New York Journal of Mathematics

New York J. Math. **27** (2021) 1465–1493.

Infinite families of reciprocal monogenic polynomials and their Galois groups

Lenny Jones

ABSTRACT. We prove a new irreducibility theorem for a particular class of polynomials, and we use it to construct infinite families of reciprocal monogenic polynomials. These results extend previous work on reciprocal sextic polynomials to reciprocal polynomials of degree $\phi\left(2^a q^b\right)$, where $q \in \{3, 5, 7\}$, and $a \geq 0$, $b \geq 1$ are integers. As an application, we construct infinite families of reciprocal monogenic polynomials with prescribed Galois group.

CONTENTS

1. Introduction

Throughout this article, for $f(x) \in \mathbb{Z}[x]$, when the words "over $\mathbb{F}$" are omitted from the statement "The polynomial $f(x)$ is irreducible over $\mathbb{F}$", it is to be understood that $\mathbb{F} = \mathbb{Q}$, unless contextual restrictions dictate otherwise. We say $f(x)$ 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 we have the well-known equation [6]

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

where $\mathbb{Z}_K$ is the ring of integers of K. We 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 $\mathbb{Z}_K$, making computations

Received January 7, 2021.
2010 *Mathematics Subject Classification.* Primary 11R04, Secondary 11R09, 12F05.
Key words and phrases. reciprocal, monogenic, Galois group, irreducible.

ISSN 1076-9803/2021

easier in $\mathbb{Z}_K$, as in the case of cyclotomic polynomials $\Phi_n(x)$ of degree $\phi(n)$ [28]. 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 $f(x)$ is monogenic and $\Delta(f)$ is not squarefree, it can be difficult to show that all square factors of $\Delta(f)$ are, in fact, factors of $\Delta(K)$.

Recently [19], the construction of infinite families of monic sextic reciprocal monogenic polynomials $f(x)$ was given, with $\mathrm{Gal}(f) \simeq D_n$, where $\mathrm{Gal}(f)$ denotes the Galois group of $f(x)$ over $\mathbb{Q}$, and D_n denotes the dihedral group of order $2n$ with $n \in \{3, 6\}$. It is the primary goal of this article to extend some of the results from [19] to larger degree polynomials. More precisely, we prove the following:

Theorem 1.1. *Let $a \geq 0$ and $b \geq 1$ be integers. Let $q \in \{3, 5, 7\}$ and let $N = 2^a q^b$. Let $r \geq 3$ be a prime such that r is a primitive root modulo q^2. Then there exist infinitely many primes p such that*

$$\mathcal{F}_{N,p}(x) := \Phi_N(x) + 4rq^2 p x^{\phi(N)/2} \text{ is monogenic,} \tag{1.2}$$

where $\Phi_N(x)$ is the cyclotomic polynomial of index N.

Remark 1.2. Theorem 1.1 can be extended to primes q with $11 \leq q \leq 211$, but this extension is conditional on the abc-conjecture for number fields.

To provide some applications of Theorem 1.1, we prove the following:

Theorem 1.3. *Let $q \in \{3, 5, 7\}$ and let $r \geq 3$ be a prime primitive root modulo q^2. Then, there exist infinitely many primes p such that, when*

I. $q = 3$,
all of $\mathcal{F}_{12,p}(x)$, $\mathcal{F}_{18,p}(x)$, $\mathcal{F}_{24,p}(x)$ and $\mathcal{F}_{36,p}(x)$ are simultaneously reciprocal monogenic polynomials with $Gal\left(\mathcal{F}_{12,p}\right) = 4\mathrm{T}2$, $Gal\left(\mathcal{F}_{18,p}\right) = 6\mathrm{T}3$, $Gal\left(\mathcal{F}_{24,p}\right) = 8\mathrm{T}9$ and $Gal\left(\mathcal{F}_{36,p}\right) = 12\mathrm{T}10$,

II. $q = 5$,
both $\mathcal{F}_{5,p}(x)$ and $\mathcal{F}_{10,p}(x)$ are simultaneously reciprocal monogenic polynomials with $Gal\left(\mathcal{F}_{5,p}\right) = Gal\left(\mathcal{F}_{10,p}\right) = 4\mathrm{T}3$,

III. $q = 7$,
   (a) *$\mathcal{F}_{7,p}(x)$ is a reciprocal monogenic polynomial with $Gal\left(\mathcal{F}_{7,p}\right) = 6\mathrm{T}11$,*
   (b) *$\mathcal{F}_{14,p}(x)$ is a reciprocal monogenic polynomial with $Gal\left(\mathcal{F}_{14,p}\right) = 6\mathrm{T}11$.*

Remark 1.4. For clarification, the infinite sets of primes for which I., II., III. (a) and III. (b) hold are not the same.

All computer computations in this article were done using either MAGMA, Maple or Sage.

2. Basic preliminaries

In this article, we make use of the "T"-notation for transitive groups as given in MAGMA and [5,10,21]. For the convenience of the reader, Table 1 gives some

common "AKA"-group names for groups isomorphic to certain "T"-notation groups. We let C_n denote the cyclic group of order n, D_n denote the dihedral group of order $2n$, and S_n denote the symmetric group on n letters of order $n!$.

T-name	AKA-names
4T2	$C_2 \times C_2$
4T3	D_4
6T3	$C_2 \times S_3, D_6$
6T11	$C_2 \times S_4, C_2 \wr S_3$
8T9	$C_2 \times D_4$
12T10	$C_2^2 \times S_3$
12T139	$(C_2 \times C_2) \wr S_3$

TABLE 1. Some common AKA group names for certain T-groups.

Lemma 2.1. [24] *Let $m \geq 1$ and $n \geq 1$ be integers. Let p be a prime with $n \equiv 0 \pmod{p}$. Then*

$$\Phi_{pn}(x) = \Phi_n(x^p).$$

Theorem 2.2. [12] *Let p be a prime such that $p \nmid n$. Let $\operatorname{ord}_n(p)$ denote the order of p modulo n. Then $\Phi_n(x)$ factors modulo p into a product of $\phi(n)/\operatorname{ord}_n(p)$ distinct irreducible polynomials, each of degree $\operatorname{ord}_n(p)$. Moreover, for any positive integer m,*

$$\Phi_{p^m n}(x) \equiv \Phi_n(x)^{\phi(p^m)} \pmod{p}.$$

Definition 2.3. [6] 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 2.4. *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 2.5. As far as we can determine, Theorem 2.4 is originally due to John Cullinan [9]. A proof of Theorem 2.4 can be found in [16].

The next two theorems are due to Capelli [27].

Theorem 2.6. *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 2.7. *Let $s \in \mathbb{Z}$ with $s \geq 2$, and let $\alpha \in \mathbb{C}$ be algebraic. Then $x^s - \alpha$ is reducible over $\mathbb{Q}(\alpha)$ if and only if either there is a prime p dividing s such that $\alpha = \beta^p$ for some $\beta \in \mathbb{Q}(\alpha)$ or $4 \mid s$ and $\alpha = -4\beta^4$ for some $\beta \in \mathbb{Q}(\alpha)$.*

The next theorem follows from Corollary (2.10) in [25].

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

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

The following theorem is sometimes refereed to in the literature as *Dedekind's Criterion*.

Theorem 2.9 (Dedekind [6])**.** *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*

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

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

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

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

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

Then

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

The following well-known theorem is also due to Dedekind.

Theorem 2.10. [8] *Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible of degree n. Let p be a prime such that $p \nmid \Delta(f)$. If $f(x)$ factors in $\mathbb{F}_p[x]$ as a product of irreducible factors of degrees $n_1, n_2, \ldots, n_t$. Then $Gal(f)$, when viewed as isomorphic to a subgroup of the symmetric group S_n, contains a permutation $\alpha_1\alpha_2 \cdots \alpha_t$, where α_i is a cycle of length n_i.*

Theorem 2.11. *Let $f(x) \in \mathbb{Z}[x]$, and suppose that $f(x)$ factors into a product of distinct irreducibles, where the largest degree of any irreducible factor of $f(x)$ is d. Define*

$$N_f(X) = \left|\{p \leq X : p \text{ is prime and } f(p) \text{ is squarefree}\}\right|$$

Then, the following asymptotic holds unconditionally if $d \leq 3$, and holds, assuming the abc-conjecture for number fields for $f(x)$, if $d \geq 4$:

$$N_f(X) \sim c_f \frac{X}{\log(X)},$$

where

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

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

Theorem 2.11 follows from work of Helfgott, Hooley and Pasten. To be more explicit, Hector Pasten has relayed to us (private communication) the following information. We consider first the unconditional part ($d \leq 3$) of Theorem 2.11. The case when $f(x)$ is a single irreducible cubic is settled in [17, Main Theorem]. Then one can use a key estimate from the proof of Helfgott's main theorem in [17], along with [26, Lemma 3.2 and Lemma 3.3] and an asymptotic formula for $N_f(X)$ from [26, p. 728], to handle the cases when $f(x)$ is a product of only cubics, only quadratics or only linear polynomials. The situation when $f(x)$ is the product of irreducibles of various degrees, all smaller than 4, is addressed in [18, Chapter 4]. The conditional part (when $d \geq 4$) of Theorem 2.11 follows from [26, Theorem 1.1].

The following immediate corollary of Theorem 2.11 is a main tool for the proof of Theorem 1.1. We require only the unconditional part here.

Corollary 2.12. *Let* $f(x) \in \mathbb{Z}[x]$*, and suppose that* $f(x)$ *factors into a product of distinct irreducibles, where the largest degree of any irreducible factor of* $f(x)$ *is* d*. To avoid the situation when* $c_f = 0$*, we suppose further that, for each prime* ℓ*, there exists some* $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$ *such that* $f(z) \not\equiv 0 \pmod{\ell^2}$*. If* $d \leq 3$*, or if* $d \geq 4$ *and assuming the abc-conjecture for number fields for* $f(x)$*, there exist infinitely many primes* p *such that* $f(p)$ *is squarefree.*

Remark 2.13. If for some prime ℓ, there does not exist $z \in \left(\mathbb{Z}/\ell^2\mathbb{Z}\right)^*$ such that $f(z) \not\equiv 0 \pmod{\ell^2}$, we say that $f(x)$ has an *obstruction* at ℓ.

Theorem 2.14. [6] *Suppose that* $\deg(f(x)) = n$*. If* $f(x)$ *is irreducible, then Gal*(f) *is isomorphic to a subgroup of the alternating group* A_n *if and only if* $\sqrt{\Delta(f)} \in \mathbb{Z}$.

Theorem 2.15. [7] *Let* q *be a prime and let* $f(x) \in \mathbb{Z}[x]$ *be a monic* q*-Eisenstien polynomial with* $\deg(f) = n$*. Let* $K = \mathbb{Q}(\alpha)$*, where* $f(\alpha) = 0$*. If* $n \not\equiv 0 \pmod{q}$*, then* $q^{n-1} || \Delta(K)$.

Definition 2.16. [23] The *Chebyshev Polynomials of the First, Second and Fourth Kind*, respectively T_n, U_n and W_n, are defined as:

$$T_0(x) = 1, \quad T_1(x) = x \quad \text{and} \quad T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \quad \text{for } n \geq 2,$$

$$U_0(x) = 1, \quad U_1(x) = 2x \quad \text{and} \quad U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x) \quad \text{for } n \geq 2,$$

$$W_0(x) = 1,\ W_1(x) = 2x + 1 \text{ and } W_n(x) = 2xW_{n-1}(x) - W_{n-2}(x) \quad \text{for } n \geq 2.$$

Definition 2.17. [22] The *Vieta Polynomials* V_n are defined as:

$$V_0(x) = 0, \quad V_1(x) = 1 \quad \text{and} \quad V_n(x) = xV_{n-1}(x) - V_{n-2}(x) \quad \text{for } n \geq 2.$$

Proposition 2.18. *Let T_n, U_n, V_n and W_n be as defined in Definitions* (2.16) *and* (2.17)*. Then*

(1) [23] $2T_n(x) = W_n(x) - W_{n-1}(x)$,

(2) [23] $W_n(x) = U_{2n}\left(\left(\frac{x+1}{2}\right)^{1/2}\right)$,

(3) [22, 23] $V_n(x) = U_{n-1}(x/2)$,

(4) [15] $V_q(x) \equiv \left(x^2-4\right)^{(q-1)/2} \pmod{q}$ *for any prime* $q \geq 3$.

