Bull. Aust. Math. Soc. **106** (2022), 437–447
doi:10.1017/S0004972722000193

RECIPROCAL MONOGENIC QUINTINOMIALS OF DEGREE 2^n

LENNY JONES

(Received 6 January 2022; accepted 15 January 2022; first published online 4 March 2022)

Abstract

We prove a new irreducibility result for polynomials over $\mathbb{Q}$ and we use it to construct new infinite families of reciprocal monogenic quintinomials in $\mathbb{Z}[x]$ of degree 2^n.

2020 *Mathematics subject classification*: primary 11R09; secondary 11R04, 12F05.

Keywords and phrases: reciprocal, monogenic, quintinomial, irreducible.

1. Introduction

Throughout this paper, for $f(x) \in \mathbb{Z}[x]$, when we say that '$f(x)$ is irreducible' without reference to a particular field, we mean that '$f(x)$ is irreducible over $\mathbb{Q}$'. We say that $f(x)$ is *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

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

where $\mathbb{Z}_K$ is the ring of integers of K [1]. We say that $f(x)$ is *monogenic* if $f(x)$ is irreducible and $\mathbb{Z}_K = \mathbb{Z}[\theta]$, or equivalently from (1.1), that $\Delta(f) = \Delta(K)$. In this situation, $\{1, \theta, \theta^2, \ldots, \theta^{\deg f - 1}\}$ is a basis for $\mathbb{Z}_K$, often referred to as a *power basis*. The existence of a power basis 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. Indeed, when $\Delta(f)$ is not squarefree, it can be quite difficult to determine whether $f(x)$ is monogenic.

Reciprocal monogenic quintinomials are scarce in the literature. One such infinite family of quartics can be found in [4]. More recently [9], infinite families of reciprocal monogenic quintinomials of degree 2^n, for every integer $n \geq 2$, were constructed by perturbing the middle coefficient of certain cyclotomic polynomials. In this paper, we take a different approach to construct new infinite families of reciprocal monogenic quintinomials of degree 2^n, for every integer $n \geq 2$.

Theorem 1.1. *Let $n, A, B \in \mathbb{Z}$, with $n \geq 2$ and $AB \not\equiv 0 \pmod 2$. Define the reciprocal quintinomial*

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

Suppose that $\mathcal{D} := (2A + B + 2)(2A - B - 2)(A^2 - 4B + 8)$ is squarefree, and that

$$(\widehat{A}, \widehat{B}) \in C := \{(1, 3), (3, 1), (3, 3)\},$$

where $\widehat{*} \in \{0, 1, 2, 3\}$ is the reduction modulo 4 of $*$. Then $\mathcal{F}_{n,A,B}(x)$ is monogenic for all $n \geq 2$.

Corollary 1.2. *Let C be as defined in Theorem 1.1. Then there exist infinitely many prime pairs (p, q) with $(\widehat{p}, \widehat{q}) \in C$, such that $\mathcal{F}_{n,p,q}(x)$ is monogenic for all $n \geq 2$.*

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 $f(x), g(x) \in \mathcal{R}[x]$, with the respective factorisations $f(x) = a\prod_{i=1}^{m}(x - \alpha_i) \in \overline{K}[x]$ 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*

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

Remark 2.3. As far as we can determine, Theorem 2.2 is originally due to Cullinan [2]. A proof of Theorem 2.2 can be found in [6].

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 monogeneity of a polynomial.

Theorem 2.4 (Dedekind; see [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 factorisation of $T(x)$ modulo q in $\mathbb{F}_q[x]$ and set

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

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press

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

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

The next theorem follows from [10, Corollary 2.10].

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*

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

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 2.7. Theorem 2.6 follows from the work of Helfgott [7], Hooley [8] and Pasten [11]. For more details, see [9].

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 $z \in (\mathbb{Z}/\ell^2\mathbb{Z})^*$, 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 where $C_G = 0$, 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 where each of the distinct irreducible factors of $G(t)$ is of the form $a_it + b_i$ 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 $2(\ell - 1)$.

