sciendo

Annales Mathematicae Silesianae (2024),
DOI: 10.2478/amsil-2024-0003

RECIPROCAL MONOGENIC SEPTINOMIALS OF DEGREE 2^n3

Lenny Jones

Abstract. We prove a new irreducibility criterion for certain septinomials in $\mathbb{Z}[x]$, and we use this result to construct infinite families of reciprocal septinomials of degree 2^n3 that are monogenic for all $n \geq 1$.

1. Introduction

Let $f(x) \in \mathbb{Z}[x]$. When we say that $f(x)$ is "irreducible" or "reducible", without reference to a particular field, we mean that $f(x)$ is "irreducible" or "reducible" over the rational numbers $\mathbb{Q}$. We call $f(x)$ *reciprocal* if $f(x) = x^{\deg(f)} f(1/x)$. We let $\Delta(f)$ 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 we have the well-known equation [1]

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

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, we have that $\{1, \theta, \theta^2, \ldots, \theta^{\deg f - 1}\}$ is a basis for $\mathbb{Z}_K$, commonly referred to as a *power basis*. The existence of a power basis

Received: 11.06.2023. Accepted: 24.01.2024.
(2020) Mathematics Subject Classification: 11R04, 11R09, 12F05.
Key words and phrases: reciprocal, monogenic, septinomial, irreducible.

makes computations in $\mathbb{Z}_K$ easier, as in the case of the cyclotomic polynomials $\Phi_n(x)$ [12]. 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.

Recently [9], a procedure was presented to manufacture infinite families of reciprocal quintinomials of degree 2^n that are monogenic for all $n \geq 2$. In this article, we use similar methods to construct infinite families of reciprocal septinomials in $\mathbb{Z}[x]$ of degree $2^n 3$ that are monogenic for all $n \geq 1$. We should point out that, using different methods, infinite families of reciprocal monogenic septinomials of degree 6 were given in [8]. Our main results here are the following:

THEOREM 1.1. *Let $n, A, B \in \mathbb{Z}$ with $n \geq 1$. Define the reciprocal polynomial*

$$\mathcal{F}_{n,A,B}(x) := x^{2^n \cdot 3} + 9Ax^{2^{n-1} \cdot 5} + (27A^2+3)x^{2^{n+1}} + 3Bx^{2^{n-1} \cdot 3} + (27A^2+3)x^{2^n} + 9Ax^{2^{n-1}} + 1. \tag{1.2}$$

If $B \not\equiv 0 \pmod 3$, $(\widehat{A}, \widehat{B}) \in \Psi := \{(1,1),(3,3)\}$, where $\widehat{*} \in \{0,1,2,3\}$ is the reduction modulo 4 of $*$, and

$$\mathcal{D} := (3B + 54A^2 + 18A + 8)(3B - 54A^2 + 18A - 8)(B - 9A^3 - 6A)$$

is squarefree, then the septinomial $\mathcal{F}_{n,A,B}(x)$ is monogenic for all $n \geq 1$.

COROLLARY 1.2. *Let $\mathcal{F}_{n,A,B}(x)$ be as defined in (1.2). Then, for any $u \in \mathbb{Z}$,*

(1) *there exist infinitely many primes q such that $\mathcal{F}_{n,4u+1,12q+1}(x)$ is monogenic for all $n \geq 1$,*
(2) *there exist infinitely many primes q such that $\mathcal{F}_{n,4u+3,12q+7}(x)$ is monogenic for all $n \geq 1$.*

2. Preliminaries

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:

$$R(f,g) = a^N \prod_{i=1}^{M} g(\alpha_i) = (-1)^{MN} b^M \prod_{i=1}^{N} f(\beta_i).$$

THEOREM 2.2. *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*

$$\Delta(f\circ g) = (-1)^{M^2N(N-1)/2}\cdot a^{N-1}b^{M(MN-N-1)}\Delta(f)^N R(f\circ g, g').$$

REMARK 2.3. As far as we can determine, Theorem 2.2 is originally due to John Cullinan [2]. A proof of Theorem 2.2 can be found in [5].

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 2.4 (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 next theorem follows from Corollary 2.10 in [10].

THEOREM 2.5. *Let K and L be number fields with $K \subset L$. Then*

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

THEOREM 2.6. *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

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

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

REMARK 2.7. Theorem 2.6 follows from work of Helfgott, Hooley and Pasten [6, 7, 11]. For more details, see [8].