Proposition 2.19. [1, 11] *Let $n \geq 2$ be an integer and let*

$$f(x) = \sum_{j=0}^{2n} a_j x^j \in \mathbb{Z}[x],$$

where $a_j = a_{2n-j}$ for all j, so that $f(x)$ is reciprocal. Define an nth degree polynomial $g(u) \in \mathbb{Z}[u]$, by

$$g(u) := a_n + 2\sum_{j=1}^{n} a_{n-j} T_j(u/2). \tag{2.1}$$

Then

$$f(x) = x^n g\left(x + x^{-1}\right). \tag{2.2}$$

The following corollary is immediate from Proposition 2.19.

Corollary 2.20. *Every zero $\rho \neq \pm 2$ of $g(u)$ corresponds to the two distinct zeros $\left(\rho \pm \sqrt{\rho^2-4}\right)\Big/ 2$ of $f(x)$. In particular, every real zero of $g(u)$ in the interval $(-2, 2)$ corresponds to a conjugate pair of distinct nonreal zeros of $f(x)$ on the unit circle. Moreover, if $g(u)$ and $f(x)$ are irreducible, it follows that Gal(g) is isomorphic to a subgroup of Gal(f).*

The following proposition is a generalization, from $\mathbb{Q}$ to an arbitrary field $\mathbb{F}$ with $\mathrm{char}(\mathbb{F}) \neq 2$, of some special cases of results in [3].

Proposition 2.21. *Let $\mathbb{F}$ be a field with* $\mathrm{char}(\mathbb{F}) \neq 2$.

(1) Let $f(x) = x^4 + cx^2 + 1 \in \mathbb{F}[x]$. Then $f(x)$ is reducible over $\mathbb{F}$ if and only if at least one of

$$c^2 - 4, \quad -c+2 \quad \text{or} \quad -c-2$$

is a square in $\mathbb{F}$.

(2) Let $f(x) = x^4 + bx^3 + cx^2 + bx + 1 \in \mathbb{F}[x]$, with $b \neq 0$. Then $f(x)$ factors over $\mathbb{F}$ into the product of two irreducible quadratics if and only if at least one of

$$8 + b^2 - 4c, \quad b^2 - 2c - 4 - 2\sqrt{4 - 4b^2 + 4c + c^2} \quad \text{or}$$
$$b^2 - 2c - 4 + 2\sqrt{4 - 4b^2 + 4c + c^2}$$

is a square in $\mathbb{F}$.

The next proposition is a special case of the results in [13].

Proposition 2.22. [13] *Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible, with* $\deg(f) = m$. *Then $f\left(x^{2^s}\right)$ is reducible if and only if there exist $S_0(x), S_1(x) \in \mathbb{Z}[x]$ such that either*

$$(-1)^m f(x) = (S_0(x))^2 - x\,(S_1(x))^2, \tag{2.3}$$

or

$$s \geq 2 \text{ and } f\left(x^2\right) = (S_0(x))^2 - x\,(S_1(x))^2. \tag{2.4}$$

Theorem 2.23. [20] *Let $f(x) = x^4 + bx^2 + d \in \mathbb{Q}[x]$ be irreducible. Then*

(1) $Gal(f) \simeq C_2 \times C_2 \iff \sqrt{d} \in \mathbb{Q}$
(2) $Gal(f) \simeq C_4 \iff \sqrt{d\,(b^2 - 4d)} \in \mathbb{Q}$
(3) $Gal(f) \simeq D_4 \iff \sqrt{d} \notin \mathbb{Q}$ and $\sqrt{d\,(b^2 - 4d)} \notin \mathbb{Q}$.

Proposition 2.24. [14] *Let $H(x) = x^3 + ax^2 + bx - c^2 \in \mathbb{Z}[x]$ be irreducible. Then $h(x) = x^6 + ax^4 + bx^2 - c^2$ is reducible if and only if $\widehat{h}(x) = x^4 + 2ax^2 - 8cx + a^2 - 4b$ has exactly one integer zero.*

Theorem 2.25. [14] *Let $f(x) = x^6 + bx^3 + c^3 \in \mathbb{Z}[x]$ be irreducible, and let $g(x) = x^3 - 3cx - b$. Then*

$$Gal(f) \simeq \begin{cases} C_2 \times S_3 & \text{if } \sqrt{\Delta(g)} \notin \mathbb{Z} \\ C_6 & \text{if } \sqrt{\Delta(g)} \in \mathbb{Z}. \end{cases}$$

Remark 2.26. If $c = 1$ in Theorem 2.25, then $f(x)$ is reciprocal, and $g(x)$ is precisely the polynomial $g(u)$ in (2.1).

The following theorem follows from Algorithm 2.3 in [2].

Theorem 2.27. [2] *Let $f(x) = x^6 + ax^4 + bx^2 + c \in \mathbb{Z}[x]$ be irreducible. Let $h(x) = x^6 - bx^4 + acx^2 - c^2$ and let $d = a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2$. Suppose that none of $-c$, d and $-cd$ is a square in $\mathbb{Z}$.*

(1) If $h(x)$ is reducible, then $Gal(f) =$ 6T3.
(2) If $h(x)$ is irreducible, then $Gal(f) =$ 6T11.

3. More preliminaries: new results

We require the following additional new machinery for the proof of Theorem 1.1. Throughout this section, we let

$$\mathcal{F}_{N,t}(x) := \Phi_N(x) + 4ktx^{\phi(N)/2}, \tag{3.1}$$

where $N = 2^a q^b$, $q \geq 3$ is prime, $a \geq 0$ and $b \geq 1$ are integers, k is some prescribed nonzero integer constant, and t is an indeterminate. The first lemma is of interest in its own right.

Lemma 3.1. *Let $r \geq 3$ be a prime that is a primitive root modulo q^2, where $q \geq 3$ is prime. Let $k = r$ in* (3.1). *Then $\mathcal{F}_{N,t}(x)$ is irreducible for all integer values of t.*

Proof. We consider two cases: $0 \leq a \leq 1$ and $a \geq 2$. Suppose first that $0 \leq a \leq 1$, so that $N = q^b$ or $N = 2q^b$. Observe that

$$\mathcal{F}_{N,t}(x) \equiv \Phi_N(x) \pmod{r}.$$

Since r is odd and r is a primitive root modulo q^2, then r is a primitive root modulo q^b and $2q^b$ for all integers $b \geq 1$ [4]. Thus, it follows from Theorem 2.2 that $\mathcal{F}_{N,t}(x)$ is irreducible over $\mathbb{F}_r$, and therefore, also irreducible over $\mathbb{Q}$.

Suppose now that $a \geq 2$. By Lemma 2.1, we have that

$$\mathcal{F}_{2^a q^b,t}(x) = \mathcal{F}_{2q^b,t}\left(x^{2^{a-1}}\right).$$

Since we have shown that $\mathcal{F}_{2q^b,t}(x)$ is irreducible, we can use Proposition 2.22 to show that $\mathcal{F}_{2^a q^b,t}(x)$ is irreducible. We assume that $\mathcal{F}_{2^a q^b,t}(x)$ is reducible and show that the assumption of either condition (2.3) or (2.4) leads to a contradiction. For both arguments, we let $S_0(x) \in \mathbb{Z}[x]$ and $S_1(x) \in \mathbb{Z}[x]$, where

$$S_0(x) = x^{\phi(N)/2} + \sum_{j=0}^{\phi(N)/2-1} c_j x^j \quad \text{and} \quad S_1(x) = \sum_{j=0}^{\phi(N)/2-1} d_j x^j, \tag{3.2}$$

with $N = 2q^b$ assuming (2.3) holds, and $N = 4q^b$ assuming (2.4) holds.

We assume first that (2.3) holds. Noting that $\deg\left(\mathcal{F}_{2q^b,t}(x)\right) = \phi\left(2q^b\right) \equiv 0 \pmod 2$ and using (3.2), we have that

$$\mathcal{F}_{2q^b,t}(x) = \Phi_{2q^b}(x) + 4rtx^{q^{b-1}(q-1)/2} = \left(S_0(x)\right)^2 - x\left(S_1(x)\right)^2. \tag{3.3}$$

Then,

$$\begin{aligned}
\mathcal{F}_{2q^b,t}(x) &\equiv \Phi_{2q^b}(x) \pmod 2 \\
&= \Phi_{2q}\left(x^{q^{b-1}}\right) \quad \text{(by Lemma 2.1)} \\
&\equiv x^{(q-1)q^{b-1}} + x^{(q-2)q^{b-1}} + \cdots + x^{2q^{b-1}} + x^{q^{b-1}} + 1 \pmod 2, \quad (3.4)
\end{aligned}$$

and

$$\begin{aligned}
\left(S_0(x)\right)^2 - x\left(S_1(x)\right)^2 &\equiv x^{\phi(N)} + \sum_{j=0}^{\phi(N)/2-1} c_j^2 x^{2j} + \sum_{j=0}^{\phi(N)/2-1} d_j^2 x^{2j+1} \pmod 2 \\
&= x^{\phi(N)} + d_{\phi(N)/2-1}^2 x^{\phi(N)-1} + c_{\phi(N)/2-1}^2 x^{\phi(N)-2} + \quad (3.5) \\
&\qquad \cdots + d_2^2 x^5 + c_2^2 x^4 + d_1^2 x^3 + c_1 x^2 + d_0^2 x + c_0^2,
\end{aligned}$$

where $N = 2q^b$. Let

$$\begin{aligned}
J &= \{0, 1, \ldots, \phi(N)/2 - 1\} = \left\{0, 1, \ldots, (q-1)q^{b-1}/2 - 1\right\}, \\
J_c &= \left\{0, q^{b-1}, 2q^{b-1}, \ldots, (q-3)q^{b-1}/2\right\} \text{ and} \\
J_d &= \left\{(q^{b-1}-1)/2, (3q^{b-1}-1)/2, \ldots, ((q-2)q^{b-1}-1)/2\right\}.
\end{aligned}$$

Then, equating coefficients in (3.11) and (3.5), yields:

$$\begin{aligned} c_j &\equiv 1 \pmod 2 \quad \text{if } j \in J_c, \\ c_j &\equiv 0 \pmod 2 \quad \text{if } j \in J \setminus J_c, \\ d_j &\equiv 1 \pmod 2 \quad \text{if } j \in J_d, \\ d_j &\equiv 0 \pmod 2 \quad \text{if } j \in J \setminus J_d. \end{aligned} \tag{3.6}$$

Now we equate coefficients in

$$(S_0(x))^2 - x\,(S_1(x))^2 = \mathcal{F}_{2q^b,t}\,(x)\,, \tag{3.7}$$

and focus on the coefficient C of x^n, where $n = q^{b-1}$. We define $c_n := 1$, when $q = 3$. Then, using (3.6), this computation reveals, for the left-hand side of (3.7), that

$$C = 2\left(\sum_{j=0}^{(n-1)/2} c_j c_{n-j} - \sum_{j=0}^{(n-3)/2} d_j d_{n-1-j}\right) - d_{(n-1)/2}^2 \equiv 2c_0c_n - 1 \pmod 4, \tag{3.8}$$

while for the right-hand side of (3.7), we get

$$C = \begin{cases} 4rt - 1 & \equiv -1 \pmod 4 \quad \text{if } q = 3 \\ -1 & \equiv -1 \pmod 4 \quad \text{if } q \geq 5. \end{cases} \tag{3.9}$$

Combining (3.8) and (3.9), we deduce that

$$2c_0c_n \equiv 0 \pmod 4,$$

which is impossible, since $c_0 \equiv c_n \equiv 1 \pmod 2$. Thus, $\mathcal{F}_{2^aq^b,t}(x)$ is irreducible if $a = 2$.

