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 $F(x) := x^m + Ax^{m-1} + B$. In this article, we determine sets of conditions on $m$, $A$, and $B$, such that the power compositional trinomial $F(x^p)$ 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 $F(x)$.

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

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

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

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

We determine sets of conditions on $m$, $A$ and $B$ so that the power compositional trinomial $F(x^p)$ 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.

Date: April 19, 2022.

2020 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
\begin{equation}
\mathcal{D} := m^m B - (-1)^m (m-1)^{m-1} A^m .
\end{equation}

(1) When $m = 2$, let $A = 4pu + p^2 + 2$ and $B = 2pt + 1$, where $u, t \in \mathbb{Z}$ are such that $B$ and $\mathcal{D}$ are squarefree, with $|B| \geq 2$.

(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, with $|B| \geq 2$.

(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, with $|B| \geq 2$, 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 $n \geq 0$.

2. Preliminaries

The formula for the discriminant of an arbitrary monic trinomial, due to Swan [25], 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 $d = \text{gcd}(n, m)$. Then
\begin{equation}
\Delta(f) = (-1)^{(n(n-1))/2} B^{m-1} \left( p^{n/d} B^{(n-m)/d} - (-1)^{n/d} (n-m)^{n-m)/d} m^{m/d} A^{n/d} \right)^d.
\end{equation}

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
\begin{equation}
\Delta(\mathcal{F}(x^p^n)) = (-1)^{mp^2(n-1)/2} B^{(m-1)p^n - 1} p^{mp^2n} \mathcal{D}^{p^n},
\end{equation}
where $\mathcal{D}$ is as defined in (1.3).

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

Theorem 2.3. 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. 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 $\theta$, and $\mathbb{Z}_K$ the ring of integers of $K$. Let $q$ be a prime number and let $\mathcal{T}$ denote reduction of $\star$ modulo $q$ (in $\mathbb{Z}$, $\mathbb{Z}[x]$ or $\mathbb{Z}[\theta]$). Let
\begin{equation}
\mathcal{T}(x) = \prod_{i=1}^{k} p_i(x)^{r_i}
\end{equation}
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 $\tau_i(x)$. Let $h(x) \in \mathbb{Z}[x]$ be a monic lift of $T(x)/g(x)$ and set

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

Then

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

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 $\gcd(M, N) = q_0$, $M = M_1q_0$ and $N = N_1q_0$. 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 $q \nmid A_2\left((-B)^{M_1}A_2^{N_1} - (-B_1)^{M_1}\right)$,

where $A_2 = \frac{B + (-B)^{q^j}}{q}$ with $q^j \mid N$;
3. if $q \nmid A$ and $q \mid B$, then either $q \mid A_1$ and $q \nmid B_2$ or $q \nmid A_1B_2^{M_1-1}\left((-A)^{M_1}A_1^{N_1} - (-B_2)^{N_1} - M_1\right)$,

where $A_1 = \frac{A + (-A)^{q^j}}{q}$ with $q^j \mid N - M$, 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

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

are coprime modulo $q$;
5. if $q \nmid ABM$, then

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

**Remark 2.7.** We will find both Theorem 2.5 and Theorem 2.6 useful in our investigations.

The next theorem follows from Corollary (2.10) in [13].

**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 $z \in (\mathbb{Z}/\ell^2\mathbb{Z})^*$ such that $G(z) \equiv 0 \pmod{\ell^2}$.

Remark 2.10. Theorem 2.9 follows from work of Helfgott, Hooley and Pasten [8, 9, 19]. For more details, see [14].

Definition 2.11. In the context of Theorem 2.9, for $G(t) \in \mathbb{Z}[t]$ and a prime $\ell$, 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 $\ell$.

The following immediate corollary of Theorem 2.9 is used to establish Corollary 1.2.

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 $\rho$ such that $G(\rho)$ 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 $a_t t + b_t$ with $\gcd(a_t, b_t) = 1$. 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 $\ell$ 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 $\ell$ lifts to the $\ell$ distinct zeros

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

of $G(t)$ modulo $\ell^2$ [3, Theorem 4.11]. That is, $G(t)$ has exactly $\ell(\ell - 1) = \phi(\ell^2)$ distinct zeros $z \in (\mathbb{Z}/\ell^2\mathbb{Z})^*$. Therefore, if the number of factors $k$ of $G(t)$ satisfies $k < 2(\ell - 1)$, then there must exist $z \in (\mathbb{Z}/\ell^2\mathbb{Z})^*$ for which $G(z) \not\equiv 0 \pmod{\ell^2}$, and we do not need to check such primes $\ell$ for a local obstruction. Consequently, only finitely many primes need to be checked for local obstructions. They are precisely the primes $\ell$ such that $\ell \leq (k + 2)/2$. 
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 \( |f(0)| \geq 2 \) and \( f(0) \) is squarefree, then \( f(x^p) \) is irreducible for all \( n \geq 0 \).