DEFINITION 2.8. In the context of Theorem 2.6, 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 2.6 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 q such that $G(q)$ 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 [3, 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 $\ell \le (k+2)/2$.

The following proposition, which follows from a generalization of a theorem of Capelli, is a special case of the results in [4], and gives simple necessary and sufficient conditions for the irreducibility of polynomials of the form $w(x^{2^k}) \in \mathbb{Z}[x]$, when $w(x)$ is monic and irreducible.

PROPOSITION 2.10 ([4]). *Let $w(x) \in \mathbb{Z}[x]$ be monic and irreducible, with $\deg(w) = m$. Then $w\left(x^{2^k}\right)$ is reducible if and only if there exist $S_0(x), S_1(x) \in \mathbb{Z}[x]$ such that either*

$$(-1)^m w(x) = \left(S_0(x)\right)^2 - x\left(S_1(x)\right)^2,$$

or

$$k \ge 2 \quad \textit{and} \quad w\left(x^2\right) = \left(S_0(x)\right)^2 - x\left(S_1(x)\right)^2.$$

3. The proof of Theorem 1.1

For the proof of Theorem 1.1, we require the following lemma, which is of some independent interest.

LEMMA 3.1. *Let $n, A, B \in \mathbb{Z}$, with $n \geq 1$, and let $\mathcal{F}_{n,A,B}(x)$ be as defined in (1.2). Then $\mathcal{F}_{n,A,B}(x)$ is irreducible for all $n \geq 1$ if and only if*

$$(\widehat{A}, \widehat{B}) \in \Gamma = \{(0,2), (1,1), (2,2), (3,3)\},$$

where $\widehat{*} \in \{0,1,2,3\}$ is the reduction modulo 4 of $*$.

PROOF. Suppose first that $(\widehat{A}, \widehat{B}) \in \Gamma$. This direction of the proof is composed of several steps, each of which involves a proof by contradiction. For most of the steps, the procedure is the same. We assume that two particular polynomials are equal, equate coefficients on the two polynomials and show that there is no solution to the resulting system of equations. To see that there is no solution, we view the system of equations arising from equating the coefficients of the two polynomials as a system of congruences modulo 4. We then use a computer to verify, for every possible viable set of values of the variables modulo 4, that there is always at least one congruence that is impossible. Because there are so many possibilities, we do not provide all details of the computer calculations.

We begin by showing that

$$\mathcal{F}_{1,A,B}(x) = x^6 + 9Ax^5 + (27A^2+3)x^4 + 3Bx^3 + (27A^2+3)x^2 + 9Ax + 1 \tag{3.1}$$

is irreducible. Assume, by way of contradiction, that $\mathcal{F}_{1,A,B}(x)$ is reducible. Observe that if

$$\mathcal{F}_{1,A,B}(1) = 54A^2 + 18A + 3B + 8 = 0,$$

then $B = -18A^2 - 6A - 8/3 \notin \mathbb{Z}$. Similarly, $\mathcal{F}_{1,A,B}(-1) \neq 0$. Hence, $\mathcal{F}_{1,A,B}(x)$ has no linear factors by the Rational Zero Theorem. Suppose then that

$$\mathcal{F}_{1,A,B}(x) = (x^2 + a_1x + a_0)(x^4 + b_3x^3 + b_2x^2 + b_1x + b_0), \tag{3.2}$$

for some $a_i, b_i \in \mathbb{Z}$. Expanding the right-hand side of (3.2) and equating coefficients with $\mathcal{F}_{1,A,B}(x)$ in (3.1), we arrive at the system of equations:

$$\begin{aligned}
\text{constant term}: &\quad a_0b_0 = 1\\
x: &\quad a_0b_1 + a_1b_0 = 9A\\
x^2: &\quad b_0 + a_1b_1 + a_0b_2 = 27A^2 + 3\\
x^3: &\quad b_1 + a_1b_2 + a_0b_3 = 3B\\
x^4: &\quad a_0 + a_1b_3 + b_2 = 27A^2 + 3\\
x^5: &\quad a_1 + b_3 = 9A.
\end{aligned} \tag{3.3}$$