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press

More precisely, in this minimum scenario,

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

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

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

of $G(t)$ modulo ℓ^2 [3, Theorem 4.11]. That is, $G(t)$ has exactly $\ell(\ell-1) = \phi(\ell^2)$ distinct zeros $z \in (\mathbb{Z}/\ell^2\mathbb{Z})^*$. 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 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 generalisation of a theorem of Capelli, is a special case of the results in [5], 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 [5]. *Let $w(x) \in \mathbb{Z}[x]$ be monic and irreducible, with $\deg(w) = m$. Then $w(x^{2^k})$ is reducible if and only if there exist $S_0(x), S_1(x) \in \mathbb{Z}[x]$ such that either*

$$(-1)^m w(x) = (S_0(x))^2 - x(S_1(x))^2$$

or

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

3. Proof of Theorem 1.1

For the proof of Theorem 1.1, we require some special cases of the following lemma, which is of some interest in its own right.

LEMMA 3.1. *Let $n, A, B \in \mathbb{Z}$, with $n \ge 2$, and let*

$$\mathcal{F}_{n,A,B}(x) = x^{2^n} + Ax^{3\cdot 2^{n-2}} + Bx^{2^{n-1}} + Ax^{2^{n-2}} + 1. \tag{3.1}$$

Then $\mathcal{F}_{n,A,B}(x)$ is irreducible for all $n \ge 2$ if and only if

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

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

PROOF. Suppose first that $(\widehat{A}, \widehat{B}) \in \Gamma$. Since the methods required in all cases of $(\widehat{A}, \widehat{B})$ are similar, we assume that $(\widehat{A}, \widehat{B}) = (1,3)$ and give details only for this particular case.

We begin by showing that $\mathcal{F}_{2,A,B}(x)$ is irreducible. Observe that $\mathcal{F}_{2,A,B}(1) \neq 0$ since $\mathcal{F}_{2,A,B}(1) = 2A + B + 2 \equiv 1 \pmod 2$. Similarly, $\mathcal{F}_{2,A,B}(-1) \neq 0$. Thus, $\mathcal{F}_{2,A,B}(x)$ has no

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press

zeros by the rational zero theorem. Suppose then that

$$\begin{aligned}\mathcal{F}_{2,A,B}(x) &= (x^2+ax+b)(x^2+cx+d)\\ &= x^4+(c+a)x^3+(d+ac+b)x^2+(ad+bc)x+bd,\end{aligned}$$

where $a, b, c, d \in \mathbb{Z}$. Equating coefficients yields the system of equations

$$\begin{aligned} a+c &= A,\\ ac+b+d &= B,\\ ad+bc &= A,\\ bd &= 1.\end{aligned}$$

Letting $b = d = 1$ and reducing this system modulo 4, we arrive at the system of congruences

$$\begin{aligned} a+c &\equiv 1 \pmod 4,\\ ac &\equiv 1 \pmod 4,\end{aligned}$$

which produces the insoluble congruence $c^2 \equiv 3 \pmod 4$. The situation $b = d = -1$ is also easily seen to be impossible. Hence, $\mathcal{F}_{2,A,B}(x)$ is irreducible.

Observing that $\mathcal{F}_{n,A,B}(x) = \mathcal{F}_{2,A,B}(x^{2^{n-2}})$ for $n \geq 2$, we apply Proposition 2.10 with $w(x) = \mathcal{F}_{2,A,B}(x)$ and $m = 4$. We treat separately the case $n = 3$, which corresponds to $k = 1$ in Proposition 2.10. By way of contradiction, we assume that $\mathcal{F}_{3,A,B}(x) = \mathcal{F}_{2,A,B}(x^2)$ is reducible. Then, by Proposition 2.10, there exist $S_0(x), S_1(x) \in \mathbb{Z}[x]$ such that

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

Since $\deg(\mathcal{F}_{2,A,B}) = 4$, it follows that

$$S_0(x) = x^2+ax+b \quad \text{and} \quad S_1(x) = cx+d$$

for some $a, b, c, d \in \mathbb{Z}$. Then

$$(S_0(x))^2 - x(S_1(x))^2 = x^4+(2a-c^2)x^3+(2b+a^2-2cd)x^2+(2ab-d^2)x+b^2. \tag{3.2}$$

Equating the coefficients of (3.2) and $\mathcal{F}_{2,A,B}(x)$, we arrive at the three solutions:

(1) $\{b=-1, 4a = c^2-d^2, 2A = -c^2-d^2, 16B = c^4-2c^2d^2+d^4-8cd-32\}$,
(2) $\{b = 1, c = d, A = 2a-d^2, B = a^2-2d^2+2\}$,
(3) $\{b = 1, c = -d, A = 2a-d^2, B = a^2+2d^2+2\}$.