Suppose then that $a \geq 3$ and assume condition (2.4) holds. Then

$$\begin{aligned} \mathcal{F}_{2q^b,t}\left(x^2\right) &= \Phi_{2q^b}\left(x^2\right) + 4rt\left(x^2\right)^{q^{b-1}(q-1)/2} \\ &= \Phi_{4q^b}\left(x\right) + 4rtx^{q^{b-1}(q-1)} \text{ (by Lemma 2.1)} \\ &= (S_0(x))^2 - x\,(S_1(x))^2\,. \end{aligned} \tag{3.10}$$

Thus, from (3.10) and Lemma 2.1, we have that

$$\begin{aligned} \mathcal{F}_{2q^b,t}\left(x^2\right) &\equiv \Phi_{2q^b}\left(x^2\right) \pmod 2 \\ &\equiv \Phi_q\left(x^{2q^{b-1}}\right) \pmod 2 \\ &\equiv x^{2q^{b-1}(q-1)} + x^{2q^{b-1}(q-2)} + \cdots + x^{2q^{b-1}} + 1 \pmod 2. \end{aligned} \tag{3.11}$$

Let

$$J = \{0, 1, \ldots, \phi(N)/2 - 1\} = \left\{0, 1, \ldots, (q-1)q^{b-1} - 1\right\}$$

and

$$\widehat{J} = \left\{0, q^{b-1}, 2q^{b-1}, \ldots, (q-2)q^{b-1}\right\}.$$

Then, equating coefficients in (3.11) and (3.5) with $N = 4q^b$, yields:

$$\begin{aligned} d_j &\equiv 0 \pmod 2 \quad \text{for all } j \in J, \\ c_j &\equiv 1 \pmod 2 \quad \text{for all } j \in \widehat{J}, \\ c_j &\equiv 0 \pmod 2 \quad \text{for all } j \in J \setminus \widehat{J}. \end{aligned} \tag{3.12}$$

As in the previous argument, we equate coefficients in

$$(S_0(x))^2 - x\,(S_1(x))^2 = \mathcal{F}_{2q^b,t}\left(x^2\right) = \mathcal{F}_{4q^b,t}(x), \tag{3.13}$$

and focus on the coefficient C of x^n, where $n = q^{b-1}$. For the left-hand side of (3.13), using (3.12) we get that

$$C = 2\left(\sum_{j=0}^{(n-1)/2} c_j c_{n-j} - \sum_{j=0}^{(n-3)/2} d_j d_{n-1-j}\right) - d_{(n-1)/2}^2 \equiv 2c_0c_n \pmod 4,$$

while for the right-hand side of (3.13), we see that $C = 0$. Then, since $c_0 \equiv c_n \equiv 1 \pmod 2$, we arrive at the same contradiction as in the previous case. Hence, $\mathcal{F}_{2^a q^b,t}(x)$ is irreducible for any integer t. □

We require formulas for $\Delta(\mathcal{F}_{N,t})$ in the indeterminate t, where $N \in \{q, 2q\}$ and $k = rq^2$ in (3.1). Later, we will set r equal to an odd prime that is a primitive root modulo q^2, but for now, r can be thought of as an arbitrary nonzero constant. We use (2.1) in Proposition 2.19 to construct the polynomials $g_a(u)$, with $a \in \{0, 1\}$, corresponding respectively to the reciprocal polynomials $\mathcal{F}_{2^a q,t}(x)$, with $a \in \{0, 1\}$:

$$g_a(u) = \begin{cases} 4rq^2t + 1 + 2\displaystyle\sum_{j=1}^{(q-1)/2} T_j(u/2) & \text{if } a = 0 \\ 4rq^2t + (-1)^{(q-1)/2}\left(1 + 2\displaystyle\sum_{j=1}^{(q-1)/2} (-1)^j T_j(u/2)\right) & \text{if } a = 1. \end{cases} \tag{3.14}$$

Lemma 3.2. *Let $g_a(u)$ be as in* (3.14)*. Then $g_0(u+2)$ and $g_1(u-2)$ are q-Eisenstein. Consequently, $g_a(u)$ is irreducible for all integers t.*

Proof. We first consider $g_0(u)$. Define

$$\gamma_0(u) := 1 + \sum_{j=1}^{(q-1)/2} 2T_j(u/2),$$

so that $g_0(u) = 4rq^2t + \gamma_0(u)$. Then, by Proposition 2.18, we have that

$$\begin{aligned}\gamma_0(u) &= 1 + \sum_{j=1}^{(q-1)/2} \left(W_j(u/2) - W_{j-1}(u/2)\right) \\ &= 1 + W_{(q-1)/2}(u/2) - W_0(u/2) \\ &= W_{(q-1)/2}(u/2) \\ &= U_{q-1}\left(\frac{(u+2)^{1/2}}{2}\right) \\ &= V_q\left((u+2)^{1/2}\right) \\ &\equiv (u-2)^{(q-1)/2} \pmod{q}.\end{aligned} \tag{3.15}$$

Hence, noting that $V_q(2) = q$, we deduce from (3.15) that

$$g_0(2) = 4rq^2t + \gamma_0(2) = 4rq^2t + V_q(2) = 4rq^2t + q \equiv q \pmod{q^2},$$

and

$$g_0(u+2) \equiv u^{(q-1)/2} \pmod{q}.$$

Thus, $g_0(u+2)$ is q-Eisenstein and $g_0(u)$ is irreducible.

To examine $g_1(u)$, define

$$\gamma_1(u) := 1 + \sum_{j=1}^{(q-1)/2} (-1)^j 2T_j(u/2),$$

so that $g_1(u) = 4rq^2t + (-1)^{(q-1)/2}\gamma_1(u)$. Since $T_n(x)$ is an even function if n is even, and an odd function if n is odd [23], it follows that

$$\gamma_1(u) = 1 + \sum_{j=1}^{(q-1)/2} 2T_j(-u/2).$$

Then, using Proposition 2.18 and proceeding as in (3.15) yields

$$\gamma_1(u) = V_q\left((-u+2)^{1/2}\right) \equiv (-1)^{(q-1)/2}(u+2)^{(q-1)/2} \pmod{q}.$$

Therefore,

$$\begin{aligned}g_1(-2) &= 4rq^2t + (-1)^{(q-1)/2}\gamma_1(-2) \\ &= 4rq^2t + (-1)^{(q-1)/2}V_q(2) \\ &= 4rq^2t + (-1)^{(q-1)/2}q \\ &\equiv (-1)^{(q-1)/2}q \pmod{q^2},\end{aligned}$$

and

$$g_1(u-2) \equiv (-1)^{(q-1)/2}u^{(q-1)/2} \pmod{q}.$$

Thus, $g_1(u-2)$ is q-Eisenstein and $g_1(u)$ is irreducible. □

Based on computer calculations, we make the following conjecture.

Conjecture 3.3. *Let $q \geq 3$ be prime. Let $N = 2^a q$, with $a \in \{0, 1\}$, and $k = rq^2$ in* (3.1)*, where r is an arbitrary nonzero constant. Then*

$$\Delta\left(\mathcal{F}_{2^a q,t}\right) = \begin{cases} q(4qrt+1)\left(4q^2rt + (-1)^{(q-1)/2}\right)\Delta\left(g_0\right)^2 & \text{if } a = 0 \\ q\left(4qrt + (-1)^{(q-1)/2}\right)\left(4q^2rt+1\right)\Delta\left(g_1\right)^2 & \text{if } a = 1, \end{cases} \tag{3.16}$$

where

$$\Delta\left(g_a\right) = q^{(q-3)/2} h_a\left(t\right), \tag{3.17}$$

such that $h_a(t)$ has content 1, $h_a(t) = 1$ if $q = 3$, and $h_a(t) \in \mathbb{Z}[t]$ is irreducible with $\deg(h_a) = (q-3)/2$, if $q \geq 5$.

We then have the following result, which is conditional on Conjecture 3.3.

Theorem 3.4. *Let $q \geq 3$ be prime, and let $r \geq 3$ be a prime that is a primitive root modulo q^2. Let $\mathcal{F}_{2^a q^b,t}(x)$ be as in* (3.1)*, with $k = rq^2$, and let $g_0(u)$ and $g_1(u)$ be as in* (3.14)*. Assume Conjecture* 3.3 *is true, with $h_0(t)$ and $h_1(t)$ as in* (3.17)*. Define*

$$\begin{aligned} \mathcal{B}_q(t) &:= (4qrt+1)\left(4q^2rt + (-1)^{(q-1)/2}\right)h_0(t) \\ \mathcal{C}_q(t) &:= \left(4qrt + (-1)^{(q-1)/2}\right)\left(4q^2rt+1\right)h_1(t), \quad \text{and} \end{aligned} \tag{3.18}$$

$$\mathcal{A}_q(t) := \operatorname{lcm}\left(\mathcal{B}_q(t), \mathcal{C}_q(t)\right). \tag{3.19}$$

If there exists an integer t_1 such that $\mathcal{B}_q(t_1)$ is squarefree, then $g_0(u)$ is monogenic, and $\mathcal{F}_{q^b,t}(x)$ is monogenic for all integers $b \geq 1$. If there exists an integer t_2 such that $\mathcal{C}_q(t_2)$ is squarefree, then $g_1(u)$ is monogenic, and $\mathcal{F}_{2^a q^b,t}(x)$ is monogenic for all integers $a \geq 1$ and $b \geq 1$. Consequently, if there exists an integer t (i.e. $t_1 = t_2$) such that $\mathcal{A}_q(t)$ is squarefree, then $g_0(u)$ and $g_1(u)$ are monogenic, and furthermore, $\mathcal{F}_{2^a q^b,t}(x)$ is monogenic for all integers $a \geq 0$ and $b \geq 1$.

Proof. We present the proof for the situation when there exists an integer t such that $\mathcal{A}_q(t)$ is squarefree. We omit the proof for the situation assuming the weaker condition that $t_1 \neq t_2$, since it is similar.

We show first that $g_0(u)$ is monogenic. By Lemma 3.2, $g_0(u)$ is irreducible. Let $g_0(\alpha) = 0$, $K = \mathbb{Q}(\alpha)$ and $\mathbb{Z}_K$ be the ring of integers of K. Since $\mathcal{A}_q(t)$ is squarefree, we know that $h_0(t)$ is squarefree. Therefore, by (3.17), to prove that $g_0(u)$ is monogenic, it is enough to show that $q \nmid \left[\mathbb{Z}_K : \mathbb{Z}[\alpha]\right]$. Note that $\deg(g_0) = (q-1)/2 \not\equiv 0 \pmod{q}$. Since $g_0(u+2)$ is q-Eisenstein by Lemma 3.2, it follows from Theorem 2.15 that $q^{(q-1)/2-1} = q^{(q-3)/2} || \Delta(K)$. Hence, $\Delta(K) = \Delta(g_0)$, and $g_0(u)$ is monogenic. The argument to show that $g_1(u)$ is monogenic is similar, and we omit it.