As previously mentioned, to see that the system (3.3) has no solutions, we view (3.3) as a system of congruences modulo 4. Then we use a computer to check every $(\widehat{A}, \widehat{B}) \in \Gamma$ and every possible value for $\widehat{a_i}$ and $\widehat{b_i}$, noting that either $a_0 = b_0 = 1$ or $a_0 = b_0 = -1$. In every situation, there is at least one impossible congruence. For example, if

$$(\widehat{A}, \widehat{B}) = (0, 2) \quad \text{and} \quad (\widehat{a_0}, \widehat{a_1}, \widehat{b_0}, \widehat{b_1}, \widehat{b_2}, \widehat{b_3}) = (3, 0, 3, 0, 2, 1),$$

then the left-hand side of the congruence corresponding to x^2 reduces to 1 (mod 4), while the right-hand side reduces to 3 (mod 4). Also, the left-hand side of the congruence corresponding to x^3 reduces to 3 (mod 4), while the right-hand side reduces to 2 (mod 4).

Hence, it must be that

$$\mathcal{F}_{1,A,B}(x) = (x^3 + a_2x^2 + a_1x + a_0)(x^3 + b_2x^2 + b_1x + b_0), \tag{3.4}$$

for some $a_i, b_i \in \mathbb{Z}$. However, when we apply the same procedure to (3.4), we also arrive at a contradiction in every possible scenario. For example, if

$$(\widehat{A}, \widehat{B}) = (2, 2) \quad \text{and} \quad (\widehat{a_0}, \widehat{a_1}, \widehat{a_2}, \widehat{b_0}, \widehat{b_1}, \widehat{b_2}) = (1, 1, 1, 1, 1, 1),$$

then the left-hand side of the congruence corresponding to x^3, which is

$$a_0 + a_1b_2 + a_2b_1 + b_0 \equiv 3B \pmod 4,$$

reduces to 0 (mod 4), while the right-hand side reduces to 2 (mod 4). We remark that this is the only contradictory congruence for this example. Thus, we deduce that $\mathcal{F}_{1,A,B}(x)$ is irreducible.

Observing that $\mathcal{F}_{n,A,B}(x) = \mathcal{F}_{1,A,B}(x^{2^{n-1}})$ for $n \geq 1$, we apply Proposition 2.10 with $w(x) = \mathcal{F}_{1,A,B}(x)$ and $m = 6$. We first address the case $n = 2$, which corresponds to $k = 1$ in Proposition 2.10. By way of contradiction, we assume that $\mathcal{F}_{2,A,B}(x) = \mathcal{F}_{1,A,B}(x^2)$ is reducible. Then, by Proposition 2.10, we have that there exist $S_0(x), S_1(x) \in \mathbb{Z}[x]$ such that

$$\mathcal{F}_{1,A,B}(x) = \big(S_0(x)\big)^2 - x\big(S_1(x)\big)^2.$$

Since $\deg(\mathcal{F}_{1,A,B}) = 6$, it follows that

$$S_0(x) = x^3 + a_2x^2 + a_1x + a_0 \quad \text{and} \quad S_1(x) = b_2x^2 + b_1x + b_0$$

for some $a_i, b_i \in \mathbb{Z}$. Then

$$(3.5)\quad \begin{aligned}(S_0(x))^2 - x\,(S_1(x))^2 &= x^6 + (2a_2 - b_2^2)x^5 \\ &+ (2a_1 - 2b_1b_2 + a_2^2)x^4 + (2a_0 - b_1^2 - 2b_0b_2 + 2a_1a_2)x^3 \\ &+ (a_1^2 + 2a_0a_1 - 2b_0b_1)x^2 + (2a_0a_1 - b_0^2)x + a_0^2.\end{aligned}$$

We equate coefficients on (3.5) and (3.1), which yields the system of equations:

$$(3.6)\quad \begin{aligned}\text{constant term}: &\quad a_0^2 = 1 \\ x: &\quad 2a_0a_1 - b_0^2 = 9A \\ x^2: &\quad a_1^2 + 2a_0a_2 - 2b_0b_1 = 27A^2 + 3 \\ x^3: &\quad 2a_0 - b_1^2 + 2a_1a_2 - 2b_0b_2 = 3B \\ x^4: &\quad 2a_1 + a_2^2 - 2b_1b_2 = 27A^2 + 3 \\ x^5: &\quad 2a_2 - b_2^2 = 9A.\end{aligned}$$

Noting that $a_0 = \pm 1$, and applying the same procedure as before to the system (3.6), we see that every possibility provides a contradiction. For example, if

$$(\widehat{A}, \widehat{B}) = (3, 3) \quad \text{and} \quad (\widehat{a_0}, \widehat{a_1}, \widehat{a_2}, \widehat{b_0}, \widehat{b_1}, \widehat{b_2}) = (1, 0, 0, 0, 1, 1),$$

then the left-hand side of the congruence corresponding to x reduces to $0 \pmod 4$, while the right-hand side reduces to $3 \pmod 4$.

