ACTA ARITHMETICA
Online First version

The non-unit conjecture for Misiurewicz parameters

by

Robert L. Benedetto and Vefa Goksel

Abstract. A Misiurewicz parameter is a complex number c for which the critical point $z = 0$ under $z^2 + c$ is strictly preperiodic. Such parameters play the same role as special points in dynamical moduli spaces that is played by singular moduli (corresponding to CM elliptic curves) as special points on modular curves. Building on our earlier work, we investigate whether the difference of two Misiurewicz parameters can be an algebraic unit. (The corresponding question for singular moduli was recently answered in the negative by Li.) We answer this dynamical question in many new cases under a widely believed irreducibility assumption.

Introduction. Let $f \in \mathbb{C}[z]$ be a polynomial of degree $d \geq 2$. We denote by f^n the *n-th iterate* of f, which is defined recursively by $f^n = f \circ f^{n-1}$ for $n \geq 2$. We say that f is *post-critically finite* (PCF) if each of its critical points γ has finite orbit $\mathcal{O}_f(\gamma) := \{f^n(\gamma) \,|\, n \geq 1\}$ under iteration of f. In this work, we will focus on the PCF parameters c in the family of quadratic polynomials

$$f_c := z^2 + c \in \mathbb{C}[z],$$

which has been of particular interest in the study of both complex and arithmetic dynamics. Any quadratic polynomial over $\mathbb{C}$ is linearly conjugate to a unique such f_c, so that the family $\{f_c \,|\, c \in \mathbb{C}\}$ is the appropriate dynamical parameter space of quadratic polynomials.

Since 0 is the only (finite) critical point of f_c, the post-critical orbit of f_c is given by

$$\mathcal{O}_{f_c}(0) = \{f_c(0), f_c^2(0), \dots\}.$$

If $x \in \mathbb{C}$ satisfies $f_c^n(x) = x$ for some minimal positive integer n, we say x is *periodic* (of exact period n). If x is not periodic but $f_c^m(x) = f_c^{m+n}(x)$ for some minimal positive integers m and n, we say x is (strictly) *preperiodic of type* (m, n). Note that for any PCF quadratic polynomial f_c, the point 0

2020 *Mathematics Subject Classification*: Primary 37P15; Secondary 11R09, 37P20.
Key words and phrases: post-critically finite, algebraic unit, arithmetic dynamics.
Received 8 September 2025; revised 11 May 2026.
Published online 25 June 2026.

must be either periodic or strictly preperiodic; and in the strictly preperiodic case, we must have $m \geq 2$. For ease of notation, we write

$$a_i = a_i(c) := f_c^i(0) \quad \text{for all } i \geq 1$$

throughout this paper. For $m \geq 2$, $n \geq 1$, the parameters c such that 0 is a preperiodic point of type (m, n) for f_c are called the *Misiurewicz parameters of type* (m, n). They are the roots of a monic polynomial $G_{m,n} \in \mathbb{Z}[c]$ with integer coefficients, defined by

(0.1)

$$G_{m,n}(c) := \prod_{k|n} (a_{m+k-1} + a_{m-1})^{\mu(n/k)} \cdot \begin{cases} \prod_{k|n} (a_k)^{-\mu(n/k)} & \text{if } n \mid m-1, \\ 1 & \text{if } n \nmid m-1. \end{cases}$$

See [2, Theorem 2.1] and [10, Theorem 1.1] for proofs that $G_{m,n}$ is indeed a monic polynomial. See also [2, 3, 4, 5, 7, 8, 10, 13] for further background on the *Misiurewicz polynomials* $G_{m,n}$.

In [1], Baker and DeMarco proposed a dynamical version of the André–Oort Conjecture by relating PCF parameters (including Misiurewicz parameters) in dynamical moduli spaces to special André–Oort points found on Shimura varieties. In this framework, PCF parameters in these moduli spaces play a role similar to that of CM (complex multiplication) points on modular curves, and they are believed to share similar arithmetic characteristics. For additional information on the dynamical André–Oort Conjecture, see [6].

It has been conjectured that $G_{m,n}$ is irreducible over $\mathbb{Q}$ for all $m \geq 2$, $n \geq 1$; see, for example, [12, Remark 3.5] and [14, Exercise 4.17]. Goksel [7, 8], and Buff, Epstein, and Koch [5] have proven this conjecture in some special cases. Although this irreducibility conjecture remains open, our interest in the current paper is in the following related dynamical question.

Question 0.1. *Let c_0 and c_1 be Misiurewicz parameters of type (m, n) and (k, ℓ), where $(m, n) \neq (k, \ell)$. Under what conditions is the difference $c_0 - c_1$ an algebraic unit?*

If $G_{k,\ell}$ is irreducible not only over $\mathbb{Q}$, but also over $\mathbb{Q}(c_0)$, as computational evidence has suggested, then Question 0.1 would be equivalent to the following question.

Question 0.2. *Let $m, k \geq 2$, and $n, \ell \geq 1$. Let c_0 be a Misiurewicz parameter of type (m, n), and suppose that $(m, n) \neq (k, \ell)$. Under what conditions is $G_{k,\ell}(c_0)$ an algebraic unit?*

We answered Question 0.2 in many cases in [2, 3]; the only remaining case is when $m = k$ and ℓ is a proper divisor of n. In [3, Conjecture 1.3], we conjectured that $G_{m,\ell}(c_0)$ is never an algebraic unit in this case, and in [3, Theorem 1.7], we proved this conjecture in the cases $\ell = 1, 2$, under the assumption that $G_{m,n}$ is irreducible over $\mathbb{Q}$.

Our main result in the present paper generalizes [3, Theorem 1.7] to many new periods ℓ, under the same irreducibility assumption.

THEOREM 0.3. *Let $m \geq 2$, and p be a prime not exceeding* 1021. *Let $n \neq p$ be a positive integer divisible by p. Let c_0 be a root of $G_{m,n}$. Suppose that $G_{m,p}$ and $G_{m,n}$ are irreducible over $\mathbb{Q}$. Then $G_{m,p}(c_0)$ is not an algebraic unit.*

Theorem 0.3 may be considered a dynamical analogue of a recent result of Li [11] on *singular moduli*, which are j-invariants of elliptic curves with CM. In their seminal work [9], Gross and Zagier found an explicit factorization of the algebraic norm of differences of singular moduli, showing that these have many small prime divisors in many cases. The question of whether those differences can be algebraic units or not has been a long-standing conjecture in arithmetic geometry. In a recent breakthrough, Li [11] proved that such differences can never be algebraic units, and he used this result to generalize the effective results of André–Oort type. In the notation of Theorem 0.3, if $G_{m,p}$ is irreducible not only over $\mathbb{Q}$, but even over $\mathbb{Q}(c_0)$, then by the resulting equivalence of Questions 0.1 and 0.2 mentioned above, Theorem 0.3 would yield the corresponding result for such Misiurewicz parameters: that the difference of a root of $G_{m,n}$ and a root of $G_{m,p}$ cannot be an algebraic unit.