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

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

which contradicts the fact that \( f(0) \) is squarefree since \( N(\beta) \in \mathbb{Z} \) and \( |f(0)| \geq 2 \). \( \square \)

Note that the conditions in part (b) of Theorem 1.1 contain the assumption that \( F(x) \) 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 \( F(x) \) be as defined in 1.2, and let \( D \) 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 \( D \) are squarefree, with \( |B| \geq 2 \). If \( F(x) \) is irreducible, then \( F(x^{p^n}) \) 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.

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

The next lemma is similar in nature to Lemma 3.1 in [15]. We let \( T \) 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 \( \hat{z} \in \{0, 1, 2, 3\} \) be the reduction of \( z \) modulo 4.

**Lemma 3.4.** Let \( F(x) \) 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 \( F(x^{p^n}) \) is irreducible for all \( n \geq 0 \) if \((\hat{A}, \hat{B}) \in \Gamma_m\), 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 \((a, b) \in T \setminus \Gamma_m\), there exist integers \( A \) and \( B \) with \((\hat{A}, \hat{B}) = (a, b)\) such that \( F(x^{p^n}) \) is reducible for all \( n \geq 0 \).

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

\[
F(x) = x^4 + Ax^3 + B = (x^2 + c_1x + c_0)(x^2 + d_1x + d_0),
\]
for some $c_i, d_i \in \mathbb{Z}$. Expanding this factorization and equating coefficients yields the system of equations:

$$
\begin{align*}
\text{constant term : } & \quad c_0d_0 = B \\
\text{x : } & \quad c_0d_1 + c_1d_0 = 0 \\
\text{x}^2 : & \quad c_0 + d_0 + c_1d_1 = 0 \\
\text{x}^3 : & \quad c_1 + d_1 = A.
\end{align*}
$$

(3.1)

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

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

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 $(\hat{A}, \hat{B}) \in \Gamma_4$, and we omit the details. It follows that $F(x^{p^n})$ is irreducible for all $n \geq 0$ by Lemma 3.1.

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

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

| $(\hat{A}, \hat{B}) \in T \setminus \Gamma_2$ | $(A, B)$ | Factorization of $F(x^{p^n})$ |
|-------------------------------------------|----------|-------------------------------|
| (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 2. Examples for $(\hat{A}, \hat{B}) \in T \setminus \Gamma_3$ and their factorizations

| $(\hat{A}, \hat{B}) \in T \setminus \Gamma_3$ | $(A, B)$ | Factorization of $F(x^{p^n})$ |
|-------------------------------------------|----------|-------------------------------|
| (0, 1)                                    | (−4, 5)  | $(x^{p^n} + 1)(x^{p^n} + 5)$  |
| (0, 3)                                    | (−4, 3)  | $(x^{p^n} + 1)(x^{p^n} + 3)$  |
| (1, 2)                                    | (−3, 2)  | $(x^{p^n} + 1)(x^{p^n} + 2)$  |
| (2, 1)                                    | (−2, 1)  | $(x^{p^n} + 1)(x^{p^n} + 1)$  |
| (2, 3)                                    | (−2, 3)  | $(x^{p^n} + 1)(x^{p^n} + 3)$  |
| (3, 2)                                    | (−1, 2)  | $(x^{p^n} + 1)(x^{p^n} + 2)$  |
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 $\mathcal{F}(x^p)$ is irreducible for all $n \geq 0$ if $(\hat{A}, \hat{B}) \in \Gamma_m$, where

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

**Remark 3.6.** Note that the truth of Conjecture 3.5 also implies the conclusion of Corollary 3.2.

**Lemma 3.7.** Let $\mathcal{F}(x)$ be as defined in (1.2), and let $p$ be a prime. Suppose that $B$ is squarefree with $|B| \geq 2$, 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 3.2 that

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

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 (3) 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 (3) are trivially true. For statement (4), 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 (4) is true and $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \neq 0$ (mod $q$).

Suppose now that $q$ is a prime such that $q \nmid B$. 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, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \neq 0$ (mod $q$), and consequently, $\mathcal{F}(x)$ is monogenic, which completes the proof of the lemma.