We now show that $\mathcal{F}_{2^a q^b,t}(x)$ is monogenic by considering several cases. Note, by Lemma 3.1, $\mathcal{F}_{2^a q^b,t}(x)$ is irreducible for all $t \in \mathbb{Z}$. We consider first the case

$(a,b)=(0,1)$. Suppose that $\mathcal{F}_{q,t}(\theta)=0$, and let $L=\mathbb{Q}(\theta)$. By Corollary 2.20, $K\subset L$. Hence, by Theorem 2.8 and (3.17), we have that

$$\Delta(K)^{[L:K]}=\Delta\left(g_0\right)^2=q^{q-3}h_0(t)^2\;\big|\;\Delta(L).$$

Since $\mathcal{A}_q$ is squarefree, it follows from (3.16) that $\Delta\left(\mathcal{F}_{q,t}\right)=\Delta(L)$, so that $\mathcal{F}_{q,t}(x)$ is monogenic. A similar argument handles the case $(a,b)=(1,1)$.

Next, we need to calculate $\left|\Delta\left(\mathcal{F}_{2^aq^b,t}\right)\right|$ when $(a,b)\notin\{(0,1),(1,1)\}$. Suppose first that $a\geq 1$. By Lemma 2.1,

$$\mathcal{F}_{2^aq^b,t}(x)=\mathcal{F}_{2q,t}\left(x^{2^{a-1}q^{b-1}}\right)=\left(\mathcal{F}_{2q,t}\circ G\right)(x),$$

where

$$G(x)=x^{2^{a-1}q^{b-1}}.$$

Then, by Theorem 2.4 and Definition 2.3, we have that

$$\begin{aligned}\left|\Delta\left(\mathcal{F}_{2^aq^b,t}\right)\right|&=\left|\Delta\left(\mathcal{F}_{2q,t}\right)^{2^{a-1}q^{b-1}}R\left(\mathcal{F}_{2q,t}\circ G,G'\right)\right|\\&=\left|\Delta\left(\mathcal{F}_{2q,t}\right)^{2^{a-1}q^{b-1}}\left(2^{a-1}q^{b-1}\right)^{\phi\left(2^aq^b\right)^{2^{a-1}q^{b-1}-1}}\prod_{i=1}^{2^{a-1}q^{b-1}-1}\mathcal{F}_{2^aq^b,t}(0)\right|\\&=\left|\Delta\left(\mathcal{F}_{2q,t}\right)^{2^{a-1}q^{b-1}}\left(2^{a-1}q^{b-1}\right)^{\phi\left(2^aq^b\right)}\right|.\end{aligned}$$

The case $a=0$ is similar, and we omit the details. To summarize, we have that

$$\left|\Delta\left(\mathcal{F}_{2^aq^b,t}\right)\right|=\begin{cases}\left|\Delta\left(\mathcal{F}_{q,t}\right)^{q^{b-1}}\left(q^{b-1}\right)^{\phi\left(q^b\right)}\right| & \text{if } a=0\\ \left|\Delta\left(\mathcal{F}_{2q,t}\right)^{2^{a-1}q^{b-1}}\left(2^{a-1}q^{b-1}\right)^{\phi\left(2^aq^b\right)}\right| & \text{if } a\geq 1.\end{cases}\tag{3.20}$$

We focus now on the cases when $a\geq 2$ and $b\geq 2$, so that the powers of 2 and q do not vanish in (3.20). The remaining cases are similar and we omit the details. Suppose that $\mathcal{F}_{2^aq^b,t}(\theta)=0$. Then $\mathcal{F}_{2q,t}\left(\theta^{2^{a-1}q^{b-1}}\right)=0$. Let

$$K=\mathbb{Q}\left(\theta^{2^{a-1}q^{b-1}}\right)\quad\text{and}\quad L=\mathbb{Q}(\theta).$$

Then

$$K\subset L\quad\text{and}\quad[L:K]=2^{a-1}q^{b-1}.$$

Since $\mathcal{F}_{2q,t}(x)$ is monogenic, we have that $\Delta\left(\mathcal{F}_{2q,t}\right)=\Delta(K)$. Thus, by Theorem 2.8, it follows that

$$\Delta\left(\mathcal{F}_{2q,t}\right)^{2^{a-1}q^{b-1}}\Big|\Delta\left(L\right).\tag{3.21}$$

Also, from (1.1) and (3.20), we have that

$$\left|\Delta\left(\mathcal{F}_{2q,t}\right)^{2^{a-1}q^{b-1}}\left(2^{a-1}q^{b-1}\right)^{\phi\left(2^aq^b\right)}\right|=\left[\mathbb{Z}_L:\mathbb{Z}[\theta]\right]^2\cdot\left|\Delta(L)\right|.\tag{3.22}$$

Thus, we conclude from (3.21) and (3.22) that to prove $\mathcal{F}_{2^aq^b,t}(x)$ is monogenic, it is enough to show that

$$[\mathbb{Z}_L : \mathbb{Z}[\theta]] \not\equiv 0 \pmod 2 \quad \text{and} \quad [\mathbb{Z}_L : \mathbb{Z}[\theta]] \not\equiv 0 \pmod q. \tag{3.23}$$

To establish (3.23), we use Theorem 2.9 with $T := \mathcal{F}_{2^aq^b,t}(x)$. By Theorem 2.2, we have that

$$\Phi_{2^aq^b}(x) \equiv \begin{cases} \Phi_{q^b}(x)^{\phi(2^a)} \pmod 2 \\ \Phi_{2^a}(x)^{\phi(q^b)} \pmod q. \end{cases} \tag{3.24}$$

We examine the prime 2 first. By Theorem 2.2,

$$\Phi_{q^b}(x) \equiv \prod_{i=1}^{\phi(q^b)/\operatorname{ord}_{q^b}(2)} \gamma_i(x) \pmod 2, \tag{3.25}$$

where $\gamma_i(x)$ is irreducible over $\mathbb{F}_2$ and $\deg(\gamma_i) = \operatorname{ord}_{q^b}(2)$. Thus, in Theorem 2.9, we may let

$$g(x) = \prod_{i=1}^{\phi(q^b)/\operatorname{ord}_{q^b}(2)} \gamma_i(x) \quad \text{and} \quad g(x)h(x) = \left(\prod_{i=1}^{\phi(q^b)/\operatorname{ord}_{q^b}(2)} \gamma_i(x) \right)^{\phi(2^a)}.$$

By (3.25), we may write

$$g(x) = \Phi_{q^b}(x) + 2\rho(x) = \frac{x^{q^b}-1}{x^{q^{b-1}}-1} + 2\rho(x),$$

where $\rho(x) \in \mathbb{Z}[x]$. Define

$$F_a(x) := \frac{g(x)^{2^{a-1}} - \mathcal{F}_{2^aq^b,t}(x)}{2} = \frac{g(x)^{2^{a-1}} - \left(\Phi_{2q^b}\left(x^{2^{a-1}}\right) + 4rq^2t\left(x^{2^{a-1}}\right)^{\phi(q^b)/2} \right)}{2}.$$

Since

$$g(x)^{2^a} \equiv g\left(x^2\right)^{2^{a-1}} \pmod 4 \quad \text{for } a \geq 2,$$

it follows that

$$\begin{aligned} 2F_{a+1}(x) &= g(x)^{2^a} - \left(\Phi_{2q^b}\left(x^{2^a}\right) + 4rq^2t\left(x^{2^a}\right)^{\phi(q^b)/2} \right) \\ &\equiv g\left(x^2\right)^{2^{a-1}} - \left(\Phi_{2q^b}\left(\left(x^2\right)^{2^{a-1}}\right) + 4rq^2t\left(\left(x^2\right)^{2^{a-1}}\right)^{\phi(q^b)/2} \right) \pmod 4 \\ &= 2F_a\left(x^2\right), \end{aligned}$$

for $a \geq 2$. Hence,

$$F_{a+1}(x) \equiv F_a\left(x^2\right) \equiv F_a(x)^2 \pmod 2 \quad \text{for } a \geq 2.$$

Consequently, to show that $\gcd\left(\overline{F_a}, \overline{g}\right) = 1$ for all $a \geq 2$, it is enough to show that $\gcd\left(\overline{F_2}, \overline{g}\right) = 1$. Straightforward computations show that

$$\begin{aligned} F_2(x) &= \frac{\Phi_{q^b}(x)^2 - \Phi_{2q^b}\left(x^2\right)}{2} + 2E(x) \\ &= \frac{\left(\dfrac{x^{q^b}-1}{x^{q^{b-1}}-1}\right)^2 - \left(\dfrac{x^{2q^b}+1}{x^{2q^{b-1}}+1}\right)}{2} + 2E(x) \\ &= \frac{x^{q^{b-1}}\left(\left(x^{q^{b-1}}\right)^{q+1}-1\right)\left(\left(x^{q^{b-1}}\right)^{q-1}-1\right)}{\left(x^{q^{b-1}}-1\right)^2\left(x^{2q^{b-1}}+1\right)} + 2E(x), \end{aligned}$$

where

$$E(x) = \rho(x)\Phi_{q^b}(x) + \rho(x)^2 - rq^2t\left(x^2\right)^{\phi(q^b)/2}.$$

Hence,

$$\overline{F_2}(x) = \frac{x^{q^{b-1}}\left(\left(x^{q^{b-1}}\right)^{q+1}-1\right)\left(\left(x^{q^{b-1}}\right)^{q-1}-1\right)}{\left(x^{q^{b-1}}-1\right)^2\left(x^{2q^{b-1}}+1\right)}. \tag{3.26}$$

Suppose that $\overline{g}(\alpha) = 0$, where α is an element of some algebraic closure $\mathcal{K}$ of $\mathbb{F}_2$. Then the order of α in $\mathcal{K}$ is q^b, and it is easy to see from (3.26) that $\overline{F_2}(\alpha) \neq 0$ in $\mathcal{K}$, from which we conclude that $\gcd\left(\overline{F_2}, \overline{g}\right) = 1$.