The outline of the paper is as follows. We introduce key terminology including multiplier polynomials and p-specialness in Section 1, where we also prove several results about sums of roots of certain polynomials. (We introduced p-specialness in [3] to study Question 0.1, but in this paper we push the concept further, making heavy use of the elementary complex analysis result of Proposition 1.8.) Section 2 is devoted to the statement and proof of Theorem 2.1, relating the coefficients of certain multiplier polynomials. The proof requires several technical lemmas, for which we make repeated use of Proposition 1.8. In Section 3, we combine these ingredients to prove Theorem 0.3 by inductively showing that the relevant multiplier polynomials are 2-special. Finally, Section 4 is an appendix exhibiting some computational data needed to verify the base cases of Section 3.

1. Preliminaries. If $f \in \mathbb{C}[z]$ is a polynomial, and if $x \in \mathbb{C}$ is periodic of exact period $n \geq 1$, the *multiplier* $\lambda \in \mathbb{C}$ of x is defined by

$$\lambda := (f^n)'(x) = \prod_{i=0}^{n-1} f'(f^i(x)). \tag{1.1}$$

The multiplier λ is the same for each point $x, f(x), f^2(x), \ldots, f^{n-1}(x)$ of the forward orbit of x, and hence we may refer to the multiplier of the periodic cycle.

Let $m \geq 2$ and $n \geq 1$. Now consider a root α of $G_{m,n}$. Since $f_\alpha(z) = z^2+\alpha$ has $f'_\alpha(z) = 2z$, and since $a_{m+n-1}(\alpha) + a_{m-1}(\alpha) = 0$, equation (1.1) shows that the multiplier of the periodic cycle $\{a_m(\alpha), \ldots, a_{m+n-1}(\alpha)\}$ is

$$\lambda_{m,n}(\alpha) = 2^n \prod_{i=0}^{n-1} a_{m+i}(\alpha) = -2^n \prod_{i=0}^{n-1} a_{m+i-1}(\alpha). \tag{1.2}$$

We are thus led to define the following *multiplier polynomial*, which has the multipliers $\lambda_{m,n}(\alpha)$ as roots, where α runs through the roots of $G_{m,n}$.

DEFINITION 1.1. Let $m \geq 2$ and $n \geq 1$ be integers. Let $\alpha_1, \ldots, \alpha_k$ be all the roots of $G_{m,n}$. The *multiplier polynomial* $P_{m,n}$ associated with $G_{m,n}$ is

$$P_{m,n}(x) = \prod_{j=1}^{k} (x - \lambda_{m,n}(\alpha_j)) \in \mathbb{Z}[x],$$

where $\lambda_{m,n}(\cdot)$ is defined as in (1.2).

We will make use of the following two results and one definition from [3]. Throughout the present paper, for any prime p, we write v_p for the p-adic valuation on $\mathbb{Z}$, normalized so that $v_p(p) = 1$. We also denote by Φ_i the i-th cyclotomic polynomial.

PROPOSITION 1.2 ([3, Proposition 5.3]). *Let $m, n \geq 2$ be integers. Let α be a root of $G_{m,n}$. Let $\ell \geq 1$ be a proper divisor of n, and suppose that* $\mathrm{Res}(P_{m,\ell}, \Phi_{n/\ell}) \neq \pm 1$. *If $G_{m,n}$ and $G_{m,\ell}$ are irreducible over $\mathbb{Q}$, then $G_{m,\ell}(\alpha)$ is not an algebraic unit.*

DEFINITION 1.3 ([3, Definition 6.1]). Let $P(x) = x^i + A_{i-1}x^{i-1} + \cdots + A_1 x + A_0 \in \mathbb{Z}[x]$ be a monic polynomial with integer coefficients. Let p be a prime number. We say that $P(x)$ is *p-special* if it satisfies the following two conditions:

(a) $v_p(A_{i-1}) > v_p(2)$,
(b) $v_p(A_j) > v_p(A_{i-1})$ for $j = 0, 1, \ldots, i-2$.

THEOREM 1.4 ([3, Theorem 6.2]). *Let $P(x) \in \mathbb{Z}[x]$ be a p-special polynomial for some prime p. Then for every integer $\ell \geq 1$, we have $|\mathrm{Res}(P, \Phi_\ell)| > 1$, where $\Phi_\ell(x) \in \mathbb{Z}[x]$ is the ℓ-th cyclotomic polynomial.*

Our next result will be useful for proving that multiplier polynomials are 2-special. In particular, it shows that for $p = 2$, point (a) of Definition 1.3 holds for multiplier polynomials, and it provides a useful lower bound for the valuations that arise in point (b).

PROPOSITION 1.5. *Let $m \geq 2$ and $n \geq 1$ be integers, and let $P_{m,n}(x) = x^k + \sum_{i=0}^{k-1} b_i x^i$ be the associated multiplier polynomial. Then for each $\ell =$*

$1, \dots, k$, *we have*

$$v_2(b_{k-\ell}) \geq n\ell + 1.$$

Proof. Let $\alpha_1, \dots, \alpha_k$ be the roots of $G_{m,n}$. Since $G_{m,n}(c) \in \mathbb{Z}[c]$ is monic, each α_i is an algebraic integer. Because $a_j(c) \in \mathbb{Z}[c]$ for each $j \geq 1$, it follows that each $a_j(\alpha_i)$ is also an algebraic integer, so that $v_2(a_j(\alpha_i)) \geq 0$ for any extension of the valuation v_2 to $\mathbb{Q}(\alpha_i)$.

Furthermore, for any j divisible by n, we have $v_2(a_j(\alpha_i)) > 0$, by [7, Theorem 1.3] (or by [2, Theorem 3.3]). Thus, the multiplier $\lambda_i = \lambda_{m,n}(\alpha_i)$ satisfies

$$v_2(\lambda_i) = v_2\Big(2^n \prod_{j=0}^{n-1} a_{m+j-1}(\alpha_i)\Big) > nv_2(2)$$

by (1.2), together with the fact that $n \mid (m+j-1)$ for some $0 \leq j \leq n-1$. By the definition of $P_{m,n}$, it follows that $v_2(b_{k-\ell}) > n\ell v_2(2)$, since $b_{k-\ell}$ is a homogeneous polynomial in $\lambda_1, \dots, \lambda_k$ of degree ℓ. Finally, because $b_{k-\ell} \in \mathbb{Z}$, its 2-adic valuation is an integer, and therefore $v_2(b_{k-\ell}) \geq n\ell + 1$. ∎

The following definition will be handy in the computations throughout the paper.