Now suppose that $n \geq 3$, which corresponds to $k \geq 2$ in Proposition 2.10. Assume, by way of contradiction, that $\mathcal{F}_{n,A,B}(x)$ is reducible. Then, by Proposition 2.10, there exist $S_0(x), S_1(x) \in \mathbb{Z}[x]$ such that

$$(3.7)\qquad w(x^2) = \mathcal{F}_{1,A,B}(x^2) = \mathcal{F}_{2,A,B}(x) = \big(S_0(x)\big)^2 - x\big(S_1(x)\big)^2,$$

where

$$S_0(x) = x^6 + \sum_{j=0}^{5} c_j x^j \quad \text{and} \quad S_1(x) = \sum_{j=0}^{5} d_j x^j,$$

for some $c_j, d_j \in \mathbb{Z}$. Noting that $c_0 = \pm 1$, we equate the other coefficients in (3.7) and use the same procedure as before to verify that there is no solution to the resulting system of equations. For example, if $(\widehat{A}, \widehat{B}) = (1, 1)$ and

$$(\widehat{c_0}, \widehat{c_1}, \widehat{c_2}, \widehat{c_3}, \widehat{c_4}, \widehat{c_5}, \widehat{d_0}, \widehat{d_1}, \widehat{d_2}, \widehat{d_3}, \widehat{d_3}) = (1, 0, 0, 0, 0, 0, 2, 0, 0, 1, 1, 1),$$

Table 1. Examples for (3.8) and their factorizations

$(\widehat{A},\widehat{B})$	(A,B)	Factorization of $\mathcal{F}_{n,A,B}(x)$
$(0,0)$	$(4,24)$	$(x^{2^{n+1}}+36x^{2^{n-1}3}+434x^{2^n}+36x^{2^{n-1}}+1)\Phi_{2^{n+1}}(x)$
$(0,1)$	$(4,357)$	$(x^{2^n}+3x^{2^{n-1}}+1)(x^{2^{n+1}}+33x^{2^{n-1}3}+335x^{2^n}+33x^{2^{n-1}}+1)$
$(0,3)$	$(4,591)$	$(x^{2^n}+9x^{2^{n-1}}+1)(x^{2^{n+1}}+27x^{2^{n-1}3}+191x^{2^n}+27x^{2^{n-1}}+1)$
$(1,0)$	$(1,24)$	$(x^{2^n}+6x^{2^{n-1}}+1)(x^{2^{n+1}}+3x^{2^{n-1}3}+11x^{2^n}+3x^{2^{n-1}}+1)$
$(1,2)$	$(1,6)$	$(x^{2^{n+1}}+9x^{2^{n-1}3}+29x^{2^n}+9^{2^{n-1}}+1)\Phi_{2^{n+1}}(x)$
$(1,3)$	$(1,15)$	$(x^{2^n}+3x^{2^{n-1}}+1)^3$
$(2,0)$	$(2,12)$	$(x^{2^{n+1}}+18x^{2^{n-1}3}+110x^{2^n}+18x^{2^{n-1}}+1)\Phi_{2^{n+1}}(x)$
$(2,1)$	$(2,93)$	$(x^{2^n}+9x^{2^{n-1}}+1)(x^{2^{n+1}}+9x^{2^{n-1}3}+29x^{2^n}+9x^{2^{n-1}}+1)$
$(2,3)$	$(2,75)$	$(x^{2^n}+3x^{2^{n-1}}+1)(x^{2^{n+1}}+15x^{2^{n-1}3}+65x^{2^n}+15x^{2^{n-1}}+1)$
$(3,0)$	$(3,252)$	$(x^{2^n}+6x^{2^{n-1}}+1)(x^{2^{n+1}}+21x^{2^{n-1}3}+119x^{2^n}+21x^{2^{n-1}}+1)$
$(3,1)$	$(3,189)$	$(x^{2^n}+3x^{2^{n-1}}+1)(x^{2^{n+1}}+24x^{2^{n-1}3}+173x^{2^n}+24x^{2^{n-1}}+1)$
$(3,2)$	$(3,18)$	$(x^{2^{n+1}}+27x^{2^{n-1}3}+245x^{2^n}+27x^{2^{n-1}}+1)\Phi_{2^{n+1}}(x)$