**Proof of Theorem 3.7.** For part (1), we see that

$$(\hat{A}, \hat{B}) \in \{(3, 1), (3, 3)\} \subset \Gamma_2.$$
Thus, \( \mathcal{F}(x^n) \) is irreducible for all \( n \geq 0 \) by Lemma 3.7 and \( \mathcal{F}(x) \) is monogenic by Lemma 3.7. By Corollary 2.2, we have that
\[
\Delta(\mathcal{F}(x^n)) = (-1)^p n(2p^{n-1})Bp^{n-1}p^{2n}D^n,
\]
where \( D = 4B - A^2 \).

Define
\[
\theta_n := \theta^{1/p^n} \quad \text{and} \quad K_n := \mathbb{Q}(\theta_n) \quad \text{for} \quad n \geq 0,
\]
noting that \( \theta_0 = \theta \) and \( K_0 = K \) from the proof of Lemma 3.7. Furthermore, observe that \( \mathcal{F}((\theta_n)^p) = 0 \) and \( [K_{n+1} : K_n] = p \) for all \( n \geq 0 \). We assume that \( \mathcal{F}(x^n) \) is monogenic and proceed by induction on \( n \). Then \( \Delta(\mathcal{F}(x^n)) = \Delta(K_n) \), and we deduce from Theorem 2.8 that
\[
\Delta(\mathcal{F}(x^n))^p \mid \Delta(K_{n+1}).
\]

By (3.3), we have that
\[
\Delta(\mathcal{F}(x^{n+1}))/\Delta(\mathcal{F}(x^n))^p = Bp + p^p + 1.
\]

Hence, to show that \( \mathcal{F}(x^{n+1}) \) is monogenic, we only have to show that
\[
[\mathbb{Z}_{K_{n+1}} : \mathbb{Z}[\theta_{n+1}]] \neq 0 \quad \text{(mod} \quad q \text{)}
\]
for all primes \( q \) dividing \( Bp \). We check that all statements in Theorem 2.6 are true for such primes, when applied to \( \mathcal{F}(x^{n+1}) = x^{2p^{n+1}} + Ax^{p+1} + B \).

Suppose first that \( q = p \). We use Theorem 2.5 with \( T(x) := \mathcal{F}(x^{p+1}) \). Since \( A \equiv 2 \pmod{p} \) and \( B \equiv 1 \pmod{p} \), we get that \( T(x) = (x + 1)^{2p^{n+1}} \). Thus, we can let \( g(x) = x + 1 \) and \( h(x) = (x + 1)^{2p^{n+1}} - 1 \), so that
\[
F(x) = \frac{g(x)h(x) - T(x)}{p^3}
= \frac{(x + 1)^{2p^{n+1}} - x^{2p^{n+1}} - A x^{p+1} - B}{p^3}
= \sum_{j=1}^{\frac{2p^{n+1}-1}{p}} \frac{\binom{2p^{n+1}}{j}}{p^3} x^j + \frac{(\binom{2p^{n+1}}{p} - A)x^{p+1}}{p^3} + \frac{1 - B}{p^3}.
\]

To show that \( \text{gcd}(T, \mathcal{F}) = 1 \), it is enough to show that \( F(-1) \neq 0 \pmod{p} \). Since
\[
\sum_{j=1}^{\frac{2p^{n+1}-1}{p}} \binom{2p^{n+1}}{j} x^j = (x + 1)^{2p^{n+1}} - x^{2p^{n+1}} - 1 - \binom{2p^{n+1}}{p+1} x^{p+1},
\]
it follows that
\[
\sum_{j=1}^{\frac{2p^{n+1}-1}{p}} \binom{2p^{n+1}}{j} (-1)^j = -2 + \binom{2p^{n+1}}{p+1} \equiv 0 \pmod{p^2} \quad \text{(mod} \quad p^2 \text{)}.
\]

Hence, the sum in \( 3.4 \) is zero modulo \( p \) when \( x = -1 \). Also, since \( A \equiv 2 \pmod{p} \) and \( B - 1 \) is squarefree, we see from \( 3.4 \) that
\[
F(-1) \equiv \frac{1 - B}{p} \neq 0 \pmod{p}.
\]