Definition 1.6. Let K be a field, and let $f, g \in K[x]$ with $g \neq 0$. Define $T(f,g) \in K$ to be the sum of $f(c_i)$ over all the roots c_i of g, repeated according to multiplicity.

The following lemma establishes some basic properties of $T(f,g)$.

Lemma 1.7. *Let K be a field. Then:*

(a) *T is linear in the first coordinate, i.e.,*

$$T(af,h) = aT(f,h) \quad \text{and} \quad T(f+g,h) = T(f,h) + T(g,h)$$

for any $a \in K$ and $f, g, h \in K[x]$ with $h \neq 0$.

(b) *$T(f,gh) = T(f,g) + T(f,h)$ for any $f,g,h \in K[x]$ with $g,h \neq 0$.*

Proof. Immediate from the definition. ∎

Our next result, an elementary fact from complex analysis, will be essential in many proofs in this section.

Proposition 1.8. *Let $f, g \in \mathbb{C}[x]$ be polynomials such that $f(0) = g(0) = 0$. Let $0 = c_1, c_2, \dots, c_k$ be the roots of g, and assume that none are multiple roots. Let $h \in \mathbb{C}[x]$ be the remainder when fg' is divided by the polynomial $g(x)/x$, i.e., $\deg h < \deg g - 1$ and $h \equiv fg' \pmod{g/x}$. Then*

$$T(f,g) = -\frac{h(0)}{g'(0)}.$$

Proof. For any large enough radius $R > 0$, we know from complex analysis that

$$\frac{1}{2\pi i}\oint_{|z|=R}\frac{h(z)\,dz}{g(z)} = \sum_{i=1}^{k}\operatorname{resid}\left(\frac{h}{g}, c_i\right), \tag{1.3}$$

where $\operatorname{resid}(F, c)$ denotes the residue of $F(z)$ at $z = c$. Since g has only simple roots, we have $\operatorname{resid}(h/g, c_i) = h(c_i)/g'(c_i)$. On the other hand, for sufficiently large $|z|$, we have $|h(z)/g(z)| = O(|z|^{-2})$, because $\deg g - \deg h \geq 2$. Thus, taking the limit of equation (1.3) as $R \to \infty$, we obtain

$$\sum_{i=1}^{k}\frac{h(c_i)}{g'(c_i)} = 0. \tag{1.4}$$

By our choice of h, we have $h(c_i)/g'(c_i) = f(c_i)$ for $i = 2, \dots, k$. Hence, we obtain

$$\sum_{i=2}^{k}\frac{h(c_i)}{g'(c_i)} = \sum_{i=2}^{k} f(c_i).$$

From $f(c_1) = f(0) = 0$ and (1.4), the desired identity follows immediately. ∎

Recall that the trace $\operatorname{tr}(P)$ of a monic polynomial $P(x)$ of degree $n \geq 1$ is the sum of its roots, or equivalently, the negative of the x^{n-1}-coefficient of P. Our next result provides an explicit formula for the trace of the multiplier polynomial $P_{m,n}$.

LEMMA 1.9. *Let $m \geq 2$ and $n \geq 1$. Then*

$$\operatorname{tr}(P_{m,n}) = 2^n \sum_{d|n} (-1)^{n/d}\mu\left(\frac{n}{d}\right) T\left(\left(\prod_{i=m-1}^{m+d-2} a_i\right)^{n/d}, a_{m+d-1} + a_{m-1}\right).$$

Proof. First assume that $n \nmid m-1$. Then we have

$$\begin{aligned}
\operatorname{tr}(P_{m,n}) &= T\left(2^n \prod_{i=m}^{m+n-1} a_i, G_{m,n}\right)\\
&= 2^n T\left(\prod_{i=m}^{m+n-1} a_i, \prod_{d|n}(a_{m+d-1} + a_{m-1})^{\mu(n/d)}\right)\\
&= 2^n \sum_{d|n}\mu\left(\frac{n}{d}\right) T\left(\prod_{i=m}^{m+n-1} a_i, a_{m+d-1} + a_{m-1}\right)\\
&= 2^n \sum_{d|n} (-1)^{n/d}\mu\left(\frac{n}{d}\right) T\left(\left(\prod_{i=m-1}^{m+d-2} a_i\right)^{n/d}, a_{m+d-1} + a_{m-1}\right),
\end{aligned}$$

where we used Lemma 1.7(a) in the second equality and Lemma 1.7(b) in the third. The fourth equality also holds by periodicity and the fact that for any root c of $a_{m+d-1}+a_{m-1}$, we have $a_{m+d-1}(c)=-a_{m-1}(c)$. Thus, we are done in this case.

We now assume $n\,|\,m-1$. By the first part of the proof and using Lemma 1.7(b), we have

$$\begin{aligned}\operatorname{tr}(P_{m,n}) &= T\Big(2^n\prod_{i=m}^{m+n-1}a_i, G_{m,n}\Big)\\ &= 2^n\Big(T\Big(\prod_{i=m}^{m+n-1}a_i, \prod_{d|n}(a_{m+d-1}+a_{m-1})^{\mu(n/d)}\Big)-T\Big(\prod_{i=m}^{m+n-1}a_i, \prod_{d|n}a_d^{\mu(n/d)}\Big)\Big)\\ &= 2^n\sum_{d|n}\mu\Big(\frac{n}{d}\Big)\Big(T\Big(\prod_{i=m}^{m+n-1}a_i, a_{m+d-1}+a_{m-1}\Big)-T\Big(\prod_{i=m}^{m+n-1}a_i, a_d\Big)\Big)\\ &= 2^n\sum_{d|n}(-1)^{n/d}\mu\Big(\frac{n}{d}\Big)T\Big(\Big(\prod_{i=m-1}^{m+d-2}a_i\Big)^{n/d}, a_{m+d-1}+a_{m-1}\Big).\end{aligned}$$

Note that the fourth equality holds because for any root c of a_d, by periodicity, $a_{dk}(c)=0$ for any $k\ge 1$, thus $a_i(c)=0$ for some $i\in\{m,m+1,\ldots,m+n-1\}$. ∎

Since the case that $n=p$ is a prime is of particular interest for our main result, we now use Lemma 1.9 to describe $\operatorname{tr}(P_{m,p})$ for any odd prime p.