then the left-hand side of the congruence corresponding to x^3, which is

$$c_1^2+2c_0c_2-2d_0d_1\equiv 9A \pmod 4,$$

reduces to $0 \pmod 4$, while the right-hand side reduces to $1 \pmod 4$. Hence, we conclude, by Proposition 2.10, that $\mathcal{F}_{n,A,B}(x)$ is irreducible for all $n\geq 1$, and the proof of the lemma is complete in this direction.

For the other direction of the proof, suppose that $(\widehat{A},\widehat{B})\notin\Gamma$. That is, assume $(\widehat{A},\widehat{B})$ is an element of the set

$$\{(0,0),(0,1),(0,3),(1,0),(1,2),(1,3),\\ (2,0),(2,1),(2,3),(3,0),(3,1),(3,2)\}. \tag{3.8}$$

For each $(\widehat{A},\widehat{B})$ in (3.8), we provide in Table 1 an explicit example of (A,B) such that $\mathcal{F}_{n,A,B}(x)$ is reducible, not only for some n, but for all $n\geq 1$. In Table 1, we let $\Phi_N(x)$ denote the cyclotomic polynomial of index N. □

Proof of Theorem 1.1. Observe first that since $\Psi\subset\Gamma$, $\mathcal{F}_{n,A,B}(x)$ is irreducible for all $n\geq 1$ by Lemma 3.1. To complete the proof of monogenicity, we examine the prime divisors of $\Delta(\mathcal{F}_{n,A,B})$.

We begin with the case $n = 1$. Suppose that $\mathcal{F}_{1,A,B}(\theta) = 0$. A computation in Maple produces

$$\Delta(\mathcal{F}_{1,A,B}) = 3^{10}(3B+54A^2+18A+8)(3B-54A^2+18A-8)(B-9A^3-6A)^4. \tag{3.9}$$

We use Theorem 2.4 with $T(x) := \mathcal{F}_{1,A,B}(x)$ to show that $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$, for every prime q dividing $\Delta(\mathcal{F}_{1,A,B})$, where $\mathbb{Z}_K$ is the ring of integers of $K = \mathbb{Q}(\theta)$. Because $\mathcal{D}$ is squarefree, it follows from (3.9) and (1.1) that no prime dividing

$$(3B + 54A^2 + 18A + 8)(3B - 54A^2 + 18A - 8)$$

can divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Hence, we only need to focus on the prime 3 and primes dividing $B - 9A^3 - 6A$.

Suppose first that $q = 3$. Then, in Theorem 2.4, we have $\overline{T}(x) = (x^2+1)^3$, so that we can let

$$g(x) = x^2 + 1 \text{ and } h(x) = (x^2 + 1)^2.$$

Then

$$\overline{F}(x) = \overline{\left(\frac{(x^2 + 1)^3 - T(x)}{3}\right)} = 2Bx^3 \not\equiv 0 \pmod{3}$$

since $B \not\equiv 0 \pmod{3}$. Thus, it is easy to see that $\gcd(\overline{F}, \overline{g}) = 1$, and consequently, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{3}$ by Theorem 2.4.

Next, suppose that $q \neq 3$ is a prime divisor of $B - 9A^3 - 6A$. Then

$$\overline{T}(x) = (x^2 + 3Ax + 1)^3 = \overline{\tau}(x)^3.$$

By the quadratic formula, there are three cases to consider:

(1) $\overline{\tau}(x) \equiv (x + 3A/2)^2 \pmod{q}$,

(2) $\overline{\tau}(x)$ is irreducible over $\mathbb{F}_q$,

(3) $\overline{\tau}(x) \equiv (x - (-3A + w)/2)(x - (-3A - w)/2) \pmod{q}$, where $w^2 \equiv 9A^2 - 4 \pmod{q}$.