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 2.3 and we want to show that all statements are true for \( F(x^{p^{n+1}}) \) 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
\[
\ell - F = p^{n+1} - x^{3p^{n+1} - 1} - 2x^{2p^{n+1}} + B,
\]
where
\[
D = 27B + 4A^3.
\]
Using (3.5) and Theorem 2.8 for
\[
\mathcal{F}(x^{p^{n+1}}) = x^{3p^{n+1} + 1} + Ax^{2p^{n+1}} + B,
\]
and arguing as in part (1) with \( \theta_q \) 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 \( T(x) := F(x^{p^{n+1}}) \). Since \( A \equiv 1 \pmod{p} \) and \( B \equiv 0 \pmod{p} \), we get that
\[
T(x) = x^{2p^{n+1}} + (x + 1)^{p^{n+1}}.
\]
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
\[
F(x) = \frac{g(x)h(x) - T(x)}{p}
= \frac{x^{2p^{n+1}}(x + 1)^{p^{n+1}} - x^{3p^{n+1} + 1} - A2p^{n+1} - B}{p}
= \sum_{j=1}^{p^{n+1} - 1} \frac{p^{n+1}}{p} - x^{j+2p^{n+1}} + \left(1 - \frac{A}{p}\right)x^{2p^{n+1}} - \frac{B}{p}
\]
(3.6)
To show that \( \gcd(\overline{g,F}) = 1 \), it is enough to show that \( F(c) \equiv 0 \pmod{p} \), 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,
\[
F(c) \equiv -\frac{B}{p} \equiv 0 \pmod{p},
\]
since \( B \) is squarefree. Thus, we deduce from Theorem 2.6 that (3.6) 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 \( F(x^{p^{n+1}}) \) 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, \(33\) is true. Consequently, \(F(x^n)\) is monogenic for all \(n \geq 0\) by induction. \(\square\)

4. Proof of Corollary \ref{corollary}

\textbf{Proof.} For all cases of \(m\) in Theorem \ref{theorem} we define \(G(t) := BD\). We wish to apply Corollary \ref{corollary} and so we must check for local obstructions. In light of the discussion following Corollary \ref{corollary} since \(B\) and \(D\) 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 \ref{theorem} (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 \ref{corollary} there exist infinitely many primes \(\rho\) such that \(G(\rho)\) is squarefree. Therefore, we see that \(|B| \geq 2\), and both \(B\) and \(D\), individually, are squarefree for such primes \(\rho\). Note also that \(B - 1 = 2pt\) is squarefree when \(t = \rho > p\). Consequently, for each \(t = \rho > p\), \(F(x^n)\) is monogenic for all integers \(n \geq 0\) by Theorem \ref{theorem}.

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 \ref{corollary} that there exist infinitely many primes \(\rho\) such that \(G(\rho)\) is squarefree. Consequently, for each \(t = \rho\), \(F(x^n)\) is monogenic for all integers \(n \geq 0\) by Theorem \ref{theorem}. \(\square\)

\textbf{References}

[1] D. F. Bailey, Some binomial coefficient congruences, \textit{Appl. Math. Lett.} 4 (1991), no. 4, 1–5.
[2] D. W. Boyd, G. Martin and M. Thom, \textit{Squarefree values of trinomial discriminants}, LMS J. Comput. Math. 18 (2015), no. 1, 148–169.
[3] H. Cohen, \textit{A Course in Computational Algebraic Number Theory}, Springer-Verlag, 2000.
[4] C. T. Davis and B. K. Spearman, \textit{The index of a quartic field defined by a trinomial} \(ax^4+ax+b\), J. Algebra Appl. 17 (2018), no. 10, 1850197, 18 pp.
[5] J. Dence and T. Dence, \textit{Elements of the theory of numbers}, Harcourt/Academic Press, San Diego, CA, 1999.
[6] D. Grinberg, \textit{The Lucas and Babbage congruences}, \textit{http://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf}
[7] J. Harrington, On the factorization of the trinomials \(x^n + cx^n - d\), \textit{Int. J. Number Theory} 8 (2012), no. 6, 1513–1518.
[8] H. A. Helfgott, \textit{Square-free values of \(f(p)\), \(f\) cubic}, Acta Math. 213 (2014), no. 1, 107–135.
[9] C. Hooley, \textit{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, \textit{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, \textit{Monogenic trinomials with non-squarefree discriminant}, Internat. J. Math. 32 (2021), no. 13, Paper No. 2150089, 21 pp.
[12] L. Jones, \textit{Infinite families of non-monogenic trinomials}, Acta Sci. Math. (Szeged) 87 (2021), no. 1–2, 95–105.
[13] L. Jones, \textit{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. (to appear).
[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.

DEPARTMENT OF MATHEMATICS, CEDAR CREST COLLEGE, ALLENTOWN, PENNSYLVANIA, USA

*Email address*, Joshua Harrington: Joshua.Harrington@cedarcrest.edu

PROFESSOR EMERITUS, DEPARTMENT OF MATHEMATICS, SHIPPENSBURG UNIVERSITY, SHIPPENSBURG, PENNSYLVANIA 17257, USA

*Email address*, Lenny Jones: lkjone@ship.edu