THEOREM 1.10. *Let $m\ge 3$, and let $p\ge 3$ be an odd prime number. Then*

$$\operatorname{tr}(P_{m,p}) = 2^p\big(T(a_{m-1}^p, a_m+a_{m-1}) + 2^{m+p-2}-2^{m-2}\big).$$

Proof. By Lemma 1.9, we have

$$\begin{aligned}\operatorname{tr}(P_{m,p}) &= 2^p\sum_{d|p}(-1)^{p/d}\mu\Big(\frac{p}{d}\Big)T\Big(\Big(\prod_{i=m-1}^{m+d-2}a_i\Big)^{p/d}, a_{m+d-1}+a_{m-1}\Big)\\ &= 2^p\Big(T(a_{m-1}^p, a_m+a_{m-1}) - T\Big(\prod_{i=m-1}^{m+p-2}a_i, a_{m+p-1}+a_{m-1}\Big)\Big).\end{aligned}\tag{1.5}$$

In the rest of the proof, for any polynomial $g\in\mathbb{Z}[c]$, we denote by $\overline{g}\in\mathbb{Z}[c]$ the remainder of g when divided by $(a_{m+p-1}+a_{m-1})/c$. In particular, if $\deg g<\deg((a_{m+p-1}+a_{m-1})/c)$, then $g=\overline{g}$.

By Proposition 1.8, we have

$$T\Big(\prod_{i=m-1}^{m+p-2} a_i, a_{m+p-1}+a_{m-1}\Big) = -\overline{H}(0)/2,$$

where $H = (\prod_{i=m-1}^{m+p-2} a_i)(a'_{m+p-1}+a'_{m-1})$. Write $H = A + B$, where

$$A = a'_{m+p-1}\prod_{i=m-1}^{m+p-2} a_i \quad \text{and} \quad B = a'_{m-1}\prod_{i=m-1}^{m+p-2} a_i.$$

To compute $\overline{H}$, we will now separately calculate the remainders $\overline{A}$ and $\overline{B}$ of A and B when divided by $(a_{m+p-1}+a_{m-1})/c$.

Remainder of A. Since $a_{m+p-1} = a_{m+p-2}^2 + c$, we deduce that $a'_{m+p-1} = 2a_{m+p-2}a'_{m+p-2} + 1$, and hence

$$A = A_1 + A_2, \quad \text{where} \quad A_1 = 2a_{m+p-2}a'_{m+p-2}\prod_{i=m-1}^{m+p-2} a_i, \quad A_2 = \prod_{i=m-1}^{m+p-2} a_i.$$

We first consider A_2. Note that

$$\deg A_2 = \sum_{i=m-1}^{m+p-2} 2^{i-1} = 2^{m+p-2} - 2^{m-2}. \tag{1.6}$$

Since $m \geq 3$, we have $\deg A_2 < 2^{m+p-2} - 1 = \deg((a_{m+p-1}+a_{m-1})/c)$, and hence $\overline{A_2} = A_2$, which vanishes at 0.

We now consider A_1. Noting that

$$a_{m+p-2}^2 = a_{m+p-1} - c \equiv -a_{m-1} - c \pmod{(a_{m+p-1}+a_{m-1})/c},$$

we obtain

$$A_1 \equiv 2a'_{m+p-2}(-a_{m-1}-c)\prod_{i=m-1}^{m+p-3} a_i = -C_1 - C_2 \pmod{(a_{m+p-1}+a_{m-1})/c},$$

where

$$C_1 = 2a'_{m+p-2}a_{m-1}\prod_{i=m-1}^{m+p-3} a_i, \qquad C_2 = 2ca'_{m+p-2}\prod_{i=m-1}^{m+p-3} a_i.$$

By direct computation, we obtain

$$\begin{aligned}\deg C_1 &= 2^{m+p-3} - 1 + 2^{m-2} + \sum_{i=m-1}^{m+p-3} 2^{i-1} \\ &= 2^{m+p-2} - 1 = \deg((a_{m+p-1}+a_{m-1})/c).\end{aligned}$$

Thus, by comparing the leading coefficients, we have

$$\overline{C}_1 = C_1 - 2^{m+p-2}\frac{a_{m+p-1}+a_{m-1}}{c},$$

which evaluates to -2^{m+p-1} at 0.

We also have

$$\deg C_2 = 1 + 2^{m+p-3} - 1 + \sum_{i=m-1}^{m+p-3} 2^{i-1} = 2^{m+p-2} - 2^{m-2}. \tag{1.7}$$

As with A_2 above, we have $\deg C_2 < \deg((a_{m+p-1} + a_{m-1})/c)$, since $m \geq 3$. Thus, $\overline{C}_2 = C_2$, which vanishes at 0.

Combining the foregoing computations, we conclude that

$$\overline{A}(0) = -\overline{C}_1(0) - \overline{C}_2(0) + \overline{A}_2(0) = 2^{m+p-1}. \tag{1.8}$$

Remainder of B. We have

$$\deg B = 2^{m-2} - 1 + \sum_{i=m-1}^{m+p-2} 2^{i-1} = 2^{m+p-2} - 1 = \deg((a_{m+p-1} + a_{m-1})/c).$$

Therefore, by comparing the leading coefficients, we obtain

$$\overline{B} = B - 2^{m-2} \frac{a_{m+p-1} + a_{m-1}}{c},$$

which evaluates to -2^{m-1} at 0. Thus, we conclude that

$$\overline{B}(0) = -2^{m-1}. \tag{1.9}$$

Applying Proposition 1.8 to $H = A + B$, together with (1.8) and (1.9), yields

$$\begin{aligned} T\Big(\prod_{i=m-1}^{m+p-2} a_i, a_{m+p-1} + a_{m-1}\Big) &= -\overline{H}(0)/2 = -\tfrac{1}{2}(\overline{A}(0) + \overline{B}(0)) \\ &= 2^{m-2} - 2^{m+p-2}. \end{aligned}$$

Plugging this value into (1.5) completes the proof. ∎

REMARK 1.11. We assumed $m \geq 3$ in Theorem 1.10, but the computations are only modestly more involved when $m = 2$. In particular, in that case, equations (1.6) and (1.7) yield

$$\deg A_2 = \deg C_2 = \deg((a_{p+1} + a_1)/c).$$

Therefore, comparing the leading coefficients, we obtain

$$\overline{A}_2 = A_2 - \frac{a_{p+1} + a_1}{c} \quad \text{and} \quad \overline{C}_2 = C_2 - 2^p \left(\frac{a_{p+1} + a_1}{c}\right).$$

