. Sangwan, *Characterization of primes dividing the index of a trinomial*, Int. J. Number Theory **13** (2017), no. 10, 2505–2514.

[11] L. Jones and D. White, *Monogenic trinomials with non-squarefree discriminant*, Internat. J. Math. **32** (2021), no. 13, Paper No. 2150089, 21 pp.
[12] L. Jones, *Infinite families of non-monogenic trinomials*, Acta Sci. Math. (Szeged) **87** (2021), no. 1–2, 95–105.
[13] L. Jones, *Monogenic reciprocal trinomials and their Galois groups*, J. Algebra Appl. **21** (2022), no. 2, Paper No. 2250026, 11 pp.
[14] L. Jones, Infinite families of reciprocal monogenic polynomials and their Galois groups, *New York J. Math.* **27** (2021), 1465–1493.
[15] L. Jones, *Reciprocal monogenic quintinomials of degree* 2^n, Bull. Aust. Math. Soc. **106** (2022), no. 3, 437–447.
[16] L. Jones and T. Phillips, *Infinite families of monogenic trinomials and their Galois groups*, Internat. J. Math. **29** (2018), no. 5, 1850039, 11 pp.
[17] B. Koley and A. S. Reddy, *Survey on irreducibility of trinomials*, arXiv:2012.07568.
[18] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.
[19] H. Pasten, *The ABC conjecture, arithmetic progressions of primes and squarefree values of polynomials at prime arguments*, Int. J. Number Theory **11** (2015), no. 3, 721–737.
[20] J. Patsolic and J. Rouse, *Trinomials defining quintic number fields*, Int. J. Number Theory **13** (2017), no. 7, 1881–1894.
[21] W. Sawin, M. Shusterman and M. Stoll, Irreducibility of polynomials with a large gap, *Acta Arith.* **192** (2020), no. 2, 111–139.
[22] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, **77**, Cambridge University Press, Cambridge, 2000.
[23] I. E. Shparlinski, *On the distribution of irreducible trinomials*, Canad. Math. Bull. **54** (2011), no. 4, 748–756.
[24] H. Smith, Two families of monogenic S_4 quartic number fields, *Acta Arith.* **186** (2018), no. 3, 257–271.
[25] R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.
[26] L. C. Washington, *Introduction to cyclotomic fields, Second edition*, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1997.

Joshua Harrington
Department of Mathematics
Cedar Crest College
Allentown, Pennsylvania, USA
e-mail address: Joshua.Harrington@cedarcrest.edu

Lenny Jones, Professor Emeritus
Department of Mathematics
Shippensburg University
Shippensburg, Pennsylvania, USA
e-mail address: doctorlennyjones@gmail.com

(*Received April 28, 2023*)
(*Accepted December 11, 2023*)