Case (1) occurs if $\Delta(x^2 + 3Ax + 1) = 9A^2 - 4 \equiv 0 \pmod{q}$. Then, $A \equiv \pm(2/3) \pmod{q}$ and, respectively, $B \equiv \pm(20/3) \pmod{q}$ since $B \equiv 9A^3 + 6A \pmod{q}$. But then, respectively,

$$3B \mp 54A^2 + 18A \mp 8 \equiv 0 \pmod{q},$$

contradicting, in either situation, the fact that $\mathcal{D}$ is squarefree. Hence, case (1) cannot happen.

Suppose next that we are in case (2), so that we can let

$$g(x) = x^2 + 3Ax + 1 \quad \text{and} \quad h(x) = (x^2 + 3Ax + 1)^2.$$

Then

$$\overline{F}(x) = \overline{\left(\frac{g(x)h(x) - T(x)}{q}\right)} = -3\overline{\left(\frac{B - 9A^3 - 6A}{q}\right)}x^2 \not\equiv 0 \pmod{q},$$

since $B - 9A^3 - 6A$ is squarefree and $q \neq 3$. Then it is easy to see that $\gcd(\overline{F}, \overline{g}) = 1$. Hence, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$ by Theorem 2.4, and $\mathcal{F}_{1,A,B}(x)$ is monogenic in this case.

Finally, suppose that we are in case (3). Without loss of generality, assume that $w \equiv 1 \pmod 2$. Since $w^2 \equiv 9A^2 - 4 \pmod q$, we can write

$$w^2 = 9A^2 - 4 + qk, \tag{3.10}$$

for some $k \in \mathbb{Z}$. Note that $k \equiv 0 \pmod 4$. Then $-3A \pm w \equiv 0 \pmod 2$ since $A \equiv 1 \pmod 2$. Thus, we can let

$$g(x) = h(x) = (x - (-3A + w)/2)(x - (-3A - w)/2),$$

so that

$$g(x)h(x) = x^2 + 3Ax + (9/4)A^2 - w^2/4 = x^2 + 3Ax + 1 - qk/4 \in \mathbb{Z}[x]$$

by (3.10). Therefore, to prove that $\gcd(\overline{F}, \overline{g}) = 1$, we only have to show that $\overline{F}((-3A \pm w)/2) \neq 0$. Because the methods are the same, we give details only for $x = (-3A + w)/2$. Noting that

$$\overline{F}((-3A + w)/2) \neq 0 \quad \text{if and only if} \quad qF((-3A + w)/2) \not\equiv 0 \pmod{q^2},$$

we examine $qF((-3A + w)/2)$. Then, using (3.10) and the fact that q divides $B - 9A^3 - 6A$, a straightforward calculation in Maple yields

$$\begin{aligned} 64qF((-3A + w)/2) &= -k^3q^3 - 24k(9A - w)(9A^3 + 6A - B)q \\ &\quad - 96(27A^3 - 9A - w(9A^2 - 1))(9A^3 + 6A - B) \\ &\equiv -96(27A^3 - 9A - w(9A^2 - 1))(9A^3 + 6A - B) \pmod{q^2}. \end{aligned} \tag{3.11}$$

We claim that

$$27A^3 - 9A - w(9A^2 - 1) \not\equiv 0 \pmod q. \tag{3.12}$$

Assume, by way of contradiction, that

$$27A^3 - 9A - w(9A^2 - 1) \equiv 0 \pmod{q}. \tag{3.13}$$

Then, if

$$9A^2 - 1 \equiv 0 \pmod{q}, \tag{3.14}$$

it follows that

$$27A^3 - 9A \equiv -6A \equiv 0 \pmod{q},$$

which implies that $A \equiv 0 \pmod{q}$ since $q \notin \{2, 3\}$. Consequently,

$$9A^2 - 1 \equiv -1 \pmod{q},$$

contradicting (3.14). Hence, $9A^2 - 1 \not\equiv 0 \pmod{q}$, and we have from (3.13) that

$$w^2 \equiv \frac{(27A^3 - 9A)^2}{(9A^2 - 1)^2} \pmod{q}.$$

Then, since $w^2 \equiv 9A^2 - 4 \pmod{q}$, we arrive at the congruence

$$(27A^3 - 9A)^2 \equiv (9A^2 - 1)^2(9A^2 - 4) \pmod{q},$$

which yields, after expansion, the impossible congruence $4 \equiv 0 \pmod{q}$. Hence, (3.12) is established. Since $9A^3 + 6A - B$ is squarefree, we deduce from (3.11) that $qF((-3A+w)/2) \not\equiv 0 \pmod{q^2}$, and the proof that $\mathcal{F}_{1,A,B}(x)$ is monogenic is complete.