Because $(a_{p+1} + a_1)/c$ evaluates to 2 at $c = 0$, it follows that

$$\overline{A}_2(0) = -2 \quad \text{and} \quad \overline{C}_2(0) = -2^{p+1}.$$

We still have $\overline{C}_1(0) = -2^{p+1}$ and $\overline{B}(0) = -2$ from the proof of Theorem 1.10, and therefore

$$T\Big(\prod_{i=1}^{p} a_i, a_{p+1} + a_1\Big) = -\frac{1}{2}(2^{p+1} + 2^{p+1} - 2 - 2) = 2 - 2^{p+1}.$$

We also have $a_2 + a_1 = c^2 + 2c$, and hence the roots of $a_2 + a_1$ are simply $c_1 = 0$ and $c_2 = -2$. Thus,

$$T(a_1^p, a_2 + a_1) = T(c^p, a_2 + a_1) = 0^2 + (-2)^p = -2^p,$$

by direct computation. Equation (1.5) then gives us

$$\operatorname{tr}(P_{2,p}) = 2^p(-2^p - (2 - 2^{p+1})) = 2^p(2^p - 2) = 2^{2p} - 2^{p+1}.$$

REMARK 1.12. In the proof of Theorem 1.10 and in Remark 1.11, we never used the fact that p is prime when calculating the expression

$$T\Big(\prod_{i=m-1}^{m+p-2} a_i, a_{m+p-1} + a_{m-1}\Big).$$

In particular, then, we have the formula

$$T\Big(\prod_{i=m-1}^{m+n-2} a_i, a_{m+n-1} + a_{m-1}\Big) = \begin{cases} 2 - 2^{n+1} & \text{if } m = 2, \\ 2^{m-2} - 2^{m+n-2} & \text{if } m \geq 3 \end{cases}$$

for any integers $m \geq 2$ and $n \geq 1$.

2. A trace relation for multiplier polynomials. The following result relates the coefficients of the multiplier polynomials $P_{m,n}$ under certain conditions on m and n. Combined with [3, Lemma 6.3], it will allow us to establish the 2-specialness of the polynomials $P_{m,p}$ when p is a prime less than 1024.

THEOREM 2.1. *Let $m \geq 3$ and $n \geq 1$. Write*

$$(P_{m,n}(x))^2 = x^k + \sum_{i=0}^{k-1} b_i x^i \quad \text{and} \quad P_{m+1,n}(x) = x^\ell + \sum_{i=0}^{\ell-1} c_i x^i,$$

where $k = 2\deg P_{m,n} = 2\deg G_{m,n}$ and $\ell = \deg P_{m+1,n} = \deg G_{m+1,n}$. For each integer $i \geq 1$ such that $\lfloor ni/2 \rfloor \leq 2^{m-2} - 2$, we have $b_{k-i} = c_{\ell-i}$.

COROLLARY 2.2. *Let $m \geq 3$ and $n \geq 1$. Suppose that $\lfloor n/2 \rfloor \leq 2^{m-2} - 2$. Then $\operatorname{tr}(P_{m+1,n}) = 2\operatorname{tr}(P_{m,n})$.*

Proof. Since we have $\operatorname{tr}(P_{m,n}^2) = 2\operatorname{tr}(P_{m,n})$, Corollary 2.2 immediately follows from Theorem 2.1 with $i = 1$. ■

The rest of this section is devoted to the proof of Theorem 2.1. We need several lemmas, some of which we discovered through empirical observations in Magma.

NOTATION 2.3. In this section, whenever we have integers $m \geq 2$ and $n \geq 1$, and a polynomial $f \in \mathbb{Z}[c]$, we denote by $\overline{f} \in \mathbb{Z}[c]$ the remainder of f when divided by $(a_{m+n-1} + a_{m-1})/c$.

LEMMA 2.4. *Fix positive integers $\ell, s \geq 1$ with $\ell \leq s+1$. Then*

$$a_\ell \prod_{j=\ell}^{s} a_j = a_{s+1} - c \sum_{i=\ell+1}^{s+1} \prod_{j=i}^{s} a_j,$$

where we understand an empty sum to be 0*, and an empty product to be* 1*.*

Proof. Fix s, and proceed by decreasing induction on ℓ.

For $\ell = s+1$, both sides are simply a_{s+1}, verifying the equality. Assuming the claim for $\ell+1$, we have

$$\begin{aligned} a_\ell \prod_{j=\ell}^{s} a_j &= a_\ell^2 \prod_{j=\ell+1}^{s} a_j = (a_{\ell+1} - c) \prod_{j=\ell+1}^{s} a_j = a_{\ell+1} \prod_{j=\ell+1}^{s} a_j - c \prod_{j=\ell+1}^{s} a_j \\ &= a_{s+1} - c \sum_{i=\ell+2}^{s+1} \prod_{j=i}^{s} a_j - c \prod_{j=\ell+1}^{s} a_j = a_{s+1} - c \sum_{i=\ell+1}^{s+1} \prod_{j=i}^{s} a_j, \end{aligned}$$

where the second equality is because $a_{\ell+1} = a_\ell^2 + c$, and the fourth is by our inductive assumption. ∎

LEMMA 2.5. *Fix an integer $1 \leq \ell \leq m+n-1$, and let $R \in \mathbb{Z}[c]$. Define*

$$H = Ra_\ell \prod_{j=\ell}^{m+n-2} a_j \in \mathbb{Z}[c].$$

If $\deg R \leq \min\{2^{m+n-2} - 2^{m-2} - 2, 2^\ell - 3\}$*, then* $\overline{H}(0) = 0$.