We now examine the prime q. Using (3.24) and proceeding as in the examination of the prime 2, we may take

$$g(x) = \Phi_{2^a}(x) + q\rho(x),$$

where $\rho(x) \in \mathbb{Z}[x]$. Then

$$\begin{aligned} F &= \frac{g(x)^{\phi(q^b)} - \mathcal{F}_{2^aq^b,t}(x)}{q} \\ &= \frac{\Phi_{2^a}(x)^{\phi(q^b)} - \Phi_{2^aq^b}(x) + \sum_{j=1}^{\phi(q^b)} \Phi_{2^a}(x)^{\phi(q^b)-j}\left(q\rho(x)\right)^j - 4rq^2tx^{\phi(2^aq^b)/2}}{q}. \end{aligned}$$

Thus, by Theorem 2.2, and the fact that $b \geq 2$, we have that

$$\begin{aligned} q\overline{F}(x) &= \Phi_{2^a}(x)^{\phi(q^b)} - \Phi_{2q}\left(x^{2^{a-1}q^{b-1}}\right) \\ &= \left(x^{2^{a-1}}\right)^{\phi(q^b)} + 1 + \sum_{j=1}^{\phi(q^b)-1} \binom{\phi\left(q^b\right)}{j} \left(x^{2^{a-1}}\right)^j \\ &\qquad - \left(\left(x^{2^{a-1}q^{b-1}}\right)^{q-1} + 1 + \sum_{j=1}^{q-2} (-1)^j \left(x^{2^{a-1}q^{b-1}}\right)^{q-1-j}\right) \\ &= \sum_{j=1}^{\phi(q^b)-1} \binom{\phi\left(q^b\right)}{j} \left(x^{2^{a-1}}\right)^j - \sum_{j=1}^{q-2} (-1)^j \left(x^{2^{a-1}q^{b-1}}\right)^{q-1-j}. \end{aligned}$$

Suppose that $\zeta^{2^{a-1}} + 1 = 0$ for some $\zeta \in \mathcal{K}$, an algebraic closure of $\mathbb{F}_q$. Then, in $\mathcal{K}$, we have that

$$0 = \Phi_{2^a}(\zeta)^{\phi(q^b)} = (-1)^{\phi(q^b)} + 1 + \sum_{j=1}^{\phi(q^b)-1} \binom{\phi\left(q^b\right)}{j} (-1)^j,$$

and hence,

$$\sum_{j=1}^{\phi(q^b)-1} \binom{\phi\left(q^b\right)}{j} (-1)^j = -2.$$

Thus,

$$\begin{aligned} q\overline{F}(\zeta) &= \sum_{j=1}^{\phi(q^b)-1} \binom{\phi\left(q^b\right)}{j} (-1)^j - \sum_{j=1}^{q-2} (-1)^{q-1} \\ &= -2 - (q-2) \\ &= -q, \end{aligned}$$

so that $\overline{F}(\zeta) = -1$. Therefore, $\gcd\left(\overline{g}, \overline{F}\right) = 1$ and $\mathcal{F}_{2^a q^b, t}(x)$ is monogenic. □

Using a computer, we have verified that Conjecture 3.3 is true for all primes q with $3 \leq q \leq 211$. Nevertheless, for an unconditional version of Theorem 3.4 for these primes, the question still remains as to whether there exist infinitely many prime values of t such that $\mathcal{F}_{2^a q^b, t}(x)$ is monogenic. To accomplish this task, we must show that either there exist infinitely many primes u and v such that $\mathcal{B}_q(u)$ and $\mathcal{C}_q(v)$ in (3.18) are squarefree, or that there exist infinitely many primes p such that $\mathcal{A}_q(p)$ in (3.19) is squarefree. Both of these conclusions follow from Corollary 2.12, provided that, respectively, $\mathcal{B}_q(t)$ and $\mathcal{C}_q(t)$ have no local obstructions, or $\mathcal{A}_q(t)$ has no local obstructions (see Remark 2.13). However, when $11 \leq q \leq 211$, this result is conditional on the abc-conjecture for number fields since $\deg(h_0) = \deg(h_1) = (q-3)/2 \geq 4$ for these primes.

Therefore, the only completely unconditional monogenic result we can achieve at this time is Theorem 1.1.

4. The proof of Theorem 1.1

Proof of Theorem 1.1. In light of Theorem 3.4, and since Conjecture 3.3 has been verified by computer for $q \in \{3, 5, 7\}$, it would suffice to show for each of these primes q that there exist infinitely many prime values of t such that $\mathcal{A}_q(t)$ in (3.19) is squarefree. We will see that this is possible only for the primes $q \in \{3, 5\}$. For the prime $q = 7$, because of a local obstruction of $\mathcal{A}_7(t)$ at the prime $\ell = 3$ for certain congruence classes of $r \pmod 9$, we must resort to an analysis of the two separate cases $\mathcal{B}_7(t)$ and $\mathcal{C}_7(t)$ in (3.18).

For each $q \in \{3, 5\}$, we wish to apply Corollary 2.12 to the polynomials $\mathcal{A}_q(t)$ in Table 2. We must first check $\mathcal{A}_q(t)$ for obstructions. Suppose that $q = 3$. We

q	$h_a(t)$	$\mathcal{A}_q(t)$
3	1	$(12rt + 1)(36rt - 1)(12rt - 1)(36rt + 1)$
5	$80rt - 1$	$(20rt + 1)(100rt + 1)(80rt - 1)$

TABLE 2. Computer Calculations of $h_a(t)$ and $\mathcal{A}_q(t)$ for $q \in \{3, 5\}$.

see easily that $\mathcal{A}_3(t)$ has no obstruction at $\ell = r$ since $\mathcal{A}_3(t) \equiv 1 \pmod{r^2}$. So, assume that ℓ is a prime with $\ell \neq r$, and let z be an integer such that $rz \equiv 1 \pmod{\ell^2}$. Then

$$\mathcal{A}_3(z) \equiv (12 - 1)(36 - 1)(12 + 1)(36 + 1) = 11 \cdot 5 \cdot 7 \cdot 13 \cdot 37 \not\equiv 0 \pmod{\ell^2},$$

and hence $\mathcal{A}_3(t)$ has no obstructions.

Now suppose that $q = 5$. Since

$$\mathcal{A}_5(1) \equiv -40r - 1 \not\equiv 0 \pmod{r^2},$$

we conclude that $\mathcal{A}_5(t)$ has no obstruction at $\ell = r$. Assume then that ℓ is a prime with $\ell \neq r$ and let z be an integer such that $rz \equiv 1 \pmod{\ell^2}$. Then

$$\mathcal{A}_5(z) \equiv (20 + 1)(100 + 1)(80 - 1) = 3 \cdot 7 \cdot 101 \cdot 79 \not\equiv 0 \pmod{\ell^2},$$

and hence $\mathcal{A}_5(t)$ has no obstructions.

Thus, for each $q \in \{3, 5\}$, we can apply Corollary 2.12 to $\mathcal{A}_q(t)$ to conclude that there exist infinitely many primes p such that $\mathcal{A}_q(p)$ is squarefree, and this conclusion is unconditional since $A_q(t)$ has no irreducible factor of degree $d > 3$. Hence, by Theorem 3.4, the proof of Theorem 1.1 is complete for these primes q.

Finally, we turn to $q = 7$. Note that $r = 5$ is a primitive root modulo 49. For this value of r, it is easy to check that

$$A_7(t) \equiv 0 \pmod 9 \quad \text{for all } t \in (\mathbb{Z}/9\mathbb{Z})^*.$$

Hence, $\mathcal{A}_7(t)$ has an obstruction at $\ell = 3$, and so we must break our analysis into two cases as indicated in Theorem 3.4. For the first case, we have

$$h_0(t) = 21168r^2t^2 - 56rt - 1 \quad \text{and} \quad \mathcal{B}_7(t) = (28rt+1)(196rt-1)h_0(t), \tag{4.1}$$

while for the second case, we have

$$h_1(t) = 21168r^2t^2 + 56rt - 1 \quad \text{and} \quad \mathcal{C}_7(t) = (28rt-1)(196rt+1)h_1(t). \tag{4.2}$$

Because the methods are similar for resolving each of the cases (4.1) and (4.2), we provide the details only for (4.1). Since $\mathcal{B}_7(t) \equiv 1 \pmod 4$, we see that $\mathcal{B}_7(t)$ has no obstruction at $\ell = 2$. Also, since

$$\mathcal{B}_7(t) \equiv -112rt + 1 \not\equiv 0 \pmod{r^2},$$

we conclude that $\mathcal{B}_7(t)$ has no obstruction at $\ell = r$. Next, suppose that $\ell = 3$. In Table 3, we give the possible congruences classes of $r \pmod 9$ and we indicate a value of $t \in (\mathbb{Z}/9\mathbb{Z})^*$ for which $\mathcal{B}_7(t) \not\equiv 0 \pmod 9$. Thus, $\mathcal{B}_7(t)$ has no obstruction at $\ell = 3$.

$r \pmod 9$	1	2	3	4	5	7	8
$t \pmod 9$	2	1	1	8	1	8	7
$\mathcal{B}_7(t) \pmod 9$	3	3	7	6	6	3	3

TABLE 3. Values of $r \pmod 9$, $t \pmod 9$ and $\mathcal{B}_7(t) \pmod 9$.

Suppose now that ℓ is a prime with $\ell \notin \{2, 3, r\}$. Let z be an integer such that $rz \equiv 1 \pmod{\ell^2}$. Then

$$\mathcal{B}_7(z) \equiv (28+1)(196-1)(21168-56-1) = 3^2 \cdot 5 \cdot 13 \cdot 29 \cdot 31 \cdot 227 \not\equiv 0 \pmod{\ell^2},$$

which shows that $\mathcal{B}_7(t)$ has no obstructions.

Note that the largest degree of an irreducible factor of both $\mathcal{B}_7(t)$ and $\mathcal{C}_7(t)$ is 2. Thus, combining the conclusions of Corollary 2.12 when applied to each of $\mathcal{B}_7(t)$ and $\mathcal{C}_7(t)$, together with Theorem 3.4, completes the unconditional proof of the theorem. □

5. The proof of Theorem 1.3

Proof of Theorem 1.3. For part I., suppose first that $N = 12$. Let p be a prime such that

$$\mathcal{F}_{12,p}(x) = x^4 + (36rp - 1)x^2 + 1$$

is a reciprocal monogenic polynomial from Theorem 1.1, for which $\mathcal{A}_3(p)$ in Table 2 is squarefree. We see immediately from part (1) of Theorem 2.23 that

$$\mathrm{Gal}\left(\mathcal{F}_{12,p}\right) = 4\mathrm{T}2 \simeq C_2 \times C_2.$$

For part I. with $N = 18$, let p be a prime such that

$$\mathcal{F}_{18,p}(x) = x^6 + (36rp - 1)x^3 + 1$$

is a reciprocal monogenic polynomial from Theorem 1.1, for which $\mathcal{A}_3(p)$ in Table 2 is squarefree. In the context of applying Theorem 2.25 to $\mathcal{F}_{18,p}(x)$, we get

$$g(x) = x^3 - 3x - (36rp - 1).$$

Then, a Maple computation gives that

$$\Delta(g) = -81(12rp - 1)(36rp + 1),$$

which is clearly not a square in $\mathbb{Z}$. Hence, $\mathrm{Gal}(\mathcal{F}) \simeq C_2 \times S_3$.

For part I. with $N = 24$, let p be a prime such that

$$\mathcal{F}_{24,p}(x) = x^8 + (36rp - 1)x^4 + 1$$

is a reciprocal monogenic polynomial from Theorem 1.1, for which $\mathcal{A}_3(p)$ in Table 2 is squarefree. Corresponding to the reciprocal polynomial $\mathcal{F}_{24,p}(x)$ we have from (2.1) that

$$g(u) = u^4 - 4u^2 + 36rp + 1.$$

Note that $g(u) = f(h(u))$, where

$$f(u) = u^2 - 4u + 36rp + 1 \quad \text{and} \quad h(u) = u^2.$$

Applying Theorems 2.6 and 2.7 to this situation, we let

$$\alpha = 2 + \sqrt{-3(12rp - 1)},$$

noting that $f(\alpha) = 0$ and $f(u)$ is irreducible. Then $g(u)$ is reducible if and only if $\alpha = \beta^2$ for some $\beta \in \mathbb{Q}(\alpha)$. However, the norm of α is

$$\mathcal{N}(\alpha) = 36rp + 1,$$

which is not a square in $\mathbb{Q}$, and therefore α cannot be a square in $\mathbb{Q}(\alpha)$. Hence, $g(u)$ is irreducible. Using Theorem 2.23, it is easy to verify that $\mathrm{Gal}(g) \simeq D_4$. Thus, by Corollary 2.12, $\mathrm{Gal}\left(\mathcal{F}_{24,p}\right)$ contains a subgroup of isomorphic to D_4. Suppose that $\mathcal{F}_{24,p}(\theta) = 0$, and let L be a splitting field of $\mathcal{F}_{24,p}(x)$. Since

$$-\left(\theta^4 + \theta^{-4}\right) = 36rp - 1,$$

we have that

$$\mathcal{F}_{24,p}(x) = (x - \theta)(x + \theta)\left(x - \theta^{-1}\right)\left(x + \theta^{-1}\right)\left(x^2 + \theta^2\right)\left(x^2 + \theta^{-2}\right)$$