Next, we address the monogenicity of $\mathcal{F}_{n,A,B}(x)$ for $n \geq 2$. Since $\mathcal{F}_{n,A,B}(x) = \mathcal{F}_{1,A,B}(x^{2^{n-1}})$ for $n \geq 1$, we use Theorem 2.2 and Definition 2.1 to calculate

$$\begin{aligned}\Delta(\mathcal{F}_{n,A,B}) &= \Delta\left(\mathcal{F}_{1,A,B} \circ x^{2^{n-1}}\right) \\ &= (-1)^{3^2 \cdot 2^n (2^{n-1}-1)} \Delta(\mathcal{F}_{1,A,B})^{2^{n-1}} R(\mathcal{F}_{n,A,B}, 2^{n-1} x^{2^{n-1}-1}) \\ &= 2^{3 \cdot 2^n (n-1)} \Delta(\mathcal{F}_{1,A,B})^{2^{n-1}}.\end{aligned} \tag{3.15}$$

For $n \geq 1$, we define

$$\theta_n := \theta^{1/2^{n-1}} \quad \text{and} \quad K_n := \mathbb{Q}(\theta_n),$$

noting that $\theta_1 = \theta$ and $K_1 = K$ from the case $n = 1$ earlier in this proof. Furthermore, observe that $\mathcal{F}_{n,A,B}(\theta_n) = 0$ and $[K_{n+1} : K_n] = 2$. Thus, if $\mathcal{F}_{n,A,B}(x)$ is monogenic, then $\Delta(\mathcal{F}_{n,A,B}) = \Delta(K_n)$, and we deduce from Theorem 2.5 that

$$\Delta(K_{n+1}) \equiv 0 \pmod{\Delta(\mathcal{F}_{n,A,B})^2}.$$

By (3.15), we have that

$$\Delta(\mathcal{F}_{n+1,A,B})/\Delta(\mathcal{F}_{n,A,B})^2 = 2^{3\cdot 2^{n+1}}.$$

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

$$\left[\mathbb{Z}_{K_{n+1}} : \mathbb{Z}[\theta_{n+1}]\right] \not\equiv 0 \pmod{2}. \tag{3.16}$$

We apply Theorem 2.4 with $T(x) := \mathcal{F}_{n+1,A,B}(x)$. Then

$$\overline{T}(x) = (x^6 + x^5 + x^3 + x + 1)^{2^n} = (x^2 + x + 1)^{3\cdot 2^n} = \Phi_3(x)^{3\cdot 2^n},$$

where $\Phi_3(x)$ is easily seen to be irreducible over $\mathbb{F}_2$. Therefore, we can let

$$g(x) = \Phi_3(x) \quad \text{and} \quad h(x) = \Phi_3(x)^{3\cdot 2^n - 1}.$$

A straightforward induction argument shows for $n \geq 1$ that

$$g(x)h(x) = \Phi_3(x)^{3\cdot 2^n} \equiv Q(x) \pmod{4},$$

where

$$\begin{aligned} Q(x) = {} & x^{12\cdot 2^{n-1}} + 2x^{11\cdot 2^{n-1}} + x^{10\cdot 2^{n-1}} + 2x^{9\cdot 2^{n-1}} + 2x^{8\cdot 2^{n-1}} + 2x^{7\cdot 2^{n-1}} + x^{6\cdot 2^{n-1}} \\ & + 2x^{5\cdot 2^{n-1}} + 2x^{4\cdot 2^{n-1}} + 2x^{3\cdot 2^{n-1}} + x^{2\cdot 2^{n-1}} + 2x^{2^{n-1}} + 1. \end{aligned}$$

Then, writing $g(x)h(x) = Q(x) + 4E(x)$ for some $E(x) \in \mathbb{Z}[x]$, we get that

$$\begin{aligned} F(x) &= \frac{g(x)h(x) - T(x)}{2} \\ &= x^{11\cdot 2^{n-1}} + \left(\frac{1-9A}{2}\right) x^{10\cdot 2^{n-1}} + x^{9\cdot 2^{n-1}} + \left(\frac{2-(27A^2+3)}{2}\right) x^{8\cdot 2^{n-1}} \\ &\quad + x^{7\cdot 2^{n-1}} + \left(\frac{1-3B}{2}\right) x^{6\cdot 2^{n-1}} + x^{5\cdot 2^{n-1}} + \left(\frac{2-(27A^2+3)}{2}\right) x^{4\cdot 2^{n-1}} \\ &\quad + x^{3\cdot 2^{n-1}} + \left(\frac{1-9A}{2}\right) x^{2\cdot 2^{n-1}} + x^{2^{n-1}} + 2E(x). \end{aligned}$$