Proof. Since $a_{m+n-1} \equiv -a_{m-1} \pmod{(a_{m+n-1}+a_{m-1})/c}$, it follows from Lemma 2.4 that H is congruent to

$$-R(a_{m-1} + cQ), \quad \text{where} \quad Q = \sum_{i=\ell+1}^{m+n-1} \prod_{j=i}^{m+n-2} a_j. \tag{2.1}$$

If $\ell = m+n-1$, then $Q = 0$; otherwise, the highest degree term in the sum defining Q is the $i = \ell+1$ term, and hence

$$\deg(cQ) = 1 + \sum_{j=\ell+1}^{m+n-2} 2^{j-1} = 1 + 2^{m+n-2} - 2^\ell.$$

Thus,

$$\begin{aligned} \deg(-R(a_{m-1} + cQ)) &\leq \deg R + \max\{2^{m-2}, 1 + 2^{m+n-2} - 2^\ell\} \\ &\leq 2^{m+n-2} - 2 < \deg((a_{m+n-1} + a_{m-1})/c), \end{aligned}$$

and hence $\overline{H} = -R(a_{m-1} + cQ)$. Since both a_{m-1} and c are zero at $c = 0$, it follows that $\overline{H}(0) = 0$. ∎

Lemma 2.6. *Let $\{i_1,\ldots,i_t\}$ be a non-empty, proper subset of $\{m-1, m,\ldots,m+n-2\}$ with $i_1<\cdots<i_t$. If $0\le k\le 2^{m-2}-2$, then*

$$T\Big(c^k\prod_{j=1}^t a_{i_j}, a_{m+n-1}+a_{m-1}\Big)=0.$$

Proof. By Proposition 1.8, we have

$$T\Big(c^k\prod_{j=1}^t a_{i_j}, a_{m+n-1}+a_{m-1}\Big)=-\overline{H}(0)/2,$$

where $H=c^k(a'_{m+n-1}+a'_{m-1})\prod_{s=1}^t a_{i_s}$. We will prove the lemma by showing that the polynomials $\overline{H}_1$ and $\overline{H}_2$ both vanish at $c=0$, where

$$H_1=c^k a'_{m-1}\prod_{s=1}^t a_{i_s}\quad\text{and}\quad H_2=c^k a'_{m+n-1}\prod_{s=1}^t a_{i_s}.$$

We have

$$\begin{aligned}\deg H_1&=k+(2^{m-2}-1)+\sum_{s=1}^t 2^{i_s-1}\le k-1+\sum_{j=m-1}^{m+n-2}2^{j-1}\\&\le 2^{m+n-2}-3<2^{m+n-2}-1=\deg((a_{m+n-1}+a_{m-1})/c),\end{aligned}$$

where in the first inequality we have invoked the fact that $\{i_1,\ldots,i_t\}$ is a *proper* subset of $\{m-1,\ldots,m+n-2\}$ to absorb the 2^{m-2} into the sum, and in the second we have used the fact that $k\le 2^{m-2}-2$. It follows that $\overline{H}_1=H_1$, which vanishes at $c=0$ because $t\ge 1$.

We now consider H_2. Note that for any $r\ge 2$, we have $a_r=c+a_{r-1}^2$, and hence

$$a'_r=1+2a_{r-1}a'_{r-1}. \tag{2.2}$$

Applying this formula inductively, starting from $a'_1=1$, we obtain

$$a'_r=\sum_{i=0}^{r-1}2^i\prod_{j=r-i}^{r-1}a_j,$$

where we understand the empty product in the $i=0$ term to be 1. Therefore,

$$H_2=c^k a'_{m+n-1}\prod_{s=1}^t a_{i_s}=\sum_{i=0}^{m+n-2}\Big(2^i c^k\Big(\prod_{s=1}^t a_{i_s}\Big)\prod_{j=m+n-i-1}^{m+n-2}a_j\Big). \tag{2.3}$$

For each $0\le i\le m+n-2$, the i-th term of the sum in (2.3) is

$$H_{2,i}=2^i c^k\Big(\prod_{s=1}^t a_{i_s}\Big)\prod_{j=m+n-i-1}^{m+n-2}a_j.$$

It suffices to show that for each such i, we have $\overline{H}_{2,i}(0) = 0$. We consider two cases.

First, suppose that $i_t < m+n-i-1$. Then because $m-1 \le i_1 < \cdots < i_t < m+n-i-1$, we have

$$\begin{aligned}\deg H_{2,i} &= k + \sum_{s=1}^{t} 2^{i_s-1} + \sum_{j=m+n-i-1}^{m+n-2} 2^{j-1} \le 2^{m-2} - 2 + \sum_{j=m-1}^{m+n-2} 2^{j-1} \\ &= 2^{m+n-2} - 2 < 2^{m+n-2} - 1 = \deg((a_{m+n-1} + a_{m-1})/c),\end{aligned}$$

and as before it follows that $\overline{H}_{2,i} = H_{2,i}$, which vanishes at 0.

Second, suppose that $i_t \ge m+n-i-1$. Let $\ell = i_t$, so that $m-1 \le \ell \le m+n-2$. Then we have

$$H_{2,i} = Ra_\ell \prod_{j=\ell}^{m+n-2} a_j, \quad \text{where} \quad R = 2^i c^k \Big(\prod_{s=1}^{t-1} a_{i_s}\Big) \prod_{j=m+n-i-1}^{\ell-1} a_j.$$

We will show that

$$\deg R \le \min\{2^{m+n-2} - 2^{m-2} - 2, 2^\ell - 3\}, \tag{2.4}$$

from which it follows, by Lemma 2.5, that $\overline{H}_{2,i}(0) = 0$.

Observe that

$$\begin{aligned}\deg R &= k + \sum_{s=1}^{t-1} 2^{i_s-1} + \sum_{j=m+n-i-1}^{\ell-1} 2^{j-1} \\ &\le (2^{m-2} - 2) + \Big(\sum_{s=1}^{t-1} 2^{i_s-1}\Big) + (2^{\ell-1} - 2^{m+n-i-2}) \\ &\le (2^{\ell-1} - 2^{m+n-i-2} - 2) + 2^{m-2} + \sum_{j=m-1}^{\ell-1} 2^{j-1} \\ &= (2^{\ell-1} - 2^{m+n-i-2} - 2) + 2^{\ell-1} \le 2^\ell - 3,\end{aligned} \tag{2.5}$$

where the second inequality is because $i_1 \ge m-1$, and the third is because $i \le m+n-2$, and hence $2^{m+n-i-2} \ge 1$. If $\ell \le m+n-3$, then because $n \ge 1$, we have

$$2^\ell - 3 \le 2^{m+n-3} - 3 < 2^{m+n-2} - 2^{m-2} - 2,$$

so that inequality (2.5) proves the bound (2.4) in that case.