In (1), reduction modulo 4 of the second and third equations implies that both c and d are odd. But then the fourth equation yields the contradiction

$$16B = c^4-2c^2d^2+d^4-8cd-32 \equiv 8 \pmod{16}.$$

In both (2) and (3), the third and fourth equations produce the system of congruences

$$\begin{aligned} 2a-d^2 &\equiv 1 \pmod 4,\\ a^2+2d^2 &\equiv 1 \pmod 4,\end{aligned}$$

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press

from which it is straightforward to derive the insoluble congruence $a^2 \equiv 3 \pmod 4$. Therefore, $\mathcal{F}_{3,A,B}(x)$ is irreducible.

Now suppose that $n \geq 4$, 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

$$\mathcal{F}_{3,A,B}(x) = \mathcal{F}_{2,A,B}(x^2) = (S_0(x))^2 - x(S_1(x))^2, \tag{3.3}$$

where

$$S_0(x) = x^4 + \sum_{j=0}^{3} c_j x^j \quad \text{and} \quad S_1(x) = \sum_{j=0}^{3} d_j x^j.$$

Equating coefficients in (3.3) on x and x^2, along with the constant term, yields the system of equations

$$\begin{aligned} x:&\quad 2c_0c_1 - d_0^2 = 0,\\ x^2:&\quad c_1^2 - 2d_0d_1 + 2c_0c_2 = A,\\ \text{constant term}:&\quad c_0^2 = 1. \end{aligned}$$

Examination of the equation corresponding to the coefficient on x reveals that $d_0 \equiv 0 \pmod 2$. Then reduction modulo 4 of this same equation implies that $c_1 \equiv 0 \pmod 2$, since $c_0 = \pm 1$ from the constant-term equation. Consequently, we arrive at a contradiction in the equation corresponding to x^2, since then the left-hand side is even, while the right-hand side is odd. We deduce, by Proposition 2.10, that $\mathcal{F}_{n,A,B}(x) = \mathcal{F}_{2,A,B}(x^{2^{n-2}})$ is irreducible, for all $n \geq 2$.

Finally, for the other direction of the proof, suppose that $(\widehat{A}, \widehat{B}) \notin \Gamma$. That is, assume

$$(\widehat{A}, \widehat{B}) \in \{(0,1),(0,2),(1,0),(1,1),(1,2),(2,2),(2,3),(3,0),(3,2)\}. \tag{3.4}$$

For each of these cases of $(\widehat{A}, \widehat{B}) \neq (1,1)$, 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 $n \geq 2$. For the special case of $(\widehat{A}, \widehat{B}) = (1,1)$, the example in Table 1 is irreducible for $n = 2$, but reducible for all $n \geq 3$. We let $\Phi_N(x)$ denote the cyclotomic polynomial of index N in Table 1. □

Proof of Theorem 1.1. Since $C \subset \Gamma$, it follows from Lemma 3.1 that $\mathcal{F}_{n,A,B}(x)$ is irreducible for all $n \geq 2$. A computation in Maple yields

$$\Delta(\mathcal{F}_{2,A,B}) = -(2A+B+2)(2A-B-2)(A^2-4B+8)^2. \tag{3.5}$$

Making the observation that $\mathcal{F}_{n,A,B}(x) = \mathcal{F}_{2,A,B}(x^{2^{n-2}})$ for $n \geq 2$, we then use Theorem 2.2 and Definition 2.1 to calculate

$$\begin{aligned} \Delta(\mathcal{F}_{n,A,B}) &= \Delta(\mathcal{F}_{2,A,B} \circ x^{2^{n-2}})\\ &= (-1)^{2^{n+1}(2^{n-2}-1)} \Delta(\mathcal{F}_{2,A,B})^{2^{n-2}} R(\mathcal{F}_{n,A,B}, 2^{n-2}x^{2^{n-2}-1})\\ &= 2^{2^n(n-2)} \Delta(\mathcal{F}_{2,A,B})^{2^{n-2}}\\ &= 2^{2^n(n-2)}(-(2A+B+2)(2A-B-2)(A^2-4B+8)^2)^{2^{n-2}}. \end{aligned} \tag{3.6}$$

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press

TABLE 1. Examples for (3.4) and their factorisations.