Hence,

$$\overline{F}(x) = \begin{cases} \left(x(x^3+x+1)(x^3+x^2+1)\Phi_5(x)\right)^{2^{n-1}} & \text{if } (\widehat{A},\widehat{B}) = (1,1), \\ (x+1)^{2^n}\left(x(x^4+x+1)(x^4+x^3+1)\right)^{2^{n-1}} & \text{if } (\widehat{A},\widehat{B}) = (3,3). \end{cases}$$

It is then apparent that $\gcd(\overline{F},\overline{g}) = 1$ in each case of $(\widehat{A},\widehat{B}) \in \Psi$, from which we conclude by Theorem 2.4 that (3.16) is valid. Therefore, $\mathcal{F}_{n+1,A,B}(x)$ is monogenic, and consequently, $\mathcal{F}_{n,A,B}(x)$ is monogenic for all $n \geq 1$ by induction. □

4. The proof of Corollary 1.2

Proof. Since the methods used in the proof are the same for both parts, we give details only for part (2). Define the polynomial $G(t) = g_1(t)g_2(2)g_3(t) \in \mathbb{Z}[t]$, where

$$\begin{aligned} g_1(t) &= 36t + 864u^2 + 1368u + 569, \\ g_2(t) &= 36t - 864u^2 - 1224u - 419 \quad \text{and} \\ g_3(t) &= 6t - 288u^3 - 648u^2 - 498u + 127. \end{aligned}$$

We wish to apply Corollary 2.9 to $G(t)$. Note that

$$\gcd(36, g_1(0)) = \gcd(36, g_2(0)) = \gcd(6, g_3(0)) = 1.$$

According to the discussion following Corollary 2.9, we only need to check for local obstructions at the primes ℓ satisfying $\ell \leq (k+2)/1 = 5/2$. That is, we only need to check the prime $\ell = 2$. Since $G(1) \equiv 2u+1 \pmod 4$, we see that there is no local obstruction at $\ell = 2$. Hence, by Corollary 2.9, there exist infinitely many primes q such that $G(q)$ is squarefree. Then $2G(q)$ is also squarefree since $g_i(q) \equiv 1 \pmod 2$ for each i. Observe that $\mathcal{D} = 2G(q)$ and $(\widehat{A},\widehat{B}) = (3,3)$ with $A = 4u+1$ and $B = 12q+7 \not\equiv 0 \pmod 3$. Thus, for any such prime q, we deduce from Theorem 1.1 that $\mathcal{F}_{n,4u+1,12q+7}(x)$ is monogenic for all $n \geq 1$. □

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, **138**, Springer-Verlag, Berlin, 2000.

[2] J. Cullinan, *The discriminant of a composition of two polynomials.* Avaliable at https://studylib.net

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

[4] N.H. Guersenzvaig, *Elementary criteria for irreducibility of* $f(X^r)$, Israel J. Math. **169** (2009), 109–123.

[5] J. Harrington and L. Jones, *Monogenic cyclotomic compositions*, arXiv preprint, 2019. Available at arXiv: 1909.03541

[6] H.A. Helfgott, *Square-free values of* $f(p)$*,* f *cubic*, Acta Math. **213** (2014), no. 1, 107–135.

[7] 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.

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

[9] L. Jones, *Reciprocal monogenic quintinomials of degree* 2^n, Bull. Aust. Math. Soc. **106** (2022), no. 3, 437–447.

[10] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss., **322** [Fundamental Principles of Mathematical Sciences], Springer-Verlag, Berlin, 1999.

[11] 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.

[12] L.C. Washington, *Introduction to Cyclotomic Fields*, Second edition, Graduate Texts in Mathematics, **83**, Springer-Verlag, New York, 1997.

Professor Emeritus
Department of Mathematics
Shippensburg University
Shippensburg
Pennsylvania 17257
USA
e-mail: lkjone@ship.edu