Otherwise, we have $\ell = m+n-2$. Recalling that $\{i_1, \ldots, i_t\}$ is a proper subset of $\{m-1, m, \ldots, m+n-2\}$, we deduce that

$$\sum_{s=1}^{t-1} 2^{i_s-1} \le \Big(\sum_{j=m-1}^{\ell-1} 2^{j-1}\Big) - 2^{m-2} = 2^{\ell-1} - 2^{m-1}.$$

Thus, (2.5) gives us

$$\begin{aligned}\deg R &\le (2^{m-2}-2)+(2^{\ell-1}-2^{m-1})+(2^{\ell-1}-2^{m+n-i-2})\\ &= 2^{\ell}-2^{m-2}-2^{m+n-i-2}-2 < 2^{m+n-2}-2^{m-2}-2,\end{aligned}$$

completing the proof of (2.4) and hence of Lemma 2.6. ■

LEMMA 2.7. *Let* $1 \le k \le 2^{m-2}-2$. *Then*

$$T\Big(c^k \prod_{j=m-1}^{m+n-2} a_j, a_{m+n-1}+a_{m-1}\Big) = \Big(\frac{1}{2^n}-1\Big)T(c^k, a_{m+n-1}+a_{m-1}).$$

Proof. By Proposition 1.8, we have

$$T\Big(c^k \prod_{j=m-1}^{m+n-2} a_j, a_{m+n-1}+a_{m-1}\Big) = -\overline{H}(0)/2$$

and

$$T(c^k, a_{m+n-1}+a_{m-1}) = -\overline{G}(0)/2,$$

where

$$H = c^k(a'_{m+n-1}+a'_{m-1}) \prod_{j=m-1}^{m+n-2} a_j \quad \text{and} \quad G = c^k(a'_{m+n-1}+a'_{m-1}).$$

Write $H = A + B$ where

$$A = c^k a'_{m-1} \prod_{j=m-1}^{m+n-2} a_j \quad \text{and} \quad B = c^k a'_{m+n-1} \prod_{j=m-1}^{m+n-2} a_j.$$

By (2.2), we have $a_{r-1}a'_{r-1} = \frac{1}{2}(a'_r - 1)$ for any $r \ge 2$. Applying this formula inductively, we have

$$\begin{aligned}A &= c^k(a_{m-1}a'_{m-1}) \prod_{j=m}^{m+n-2} a_j = \frac{c^k}{2}a'_m \prod_{j=m}^{m+n-2} a_j - \frac{c^k}{2}\prod_{j=m}^{m+n-2} a_j\\ &= \cdots = \frac{c^k}{2^n}a'_{m+n-1} - \sum_{i=1}^{n}\frac{c^k}{2^i}\prod_{j=m+i-1}^{m+n-2} a_j.\end{aligned}$$

For each $i = 1, \dots, n$, the i-th term in the sum above has degree

$$\begin{aligned}\deg\Big(c^k \prod_{j=m+i-1}^{m+n-2} a_j\Big) &= k + \sum_{j=m+i-1}^{m+n-2} 2^{j-1} \le 2^{m-2}-2+2^{m+n-2}-2^{m+i-2}\\ &< 2^{m+n-2}-1 = \deg((a_{m+n-1}+a_{m-1})/c),\end{aligned}$$

and since $k \ge 1$, has value 0 at $c = 0$. Thus, $\overline{A}(0) = 2^{-n}\overline{A}_0(0)$, where $A_0 = c^k a'_{m+n-1}$.

Next, we turn to B. Writing

$$\begin{aligned} a'_{m+n-1}a_{m+n-2} &= (2a_{m+n-2}a'_{m+n-2}+1)a_{m+n-2} \\ &= 2a^2_{m+n-2}a'_{m+n-2}+a_{m+n-2} \\ &= 2(a_{m+n-1}-c)a'_{m+n-2}+a_{m+n-2}, \end{aligned}$$

we have $B = B_1 - B_2 + B_3$, where

$$B_1 = 2c^k a_{m+n-1}a'_{m+n-2}\prod_{j=m-1}^{m+n-3} a_j, \qquad B_2 = 2c^{k+1}a'_{m+n-2}\prod_{j=m-1}^{m+n-3} a_j,$$

and

$$B_3 = c^k \prod_{j=m-1}^{m+n-2} a_j.$$

Since $1 \le k \le 2^{m-2}-2$, it is straightforward to check that

$$\deg B_2, \deg B_3 < 2^{m+n-2}-1 = \deg((a_{m+n-1}+a_{m-1})/c),$$

and that $B_2(0) = B_3(0) = 0$. Therefore, because $a_{m+n-1} \equiv -a_{m-1} \pmod{(a_{m+n-1}+a_{m-1})/c}$, we have $\overline{B}(0) = \overline{B}_1(0) = -\overline{C}_1(0)$, with

$$\begin{aligned} C_1 &= 2c^k a'_{m+n-2}a_{m-1}\prod_{j=m-1}^{m+n-3} a_j \\ &= 2c^k a_{m+n-2}a'_{m+n-2} - 2c^{k+1}a'_{m+n-2}\sum_{i=m}^{m+n-2}\prod_{j=i}^{m+n-3} a_j, \end{aligned}$$

where the second equality is by Lemma 2.4.

For each $i = m,\dots,m+n-2$, the i-th term in the sum above has degree

$$\begin{aligned} &\deg\Big(c^{k+1}a'_{m+n-2}\prod_{j=i}^{m+n-3} a_j\Big) \\ &\qquad = k + 2^{m+n-3} + \sum_{j=i}^{m+n-3} 2^{j-1} = k + 2^{m+n-2} - 2^{i-1} \\ &\qquad \le (2^{m-2}-2) + 2^{m+n-2} - 2^{m-1} \\ &\qquad < 2^{m+n-2}-1 \\ &\qquad = \deg((a_{m+n-1}+a_{m-1})/c), \end{aligned}$$

and in addition, each such term has value 0 at $c = 0$. Therefore, $\overline{C}_1(0) = \overline{C}_2(0)$, where

$$C_2 = 2c^k a_{m+n-2}a'_{m+n-2} = c^k(a'_{m+n-1}-1) = c^k a'_{m+n-1} - c^k.$$

Note that $\deg c^k = k < \deg((a_{m+n-1}+a_{m-1})/c)$ and that c^k has value 0 at $c = 0$, because $k \ge 1$. Therefore, $\overline{C}_2(0) = \overline{A}_0(0)$, where $A_0 = c^k a'_{m+n-1}$ as above. Combining the above computations, we have $\overline{H}(0) = \overline{H}_0(0)$, where

$$H_0 = 2^{-n}A_0 - A_0 = \left(\frac{1}{2^n} - 1\right)c^k a'_{m+n-1}.$$

On the other hand, we may write $G = G_1 + G_2$ where

$$G_1 = c^k a'_{m-1} \quad \text{and} \quad G_2 = c^k a'_{m+n-1} = A_0.$$

We have

$$\begin{aligned}\deg G_1 &= k + 2^{m-2} - 1 < 2^{m-2} - 1 + 2^{m-2} - 1 = 2^{m-1} - 2 \\ &< \deg((a_{m+n-1} + a_{m-1})/c)\end{aligned}$$