$(\widehat{A}, \widehat{B})$	(A, B)	Factorisation of $\mathcal{F}_{n,A,B}(x)$
$(0, 1)$	$(4, 5)$	$(x^{2^{n-1}} + 3x^{2^{n-2}} + 1)\Phi_3(x)\Phi_{2\cdot 3}(x)\cdots\Phi_{2^{n-2}\cdot 3}(x)$
$(0, 2)$	$(4, 2)$	$(x^{2^{n-1}} + 4x^{2^{n-2}} + 1)\Phi_{2^n}(x)$
$(1, 0)$	$(5, 8)$	$(x^{2^{n-1}} + 3x^{2^{n-2}} + 1)(\Phi_{2^{n-1}}(x))^2$
$(1, 1)$	$(1, 1)$	$\Phi_5(x)\Phi_{2\cdot 5}(x)\cdots\Phi_{2^{n-2}\cdot 5}(x)$
$(1, 2)$	$(1, 2)$	$\Phi_{2^n}(x)\Phi_3(x)\Phi_{2\cdot 3}(x)\cdots\Phi_{2^{n-2}\cdot 3}(x)$
$(2, 2)$	$(2, 2)$	$\Phi_{2^n}(x)(\Phi_{2^{n-1}}(x))^2$
$(2, 3)$	$(2, 3)$	$(\Phi_3(x)\Phi_{2\cdot 3}(x)\cdots\Phi_{2^{n-2}\cdot 3}(x))^2$
$(3, 0)$	$(3, 4)$	$(\Phi_{2^{n-1}}(x))^2\Phi_3(x)\Phi_{2\cdot 3}(x)\cdots\Phi_{2^{n-2}\cdot 3}(x)$
$(3, 2)$	$(3, 2)$	$(x^{2^{n-1}} + 3x^{2^{n-2}} + 1)\Phi_{2^n}(x)$

To establish that $\mathcal{F}_{n,A,B}(x)$ is monogenic, we begin with the case $n = 2$. Suppose that $\mathcal{F}_{2,A,B}(\theta) = 0$. We use Theorem 2.4 to show that $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$, for every prime q dividing $\mathcal{D}$, where $\mathbb{Z}_K$ is the ring of integers of $K = \mathbb{Q}(\theta)$. Because $\mathcal{D}$ is squarefree, it follows from (3.5) that no prime dividing $(2A + B + 2)(2A - B - 2)$ can divide the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Hence, we only need to focus on primes dividing $A^2 - 4B + 8$. Suppose then that q is such a prime. We apply Theorem 2.4 to q with $T(x) := \mathcal{F}_{2,A,B}(x)$. Since $B \equiv (A^2 + 8)/4 \pmod{q}$, we have

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

Then, using the quadratic formula, we see that there are three cases to consider:

(i) $\overline{\tau}(x) \equiv (x + A/4)^2 \pmod{q}$;
(ii) $\overline{\tau}(x)$ is irreducible over $\mathbb{F}_q$;
(iii) $\overline{\tau}(x) \equiv (x - (-A + w)/4)(x - (-A - w)/4) \pmod{q}$, where $w^2 \equiv A^2 - 16 \pmod{q}$.

We claim first that case (i) cannot happen. In this case, we see from the quadratic formula that $A^2 - 16 \equiv 0 \pmod{q}$. Then $B \equiv 6 \pmod{q}$ since

$$-4(B - 6) \equiv -4B + 24 \equiv A^2 - 4B + 8 \equiv 0 \pmod{q}.$$

Consequently,

$$(2A + B + 2)(2A - B - 2) = 4A^2 - B^2 - 4B - 4 \equiv 0 \pmod{q},$$

which contradicts the fact that $\mathcal{D}$ is squarefree. Therefore, case (i) is vacuous.

Suppose next that we are in case (ii). Since $A \equiv 1 \pmod{2}$, we can let

$$g(x) = h(x) = \tau(x) = x^2 + ((A + q)/2)x + 1.$$

Then

$$F(x) = \frac{g(x)h(x) - T(x)}{q}$$

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press

$$= \frac{(x^2 + ((A + q)/2)x + 1)^2 - \mathcal{F}_{2,A,B}(x)}{q}$$
$$= x\Big(x^2 + \Big(\frac{\frac{A^2-4B+8}{q} + 2A + q}{4}\Big)x + 1\Big),$$

so that

$$\overline{F}(x) = x\Big(x^2 + \Big(\frac{\overline{\big(\frac{A^2-4B+8}{q}\big) + 2A}}{4}\Big)x + 1\Big). \tag{3.7}$$