over $\mathbb{Q}(\theta)$. Thus, either $L = Q(\theta)$ or $L = \mathbb{Q}(\theta, i)$, depending on whether $x^2 + \theta^2$ is, respectively, reducible or irreducible over $\mathbb{Q}(\theta)$. Note that

$$f_1(x) := x^4 + (36rp - 1)x^2 + 1$$

is irreducible since $\mathcal{F}_{24,p}(x)$ is irreducible. Also, applying part (1) of Proposition 2.21 to

$$f_2(x) := x^4 - (36rp - 1)x^2 + 1$$

confirms that $f_2(x)$ is irreducible since neither

$$\begin{aligned} c^2-4 &= 3(12rp-1)(36rp+1),\\ -c+2 &= 36rp+1 \quad \text{nor}\\ -c-2 &= 3(12rp-1) \end{aligned}$$

is a square in $\mathbb{Q}$. Thus, $\mathbb{Q}\left(\theta^2\right)$ and $\mathbb{Q}\left(i\theta^2\right)$ are both degree-4 normal subfields of L, since they are splitting fields of, respectively, $f_1(x)$ and $f_2(x)$. If $\mathbb{Q}\left(\theta^2\right) = \mathbb{Q}\left(i\theta^2\right)$, then there exist $A, B, C, D, m \in \mathbb{Z}$, with $m \neq 0$, such that

$$i\theta^2 = \frac{A + B\theta^2 + C\theta^4 + D\theta^6}{m}. \tag{5.1}$$

Squaring both sides of (5.1) and using the fact that $\mathcal{F}_{24,p}(\theta) = 0$, we get

$$\begin{aligned} &(2CD - 72CDrp + 2AD + 2BC)\theta^6\\ &+ (-72BDrp - 72D^2rp + 2AC + B^2 + 1296D^2r^2p^2 + 2BD - 36C^2rp + C^2)\theta^4\\ &+ (m^2 - 2CD + 2AB)\theta^2 + A^2 - C^2 - D^2 + 36D^2rp - 2BD = 0. \end{aligned}$$

Since the elements of the set $\left\{1, \theta^2, \theta^4, \theta^6\right\}$ are linearly independent, we then arrive at the system of equations:

$$\begin{aligned} 2CD - 72CDrp + 2AD + 2BC &= 0\\ -72BDrp - 72D^2rp + 2AC + B^2 + 1296D^2r^2p^2 + 2BD - 36C^2rp + C^2 &= 0\\ m^2 - 2CD + 2AB &= 0\\ A^2 - C^2 - D^2 + 36D^2rp - 2BD &= 0. \end{aligned}$$

Using the Maple **isolve** command on this system confirms that there are no integer solutions with $m \neq 0$, and therefore, $\mathbb{Q}\left(\theta^2\right) \neq \mathbb{Q}\left(i\theta^2\right)$. Thus, if $L = \mathbb{Q}(\theta)$, then $\mathrm{Gal}\left(\mathcal{F}_{24,p}\right)$ contains at least two distinct normal subgroups of order 2, corresponding to the two distinct degree-4 normal subfields. Since $[\mathbb{Q}(\theta) : \mathbb{Q}] = 8$ and $\mathrm{Gal}\left(\mathcal{F}_{24,p}\right)$ contains a subgroup isomorphic to D_4, it must be that $\mathrm{Gal}\left(\mathcal{F}_{24,p}\right) \simeq D_4$. However, D_4 contains only one normal subgroup of order 2. Therefore, we conclude that $L = \mathbb{Q}(\theta, i)$ and

$$[\mathbb{Q}(\theta, i) : \mathbb{Q}] = \left|\mathrm{Gal}\left(\mathcal{F}_{24,p}\right)\right| = 16.$$

Define

$$\widetilde{g}(u) := u^4 + 4u^2 + 36rp + 1.$$

Then, using the fact that the set of zeros of $g(u)$ is

$$\left\{\pm\left(\theta + \theta^{-1}\right), \quad \pm i\left(\theta - \theta^{-1}\right)\right\},$$

and that the set of zeros of $\widetilde{g}(u)$ is

$$\left\{\pm i\left(\theta + \theta^{-1}\right), \quad \pm\left(\theta - \theta^{-1}\right)\right\},$$

along with arguments similar to the previous discussion for $f_1(x)$ and $f_2(x)$, we see that the splitting fields K_1 of $g(u)$ and K_2 of $\widetilde{g}(u)$ are such that $K_1 \neq K_2$, both K_1 and K_2 are contained in L and $[K_1 : \mathbb{Q}] = 8 = [K_2 : \mathbb{Q}]$. Thus, as before,

we deduce that Gal $\left(\mathcal{F}_{24,p}\right)$ contains at least two distinct normal subgroups of order 2. Since, by a Maple computation,

$$\Delta\left(\mathcal{F}_{24,p}\right) = 2^4 3^2 (12rp-1)^2 (36rp+1)^2,$$

we conclude that Gal $\left(\mathcal{F}_{24,p}\right)$ is even by Theorem 2.14. Examination of the six transitive groups 8T6 to 8T11 of degree 8 and order 16 reveals that only 8T9 is even, contains a subgroup isomorphic to D_4 and has at least two normal subgroups of order 2 (see [10, 21]). Thus, Gal $\left(\mathcal{F}_{24,p}\right) = 8\text{T}9$.

Next, for part I. with $N = 36$, let p be a prime such that

$$\mathcal{F}_{36,p}(x) = x^{12} + (36rp-1)x^6 + 1$$

is a reciprocal monogenic polynomial from Theorem 1.1, for which $\mathcal{A}_3(p)$ in Table 2 is squarefree. From (2.1), we have for the reciprocal polynomial $\mathcal{F}_{36,p}(x)$ that

$$g(u) = u^6 - 6u^4 + 9u^2 + 36rp - 3,$$

which is 3-Eisenstein, and hence irreducible. Let

$$\begin{aligned} a &= -6 \\ b &= 9 \\ c &= 36rp - 3 \\ d &= -81(36rp+1)(12rp-1) \text{ and} \\ h(u) &= u^6 - 9u^4 + (-216rp+18)u^2 - 1296r^2p^2 + 216rp - 9 \\ &= \left(u^3 + 3u^2 + 36rp - 3\right)\left(u^3 - 3u^2 - 36rp + 3\right). \end{aligned} \tag{5.2}$$

Thus, applying Theorem 2.27 1 to $g(u)$ with the information in (5.2), we deduce, since $\mathcal{A}_3(p)$ is squarefree, that Gal$(g) = 6\text{T}3$. Let $\mathcal{F}_{36,p}(\theta) = 0$, so that

$$[\mathbb{Q}(\theta) : \mathbb{Q}] = 12.$$

Let ζ be a primitive sixth root of unity. A straightforward computation shows that the 12 zeros of $\mathcal{F}_{36,p}(x)$ are:

$$\pm\theta, \qquad \pm\theta^{-1}, \qquad \pm\theta\zeta, \qquad \pm\theta\zeta^2, \qquad \pm\theta^{-1}\zeta, \qquad \pm\theta^{-1}\zeta^2.$$

Hence, $\mathcal{F}_{36,p}(x)$ splits completely over $\mathbb{Q}(\theta,\zeta)$. If $\zeta \in \mathbb{Q}(\theta)$, then $|\text{Gal}\left(\mathcal{F}_{36,p}\right)| = 12$, and thus $6\text{T}3 = \text{Gal}\,(g) = \text{Gal}\left(\mathcal{F}_{36,p}\right)$ by Corollary 2.20. However, since

$$\Delta\left(\mathcal{F}_{36,p}\right) = 2^{12} 3^{18} (36rp+1)^6 (12rp-1)^6,$$

we have from Theorem 2.14 that Gal $\left(\mathcal{F}_{36,p}\right)$ is isomorphic to a subgroup of A_{12}, which contradicts the fact that 6T3 is not even. Consequently,

$$[\mathbb{Q}(\theta,\zeta) : \mathbb{Q}(\theta)] = 2,$$

so that $|\text{Gal}\left(\mathcal{F}_{36,p}\right)| = 24$. Examination of the four even transitive groups 12T6, 12T7, 12T9 and 12T10 of degree 12 and order 24 reveals that the only one of these groups with a subgroup isomorphic to 6T3 is 12T10 [21], which completes the proof in this case.

For part II., we give the details only for $\mathcal{F}_{10}(x)$ since the details for $\mathcal{F}_5(x)$ are similar. Let $q = 5$ and let p be a prime such that

$$\mathcal{F}_{10,p}(x) = x^4 - x^3 + (100rp + 1)x^2 - x + 1$$

is a reciprocal monogenic polynomial from Theorem 1.1, for which $\mathcal{A}_5(p)$ in Table 2 is squarefree. Observe that $\mathcal{F}_{10,p}(x) = \Phi_{10}(x) + 100rpx^2 > 0$ for all x, which implies that $\mathcal{F}_{10,p}(x)$ has no real zeros. Applying Proposition 2.19 to the reciprocal polynomial $\mathcal{F}_{10,p}(x)$, we have from (2.1) that

$$g(u) = g_1(u) = u^2 - u + 100rp - 1.$$

Note that $\Delta(g) = -400rp + 5$, from which we conclude that $g(u)$ has no real zeros. Hence, by Corollary 2.20, $\mathcal{F}_{10,p}(x)$ has no zeros on the unit circle. Suppose that $\mathcal{F}_{10,p}(\theta) = 0$ so that $[\mathbb{Q}(\theta) : \mathbb{Q}] = 4$. Thus, θ, θ^{-1}, $\overline{\theta}$ and $\overline{\theta}^{-1}$ are the four distinct zeros of $\mathcal{F}_{10,p}(x)$, and since

$$100rp + 1 = -\theta^2 + \theta + \theta^{-1} - \theta^{-2},$$

it follows that

$$\mathcal{F}_{10,p}(x) = (x - \theta)\left(x - \theta^{-1}\right)\left(x^2 + \left(\theta + \theta^{-1} - 1\right)x + 1\right),$$

over $\mathbb{Q}(\theta)$. If $\overline{\theta} \in \mathbb{Q}(\theta)$, then $\mathcal{F}_{10,p}(x)$ splits completely over $\mathbb{Q}(\theta)$ and

$$\left|\mathrm{Gal}\left(\mathcal{F}_{10,p}\right)\right| = 4.$$

A computer calculation yields

$$\Delta\left(\mathcal{F}_{10,p}\right) = 5^3(20rp + 1)(100rp + 1)(80rp - 1)^2,$$

which confirms (3.16) in Conjecture 3.3. Since $\Delta\left(\mathcal{F}_{10,p}\right)$ is not a square, it follows that $\mathrm{Gal}\left(\mathcal{F}_{10,p}\right) = 4\mathrm{T}1 \simeq C_4$. However,

$$\sigma_1(\theta) = \theta^{-1} \quad \text{and} \quad \sigma_2(\theta) = \overline{\theta}$$

are two distinct elements of order 2 in $\mathrm{Gal}\left(\mathcal{F}_{10,p}\right)$, which contradicts the fact that C_4 has a single element of order 2. Therefore, $|\mathrm{Gal}\left(\mathcal{F}_{10,p}\right)| = 8$, and $\mathrm{Gal}\left(\mathcal{F}_{10,p}\right) = 4\mathrm{T}3$, since 4T3 is the only transitive group of degree 4 and order 8 [21].