If $\gcd(\overline{g}, \overline{F}) > 1$, then, since $\overline{g}(x)$ is irreducible over $\mathbb{F}_q$, it follows that $\overline{F}(x)$ is divisible by $\overline{g}(x)$. Thus, equating coefficients on $\overline{g}(x)$ and the quadratic factor of $\overline{F}(x)$ in (3.7) yields

$$\frac{A}{2} \equiv \frac{\overline{\big(\frac{A^2-4B+8}{q}\big) + 2A}}{4} \equiv \overline{\Big(\frac{A^2 - 4B + 8}{4q}\Big)} + \frac{A}{2} \pmod{q},$$

so that

$$\overline{\Big(\frac{A^2 - 4B + 8}{4q}\Big)} \equiv 0 \pmod{q}.$$

Hence, $A^2 - 4B + 8 \equiv 0 \pmod{q^2}$, which contradicts the fact that $A^2 - 4B + 8$ is squarefree. Therefore, $\gcd(\overline{g}, \overline{F}) = 1$, which implies that $[\mathbb{Z}_K : \mathbb{Z}[\theta]] \not\equiv 0 \pmod{q}$ by Theorem 2.4, and $\mathcal{F}_{2,A,B}(x)$ is monogenic in this case.

Finally, suppose that we are in case (iii). Without loss of generality, assume that $w \equiv 0 \pmod 2$. Then

$$-A + w + \epsilon q \equiv -A - w + \epsilon q \equiv 0 \pmod 4 \quad \text{for some } \epsilon \in \{-1, 1\},$$

where the value of ϵ depends on the congruence classes of A and q modulo 4. Since both of these possibilities for ϵ are handled identically, we give details only for $\epsilon = 1$. Thus, we can let

$$g(x) = h(x) = (x - (-A + w + q)/4)(x - (-A - w + q)/4).$$

Therefore, to prove that $\gcd(\overline{F}, \overline{g}) = 1$, we only have to show $\overline{F}((-A \pm w + q)/4) \neq 0$. Because the methods are the same, we give details only for $x = (-A + w + q)/4$. Noting that $\overline{F}((-A + w + q)/4) \neq 0$ if and only if $qF((-A + w + q)/4) \not\equiv 0 \pmod{q^2}$, we examine $qF((-A + w + q)/4)$. Since $w^2 \equiv A^2 - 16 \pmod{q}$, we can write $w^2 = A^2 - 16 + qk$, for some $k \in \mathbb{Z}$. Using this substitution for w^2 and the fact that q divides $A^2 - 4B + 8$, a straightforward calculation in Maple reveals that

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press

$$\begin{aligned}256qF((-A+w+q)/4) &= -q^4-(4w+6k)q^3+(96-k^2-4kw-16B)q^2\\ &\quad -4(2A-2w-k)(A^2-4B+8)q\\ &\quad +8(A^2-Aw-8)(A^2-4B+8)\\ &\equiv 8(A^2-Aw-8)(A^2-4B+8) \pmod{q^2}.\end{aligned}$$

If $A^2-Aw-8\equiv 0 \pmod{q}$, then, since $q\equiv 1 \pmod{2}$, we see that $A\not\equiv 0 \pmod{q}$. Thus, $w\equiv (A^2-8)/A \pmod{q}$. But $w^2\equiv A^2-16 \pmod{q}$, so that

$$\left(\frac{A^2-8}{A}\right)^2 \equiv A^2-16 \pmod{q},$$

which yields the impossible congruence $64\equiv 0 \pmod{q}$. Since A^2-4B+8 is squarefree, we conclude that $qF((-A+w+q)/4)\not\equiv 0 \pmod{q^2}$, completing the proof that $\mathcal{F}_{2,A,B}(x)$ is monogenic.

For $n\geq 2$, define

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

noting that $\theta_2=\theta$ and $K_2=K$. Furthermore, observe that $\mathcal{F}_{n,A,B}(\theta_n)=0$ and that $[K_{n+1}:K_n]=2$. 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 (3.6),

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

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

$$[\mathbb{Z}_{K_{n+1}}:\mathbb{Z}[\theta_{n+1}]]\not\equiv 0 \pmod{2}. \tag{3.8}$$

We apply Theorem 2.4 with

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

Then

$$\overline{T}(x) = (x^4+x^3+x^2+x+1)^{2^{n-1}} = \Phi_5(x)^{2^{n-1}},$$

where $\Phi_5(x)$ is easily seen to be irreducible over $\mathbb{F}_2$. Therefore, we can let

$$g(x)=\Phi_5(x) \quad \text{and} \quad h(x)=\Phi_5(x)^{2^{n-1}-1}.$$

A straightforward induction argument shows that

$$g(x)h(x)\equiv x^{2^{n+1}} + 2x^{7\cdot 2^{n-2}} + 3x^{3\cdot 2^{n-1}} + x^{2^n} + 3x^{2^{n-1}} + 2x^{2^{n-2}} + 1 \pmod{4}$$