For III., we give the details only for part (a) since part (b) is similar. Let $q = 7$ and let p be a prime such that

$$\mathcal{F}_{7,p}(x) = x^6 + x^5 + x^4 + (196rp + 1)x^3 + x^2 + x + 1$$

is a reciprocal monogenic polynomial from Theorem 1.1, for which $\mathcal{B}_7(p)$ in (3.18) is squarefree. Then, from (3.14), we have that

$$g(u) = g_0(u) = u^3 + u^2 - 2u + 196rp - 1,$$

which is monogenic by Theorem 3.4. Since

$$\Delta(g) = -7^2\left(21168r^2p^2 + 56rp + 1\right) < 0,$$

$g(u)$ has exactly one real zero ρ, two non-real zeros β and $\overline{\beta}$, and $\mathrm{Gal}(g) \simeq S_3$. Moreover, since

$$g\left(-(196rp-1)^{1/3}-1\right) < 0 \quad \text{and} \quad g\left(-(196rp-1)^{1/3}\right) > 0,$$

it follows that

$$-(196rp-1)^{1/3} - 1 < \rho < -(196rp-1)^{1/3}$$

and

$$\beta = \frac{-(\rho+1)+\sqrt{9-2\rho-3\rho^2}}{2}, \quad \text{with} \quad 9-2\rho-3\rho^2 < 0. \tag{5.3}$$

Thus, by Corollary 2.20, we deduce that $\mathcal{F}_{7,p}(x)$ has exactly two real zeros,

$$\theta = \frac{\rho+\sqrt{\rho^2-4}}{2} \quad \text{and} \quad \theta^{-1} = \frac{\rho-\sqrt{\rho^2-4}}{2}, \tag{5.4}$$

and four non-real zeros,

$$\begin{aligned} \alpha &= \frac{\beta+\sqrt{\beta^2-4}}{2}, \qquad \alpha^{-1} = \frac{\beta-\sqrt{\beta^2-4}}{2}, \\ \overline{\alpha} &= \frac{\overline{\beta}+\sqrt{\overline{\beta}^2-4}}{2} \quad \text{and} \quad \overline{\alpha}^{-1} = \frac{\overline{\beta}-\sqrt{\overline{\beta}^2-4}}{2}. \end{aligned} \tag{5.5}$$

Since

$$\mathcal{F}_{7,p}(-.5) = .671875 - 24.5rp < 0 \quad \text{and} \quad \mathcal{F}_{7,p}(0) = 1,$$

we see that $-.5 < \theta < 0$. Furthermore, $\mathcal{F}_{7,p}(x)$ has no zeros on the unit circle since a calculus argument reveals that the absolute minimum value of $g(u)$ on the interval $[-2,2]$ is $(-1+\sqrt{7})/2 + 196rp > 0$.

Thus, since $-\rho^3-\rho^2+2\rho+2 = 196rp+1$, we have that

$$\mathcal{F}_{7,p}(x) = \underbrace{\left(x^2-\rho x+1\right)}_{=\gamma_1(x)}\underbrace{\left(x^4+(\rho+1)x^3+\left(\rho^2+\rho\right)x^2+(\rho+1)x+1\right)}_{=\gamma_2(x)},$$

where $\gamma_1(x)$ has the two real zeros (5.4) and $\gamma_2(x)$ has the four non-real zeros (5.5). We claim that both $\gamma_1(x)$ and $\gamma_2(x)$ are irreducible over $\mathbb{Q}(\rho)$. We give the details for the irreducibility of $\gamma_2(x)$, and omit the details for $\gamma_1(x)$ since the argument for $\gamma_1(x)$ is similar. Since $\mathbb{Q}(\rho) \subset \mathbb{R}$ and all zeros of $\gamma_2(x)$ are non-real, it follows that if $\gamma_2(x)$ is reducible over $\mathbb{Q}(\rho)$, then $\gamma_2(x)$ must factor into the product of two irreducible quadratics.

We appeal to part (2) of Proposition 2.21 with $b = \rho+1$ and $c = \rho^2+\rho$. There are three possibilities to check. For the first possibility, we have from (5.3) that

$$8 + b^2 - 4c = -3\rho^2 - 2\rho + 9 < 0,$$

which is not a square in $\mathbb{Q}(\rho) \subset \mathbb{R}$.

For the next two possibilities in Proposition 2.21, we see that a necessary condition for either of

$$b^2 - 2c - 4 \pm 2\sqrt{4-4b^2+4c+c^2}$$

to be a square in $\mathbb{Q}(\rho)$, is that $4-4b^2+4c+c^2$ must be a square in $\mathbb{Q}(\rho)$. Repeated use of the fact that

$$\rho^3 = -\rho^2 + 2\rho - (196rp - 1) \tag{5.6}$$

yields

$$\begin{aligned} 4 - 4b^2 + 4c + c^2 &= \rho^4 + 2\rho^3 + \rho^2 - 4\rho \\ &= 2\rho^2 - (196rp + 1)\rho - (196rp - 1). \end{aligned} \tag{5.7}$$

Assume that (5.7) is a square in $\mathbb{Q}(\rho)$. Then, there exist $A, B, C, m \in \mathbb{Z}$ such that

$$m^2\left(2\rho^2 - (196rp + 1)\rho - (196rp - 1)\right) = \left(A + B\rho + C\rho^2\right)^2. \tag{5.8}$$

Note that we cannot have $A = B = C = 0$ since that would contradict the fact that the minimal polynomial of ρ has degree 3. Expanding (5.8) and using (5.6) produces the equation

$$\begin{aligned} &\left(B^2 + 3C^2 - 2BC + 2AC - 2m^2\right)\rho^2 \\ &\qquad + \left(4BC + 2AB + m^2 - C^2 - 196rpC^2 + 196rpm^2\right)\rho \\ &\quad - C^2 + 196rpm^2 - 392rpBC + 196rpC^2 + A^2 - m^2 + 2BC = 0. \end{aligned} \tag{5.9}$$

Since the elements of $\{1, \rho, \rho^2\}$ are linearly independent, we extract from (5.9) the following system of equations:

$$S = \begin{cases} B^2 + 3C^2 - 2BC + 2AC - 2m^2 = 0 \\ 4BC + 2AB + m^2 - C^2 - 196rpC^2 + 196rpm^2 = 0 \\ -C^2 + 196rpm^2 - 392rpBC + 196rpC^2 + A^2 - m^2 + 2BC = 0. \end{cases}$$

Using the **isolve** command, Maple supplies the following five solutions to S:

(1) $\{A = -2Z_2, \quad B = -Z_2, \quad C = Z_2, \quad r = Z_1, \quad p = 0, \quad m = -Z_2\}$
(2) $\{A = -2Z_2, \quad B = -Z_2, \quad C = Z_2, \quad r = 0, \quad p = Z_1, \quad m = -Z_2\}$
(3) $\{A = -2Z_2, \quad B = -Z_2, \quad C = Z_2, \quad r = 0, \quad p = Z_1, \quad m = Z_2\}$
(4) $\{A = -2Z_2, \quad B = -Z_2, \quad C = Z_2, \quad r = Z_1, \quad p = 0, \quad m = Z_2\}$
(5) $\{A = 0, \quad B = 0, \quad C = 0, \quad r = Z_1, \quad p = Z_2, \quad m = 0\}$.

Since $rp > 0$, solutions (1) to (4) can be ruled, and, as mentioned, solution (5) contradicts the degree of the minimal polynomial for ρ. Thus, $\gamma_2(x)$ is irreducible over $\mathbb{Q}(\rho)$.

Since

$$\gamma_2(x) = (x - \alpha)\left(x - \alpha^{-1}\right)\left(x^2 + \left(\alpha + \alpha^{-1} + \rho + 1\right)x + 1\right)$$

over $\mathbb{Q}(\rho, \alpha)$, the previous discussion tells us that $\mathbb{Q}(\rho, \alpha, \theta, \overline{\alpha})$ is a splitting field for $\mathcal{F}_{7,p}(x)$ and gives us the following tower of fields (with relative degrees):

$$\begin{array}{c} \mathbb{Q}(\rho,\alpha,\theta,\overline{\alpha}) \\ d \,\big|\, \\ \mathbb{Q}(\rho,\alpha,\theta) \\ 2 \,\big|\, \\ \mathbb{Q}(\rho,\alpha) \\ 4 \,\big|\, \\ \mathbb{Q}(\rho) \\ 3 \,\big|\, \\ \mathbb{Q} \end{array}$$

where $d = 1$ or $d = 2$ depending on whether $x^2 + \left(\alpha + \alpha^{-1} + \rho + 1\right) x + 1$ is, respectively, reducible or irreducible over $\mathbb{Q}(\rho, \alpha)$. We deduce that

$$\left|\mathrm{Gal}\left(\mathcal{F}_{7,p}\right)\right| \in \{24, 48\}.$$

To narrow down these choices, we use three additional facts. First, since

$$\Delta\left(\mathcal{F}_{7,p}\right) = 7^5(28rp+1)(196rp-1)\left(21168r^2p^2 - 56rp - 1\right)^2$$

is not a square, we have, by Theorem 2.14, that $\mathrm{Gal}\left(\mathcal{F}_{7,p}\right)$ is not even. Second, since $\mathrm{Gal}(g) \simeq S_3$, we have by Corollary 2.20, that $\mathrm{Gal}\left(\mathcal{F}_{7,p}\right)$ contains a subgroup isomorphic to S_3. Third, since $\mathcal{F}_{7,p}(x) \equiv \Phi_7(x) \pmod{r}$ and r is a primitive root modulo 7, we have from Theorem 2.2 that $\mathcal{F}_{7,p}(x)$ is irreducible modulo r. Therefore, by Theorem 2.10, $\mathrm{Gal}\left(\mathcal{F}_{7,p}\right)$ contains an element of order 6.

We first examine the three transitive groups [21] of degree 6 and order 24: 6T6, 6T7 and 6T8. The group 6T7 is even and therefore can be ruled out by the first fact above. The group 6T6 is isomorphic to $C_2 \times A_4$, which contains no subgroup isomorphic to S_3, and thus, by the second fact above, 6T6 can be ruled out as well. Finally, we can use the third fact above to rule out 6T8 since 6T8 $\simeq S_4$, and S_4 contains no element of order 6. Hence, $|\mathrm{Gal}\left(\mathcal{F}_{7,p}\right)| = 48$. Since there is exactly one transitive group [21] of degree 6 and order 48, namely 6T11, it follows that $\mathrm{Gal}\left(\mathcal{F}_{7,p}\right) = 6\mathrm{T}11$. □

6. Final comments

Computer calculations suggest the following:

Conjecture 6.1. *Let $\mathcal{F}_{2^a q^b,p}(x)$ be as in* (1.2)*. Let $q = 7$ and $b = 1$.*

(1) If $a = 2$, then there exist infinitely many primes p such that $\mathcal{F}_{2^a 7,p}(x)$ is a reciprocal monogenic polynomial with $Gal\left(\mathcal{F}_{2^a 7,p}\right) = 12\mathrm{T}139$.

(2) If $a \geq 3$, then there exist infinitely many primes p such that $\mathcal{F}_{2^a 7,p}(x)$ is a reciprocal monogenic polynomial with

$$\left|Gal\left(\mathcal{F}_{2^a 7,p}\right)\right| = 2^{4a-1} \cdot 3.$$

During attempts to establish part (1) of Conjecture 6.1, we encountered the following unexpected consequence:

Theorem 6.2. *Let r be a prime. Then there exist infinitely many primes p such that*

$$g(u) := u^6 - 7u^4 + 14u^2 + 196pr - 7$$

is monogenic with Gal $(g) = 6$T11.

Remark 6.3. The polynomial $g(u)$ corresponds to $\mathcal{F}_{28,p}(x)$ and arises from (2.1).

Proof. By Corollary 2.12, there exist infinitely many primes p such that

$$(28pr - 1)\left(21168p^2r^2 + 56pr - 1\right) \text{ is squarefree.}$$

Let p be such a prime. Consider the polynomial

$$\widehat{g}(u) := u^3 - 7u^2 + 14u + 196pr - 7.$$

Note that $g(u)$ and $\widehat{g}(u)$ are irreducible since they are both 7-Eisenstein. Suppose that $g(\alpha) = 0$. Then $\widehat{g}\left(\alpha^2\right) = 0$. Let $K = \mathbb{Q}\left(\alpha^2\right)$ and $L = \mathbb{Q}(\alpha)$, so that $K \subset L$. Hence, by Theorem 2.8, we deduce that

$$\Delta(K)^2 \,\Big|\, \Delta(L). \tag{6.1}$$

From Maple, we have that

$$\begin{aligned} \Delta\left(\widehat{g}\right) &= -7^2\left(21168p^2r^2 + 56pr - 1\right) \text{ and} \\ \Delta(g) &= -2^6 7^5 (28pr - 1)\left(21168p^2r^2 + 56pr - 1\right)^2. \end{aligned} \tag{6.2}$$

By Theorem 2.15, $7^2 || \Delta(K)$ and $7^5 || \Delta L$. Since $21168p^2r^2 + 56pr - 1$ is squarefree, we conclude that $\widehat{g}(u)$ is monogenic and therefore, $\Delta\left(\widehat{g}\right) = \Delta(K)$. Thus, since $28pr - 1$ is squarefree, it follows from (6.1) and (6.2) that we only have to show $2^6 || \Delta(L)$ to prove that $g(u)$ is monogenic. We apply Theorem 2.9 with the prime 2. Using Maple, we get

$$F(x) = \frac{\left(u^3 + u^2 + 1\right)^2 - g(u)}{2} = u^5 + u^3 + 4u^4 - 6u^2 + 4 - 98pr,$$

so that $\overline{F}(x) = u^5 + u^3$. Then, another Maple calculation shows that

$$\gcd\left(\overline{F}, u^3 + u^2 + 1\right) = 1,$$

which implies that $[\mathbb{Z}_L : \mathbb{Z}[\alpha]] \not\equiv 0 \pmod 2$, and hence $g(u)$ is monogenic.

To see that Gal$(g) = 6$T11, we apply Theorem 2.27 to $g(u)$ with

$$a = -7, \quad b = 14, \quad c = 196pr - 7 \quad \text{and} \quad d = \Delta(\widehat{g}).$$

Thus, from our assumptions on p, it is easy to see that none of $-c$, d and $-cd$ is a square in $\mathbb{Z}$. Next, we calculate

$$h(u) = u^6 - 14u^4 - 7(196pr - 7)u^2 - (196pr - 7)^2.$$

We claim that $h(u)$ is irreducible. To see this, we use Proposition 2.24. Let

$$H(u) = u^3 - 14u^2 - 77(196pr - 7)u - (196pr - 7)^2.$$

Observe that

$$H(u) \equiv u^3 + u + 1 \pmod 2,$$

which has no zeros modulo 2. Hence, $H(u)$ is irreducible. Then, as in Proposition 2.24, we have

$$\widehat{h}(u) = u^4 - 28u^2 + (-1568pr + 56)u + 5488pr.$$

By the Rational Zero Theorem, there are 80 possible integer zeros of $\widehat{h}(u)$, and they have the form $z_{i,j} := p^i r^j n$, where $i, j \in \{0, 1\}$ and n is a divisor of 5488. We use the Maple command **isolve**(W), where

$$W := \left\{\left(\widehat{h}\left(z_{i,j}\right)\right) = 0, p > 0, r > 0\right\},$$

to see that there are no solutions for any i and j. It follows from Proposition 2.24 that $h(u)$ is irreducible. Finally, we conclude from Theorem 2.27 that $\mathrm{Gal}(g) =$ 6T11. □

Acknowledgments

The author thanks the referee for a very thorough reading of the manuscript, and for the many positive comments and suggestions.

References

[1] Alexandersson, Per; González–Serrano, Luis A.; Maximenko, Egor A.; Moctezuma–Salazar, Mario A. Symmetric polynomials in the symplectic alphabet and the change of variables $z_j = x_j + x_j^{-1}$. *Electron. J. Combin.* **28** (2021), no. 1, Paper No. 1.56, 36 pp. MR4245289, Zbl 1461.05235, doi: 10.37236/9354. 1470

[2] Awtrey, Chad; Jakes, Peter. Galois groups of even sextic polynomials. *Canad. Math. Bull.* **63** (2020), no. 3, 670–676. MR4148127, Zbl 1458.11173, doi: 10.4153/S0008439519000754. 1471

[3] Brookfield, Gary. Factoring quartic polynomials: a lost art. *Math. Mag.* **80** (2007), no. 1, 67–70. Zbl 1227.97040, doi: 10.1080/0025570X.2007.11953453. 1470

[4] Burton, David M. Elementary number theory. Seventh edition. *McGraw-Hill Higher Education* (2011). ISBN: 978-0073-383-149. 1472

[5] Butler, Gregory; McKay, John. The transitive groups of degree up to eleven. *Comm. Algebra* **11** (1983), no. 8, 863—911. MR0695893 (84f:20005), Zbl 0518.20003, doi: 10.1080/00927878308822884. 1466

[6] Cohen, Henri. A course in computational algebraic number theory. Graduate Texts in Mathematics, 138. *Springer-Verlag, Berlin*, 1993. xii+534 pp. ISBN: 3-540-55640-0 MR1228206 (94i:11105), Zbl 0786.11071, doi: 10.5555/206777. 1465, 1467, 1468, 1469

[7] Conrad, Keith. Totally ramified primes and eisenstein polynomials. Preprint, 2012. www.math.uconn.edu/ kconrad/blurbs/gradnumthy/totram.pdf 1469

[8] Cox, David A. Galois theory. Second edition. Pure and Applied Mathematics (Hoboken). *John Wiley & Sons, Inc., Hoboken, NJ*, 2012. xxviii+570 pp. ISBN: 978-1-118-07205-9. MR2919975, Zbl 1247.12006, doi: 10.1002/9781118218457. 1468

[9] Cullinan, John. The discriminant of a composition of two polynomials. Preprint. https://studylib.net/doc/8187082/the-discriminant-of-a-composition-of-two. 1467

[10] DOKCHITSER, TIM. Transitive groups of degree up to 31. 1466, 1485 https://people.maths.bris.ac.uk/ matyd/GroupNames/T31.html.

[11] ELOUAFI, MOHAMED. On a relationship between Chebyshev polynomials and Toeplitz determinants. *Appl. Math. Comput.* **229** (2014) 27–33. MR3159851, Zbl 1364.15022, doi: 10.1016/j.amc.2013.12.029. 1470

[12] GUERRIER, W. J. The factorization of the cyclotomic polynomials mod p. *Amer. Math. Monthly* **75** (1968), 46. MR0225747 (37 #1340), Zbl 0164.05901, doi: 10.2307/2315109. 1467

[13] GUERSENZVAIG, NATALIO. Elementary criteria for irreducibility of $f(X^r)$. *Israel J. Math.* **169** (2009), 109–123. MR2460901 (2009i:13045), Zbl 1222.11041, arXiv:1303.5333, doi: 10.1007/s11856-009-0006-0. 1470, 1471

[14] HARRINGTON, J; JONES, L. The irreducibility of power compositional sextic polynomials and their Galois groups. *Math. Scand.* **120** (2017), no. 2, 181–194. MR3657411, Zbl 1414.12001, doi: 10.7146/math.scand.a-25850. 1471

[15] HARRINGTON, JOSHUA; JONES, LENNY. A new condition equivalent to the Ankeny–Artin–Chowla conjecture. *J. Number Theory* **192** (2018), 240–250. MR3841554, Zbl 1460.11130, doi: 10.1016/j.jnt.2018.04.011. 1470

[16] HARRINGTON, JOSHUA; JONES, LENNY. Monogenic cyclotomic compositions. *Kodai Math. J.* **44** (2021), no. 1, 115–125. MR4298893, Zbl 7370873, arXiv:1909.03541, doi: 10.2996/kmj44107. 1467

[17] HELFGOTT, HARALD ANDRÉS. Square-free values of $f(p)$, f cubic. *Acta Math.* **213** (2014), no. 1, 107–135. MR3261012, Zbl 1316.11084, doi: 10.1007/s11511-014-0117-2. 1469

[18] HOOLEY, CHRISTOPHER. Applications of sieve methods to the theory of numbers. Cambridge Tracts in Mathematics, 70. *Cambridge University Press, Cambridge-New York-Melbourne*, (1976). xiv+122 pp. MR0404173 (53 #7976), Zbl 0624.10037. 1469

[19] JONES, LENNY. Sextic reciprocal monogenic dihedral polynomials. *Ramanujan J* (2020). doi: 10.1007/s11139-020-00310-w. 1466

[20] KAPPE, LUISE-CHARLOTTE.; WARREN, BETTE. An elementary test for the Galois group of a quartic polynomial. *Amer. Math. Monthly* **96** (1989), no. 2, 133–137. MR0992075 (90i:12006), Zbl 0702.11075, doi: 10.2307/2323198. 1471

[21] KLÜNERS, JÜRGEN; MALLE, GUNTER. A database for number fields. http://galoisdb.math.upb.de/home. 1466, 1485, 1486, 1489

[22] KOSHY, THOMAS. Fibonacci and Lucas numbers with applications. II. Pure and Applied Mathematics (Hoboken). *John Wiley & Sons, Inc., Hoboken, NJ*, 2019. xviii+729 pp. ISBN: 978-1-118-74208-2. MR3890105, Zbl 1409.11001, doi: 10.1002/9781118742297. 1469, 1470

[23] MASON, JOHN C.; HANDSCOMB, DAVID C. Chebyshev polynomials. *Chapman & Hall/CRC, Boca Raton, FL*, 2003. xiv+341 pp. ISBN: 0-8493-0355-9. MR1937591 (2004h:33001), Zbl 1015.33001, doi: 10.1201/9781420036114. 1469, 1470, 1475

[24] NAGELL, TRYGVE. Introduction to number theory. *John Wiley & Sons, Inc., New York; Almqvist & Wiksell, Stockholm*, 1951. 309 pp. MR0043111 (13,207b) Zbl 0042.26702. 1467

[25] NEUKIRCH, JÜRGEN. Algebraic number theory. Grundlehren der Mathematischen Wissenschaften, 322. *Springer-Verlag, Berlin*, 1999. xviii+571 pp. ISBN: 3-540-65399-6. MR1697859 (2000m:11104), Zbl 1131.11002, doi: 10.1007/978-3-662-03983-0. 1468

[26] PASTEN, HECTOR. 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. MR3327840, Zbl 1337.11065, doi: 10.1142/S1793042115500396. 1469

[27] SCHINZEL, ANDRZEJ. Polynomials with special regard to reducibility. Encyclopedia of Mathematics and its Applications, 77. *Cambridge University Press, Cambridge*, 2000. x+558 pp. ISBN: 0-521-66225-7. MR1770638 (2001h:11135), Zbl 0956.12001, doi: 10.1017/CBO9780511542916. 1467

[28] WASHINGTON, LAWRENCE C. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. *Springer-Verlag, New York*, 1997. xiv+487 pp. ISBN: 0-387-94762-0. MR1421575 (97h:11130), Zbl 0966.11047, doi: 10.1112/blms/15.6.612. 1466

(Lenny Jones) PROFESSOR EMERITUS, DEPARTMENT OF MATHEMATICS, SHIPPENSBURG UNIVERSITY, SHIPPENSBURG, PENNSYLVANIA 17257, USA
lkjone@ship.edu

This paper is available via http://nyjm.albany.edu/j/2021/27-57.html.