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press

for $n \geq 2$. Thus,

$$g(x)h(x) - T(x) \\ = \begin{cases} 2x^{2^{n-2}}(x^{6\cdot 2^{n-2}} + x^{5\cdot 2^{n-2}} - x^{3\cdot 2^{n-2}} + x^{2^{n-2}} + 1) + 4E_1(x) & \text{if } (\widehat{A}, \widehat{B}) = (1,3), \\ 2x^{2^{n-2}}(x^{6\cdot 2^{n-2}} + 1) + 4E_2(x) & \text{if } (\widehat{A}, \widehat{B}) = (3,1), \\ 2x^{2^{n-2}}(x^{6\cdot 2^{n-2}} - x^{3\cdot 2^{n-2}} + 1) + 4E_3(x) & \text{if } (\widehat{A}, \widehat{B}) = (3,3), \end{cases}$$

for some $E_i(x) \in \mathbb{Z}[x]$. It follows that

$$\overline{F}(x) = \overline{\frac{g(x)h(x) - T(x)}{2}} = \begin{cases} x^{2^{n-2}}(x^2 + x + 1)^{3\cdot 2^{n-2}} & \text{if } (\widehat{A}, \widehat{B}) = (1,3), \\ x^{2^{n-2}}(x+1)^{2^{n-1}}(x^2 + x + 1)^{2^{n-1}} & \text{if } (\widehat{A}, \widehat{B}) = (3,1), \\ x^{2^{n-2}}(x^6 + x^3 + 1)^{2^{n-2}} & \text{if } (\widehat{A}, \widehat{B}) = (3,3). \end{cases}$$

It is then apparent that $\gcd(\overline{F}, \overline{g}) = 1$ in each case of $(\widehat{A}, \widehat{B}) \in C$, from which we conclude by Theorem 2.4 that (3.8) holds. Hence, $\mathcal{F}_{n+1,A,B}(x)$ is monogenic, and consequently, $\mathcal{F}_{n,A,B}(x)$ is monogenic for all $n \geq 2$ by induction. □

4. Proof of Corollary 1.2

We conclude with the proof of Corollary 1.2.

PROOF. Let p be a prime with $p \equiv 3 \pmod 4$ and define the polynomial

$$G(t) := (t + 2p + 2)(t - 2p + 2)(4t - p^2 - 8) \in \mathbb{Z}[t].$$

We wish to apply Corollary 2.9 to $G(t)$. 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 $G(1) \equiv 3 \pmod 4$, 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. Thus, for any such prime q, we deduce from Theorem 1.1 that $\mathcal{F}_{n,p,q}(x)$ is monogenic for all $n \geq 2$. □

Acknowledgement

The author thanks the anonymous referee for a careful reading of this paper.

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', https://studylib.net/doc/8187082/the-discriminant-of-a-composition-of-two.

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

[4] I. Gaál, *Diophantine Equations and Power Integral Bases: Theory and Algorithms*, 2nd edn (Birkhäuser/Springer, Cham, 2019).

[5] N. Guersenzvaig, 'Elementary criteria for irreducibility of $f(x^r)$', *Israel J. Math.* **169** (2009), 109–123.
[6] J. Harrington and L. Jones, 'Monogenic cyclotomic compositions', *Kodai Math. J.* **44**(1) (2021), 115–125.
[7] H. A. Helfgott, 'Square-free values of $f(p)$, f cubic', *Acta Math.* **213**(1) (2014), 107–135.
[8] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge Tracts in Mathematics, 70 (Cambridge University Press, Cambridge, 1976).
[9] L. Jones, 'Infinite families of reciprocal monogenic polynomials and their Galois groups', *New York J. Math.* **27** (2021), 1465–1493.
[10] J. Neukirch, *Algebraic Number Theory* (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**(3) (2015), 721–737.
[12] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edn, Graduate Texts in Mathematics, 83 (Springer-Verlag, New York, 1997).

LENNY JONES, Department of Mathematics,
Shippensburg University, Shippensburg, PA 17257, USA
e-mail: lkjone@ship.edu

https://doi.org/10.1017/S0004972722000193 Published online by Cambridge University Press