and $G_1(0) = 0$. Therefore,

$$\left(\frac{1}{2^n} - 1\right)\overline{G}(0) = \left(\frac{1}{2^n} - 1\right)\overline{A}_0(0) = \overline{H}_0(0) = \overline{H}(0),$$

completing the proof of Lemma 2.7. ∎

LEMMA 2.8. *Let $n \geq 1$, and for each $i = 0, \ldots, n-1$, let $k_i \geq 0$. Define*

$$K = \lfloor k_0/2 \rfloor + \cdots + \lfloor k_{n-1}/2 \rfloor.$$

Let $\ell \geq 0$. Then there are integers $A_0, \ldots, A_{\ell+K}$ and $B_0, \ldots, B_{\ell+K}$ with the following property. For any $m \geq 2$ such that $\ell + K \leq 2^{m-2} - 2$, we have

$$T\Big(c^\ell \prod_{i=0}^{n-1} a_{m+i-1}^{k_i}, a_{m+n-1} + a_{m-1}\Big) = R + S,$$

where

$$R = \sum_{j=0}^{\ell+K} A_j T(c^j, a_{m+n-1} + a_{m-1}),$$

$$S = \sum_{j=0}^{\ell+K} B_j T\Big(c^j \prod_{i=m-1}^{m+n-2} a_i, a_{m+n-1} + a_{m-1}\Big).$$

Proof. Let $k = k_0 + \cdots + k_{n-1}$; note that $2K \leq k \leq 2K + n$. Order the set of pairs (K, k) of non-negative integers with $2K \leq k \leq 2K + n$ as follows: $(K', k') < (K, k)$ either if $K' < K$, or if $K' = K$ and $k' < k$. (Note that for any such pair (K, k), there are only finitely many smaller such pairs (K', k').) We proceed by induction on (K, k), subject to this ordering.

If $k_i = 0$ for every i, then choose $A_\ell = 1$ and all other A_j, B_j to be 0; the desired equality is immediate. Similarly, if $k_i = 1$ for every i, then choose $B_\ell = 1$ and all other A_j, B_j to be 0. On the other hand, if $k_i = 0$ for some i, and $k_i = 1$ for other i, then by Lemma 2.6, the desired quantity is 0; setting $A_j = B_j = 0$ for all j then, we are done. The foregoing cases cover all possibilities when $K = 0$. In addition, the values of A_j and B_j are independent of m, subject to the condition $\ell + K \leq 2^{m-2} - 2$.

Now consider $k_0, \ldots, k_{n-1}$ for which $K \geq 1$. Suppose that we already know the result for all pairs $(K', k') < (K, k)$. Since $K \geq 1$, there is some $0 \leq j \leq n-1$ such that $k_j \geq 2$; consider the largest such j. We have

$$a_{m+j-1}^{k_j} \equiv \begin{cases} a_{m+j-1}^{k_j-2}(a_{m+j} - c) & \text{if } j \leq n-2, \\ a_{m+j-1}^{k_j-2}(-a_{m-1} - c) & \text{if } j = n-1 \end{cases} \pmod{a_{m+n-1} + a_{m-1}}.$$

Thus, $c^\ell \prod_{i=0}^{n-1} a_{m+i-1}^{k_i} \equiv \pm f_1 - f_2 \pmod{a_{m+n-1} + a_{m-1}}$, with

$$f_1 = c^\ell \prod_{i=0}^{n-1} a_{m+i-1}^{k'_i} \quad \text{and} \quad f_2 = c^{\ell+1} \prod_{i=0}^{n-1} a_{m+i-1}^{k''_i},$$

where the $\pm$ sign is $+$ if $j \leq n-2$, or $-$ if $j = n-1$, and where

$$k'_i = \begin{cases} k_j - 2 & \text{if } i = j \text{ and } n \geq 2, \\ k_i + 1 & \text{if } i \equiv j+1 \pmod{n} \text{ and } n \geq 2, \\ k_i - 1 & \text{if } i = 0 \text{ and } n = 1, \\ k_i & \text{otherwise,} \end{cases} \qquad k''_i = \begin{cases} k_j - 2 & \text{if } i = j, \\ k_i & \text{otherwise.} \end{cases}$$

Define $K' = \lfloor k'_0/2 \rfloor + \cdots + \lfloor k'_{n-1}/2 \rfloor$ and $K'' = \lfloor k''_0/2 \rfloor + \cdots + \lfloor k''_{n-1}/2 \rfloor$. Similarly define $k' = k'_0 + \cdots + k'_{n-1}$ and $k'' = k''_0 + \cdots + k''_{n-1}$. We have $K' \leq K$, and $k' = k - 1 < k$, and $K'' = K - 1 < K$. Therefore, $(K', k') < (K, k)$ and $(K'', k'') < (K, k)$. If we also define $\ell' = \ell$ and $\ell'' = \ell + 1$, then $\ell' + K' \leq 2^{m-2} - 2$ and $\ell'' + K'' \leq 2^{m-2} - 2$. Hence, by our inductive assumption, the desired statement holds for both f_1 and f_2. In addition, the resulting integer coefficients A_j and B_j, as linear combinations of the coefficients for f_1 and f_2, are independent of m, as desired. ∎

Proof of Theorem 2.1. Recall from Newton's identities for symmetric polynomials that, in characteristic zero, the coefficients c_i of a monic polynomial $f(x) = x^N + c_{N-1}x^{N-1} + \cdots + c_0$ can be written in terms of the power sums $p_j = \sum_{i=1}^N \alpha_i^j$ of the roots $\alpha_1, \ldots, \alpha_N$. Moreover, these identities are independent of the degree N, with c_{N-j} depending only on $p_1, \ldots, p_j$; for example, $c_{N-1} = -p_1$, and $c_{N-2} = \frac{1}{2}(p_1^2 - p_2)$. Thus, to show that the two polynomials $(P_{m,n})^2$ and $P_{m+1,n}$ have matching coefficients $b_{k-i} = c_{\ell-i}$ for all $i \geq 0$ up to some bound B, it suffices to show that the power sums of roots of the two polynomials coincide up to the same power B.

Recall from (1.2) that the roots of $P_{m,n}$ are $-2^n \prod_{j=m-1}^{m+n-2} a_j(\alpha)$ for each root α of $G_{m,n}$; similarly for $P_{m+1,n}$. Since $(P_{m,n})^2$ has each root of $P_{m,n}$ appearing twice, we see that after cancelling $(-2^n)^i$ when equating the relevant power sums, it suffices to show the equality

$$2T\Big(\prod_{j=m-1}^{m+n-2} a_j^i, G_{m,n}\Big) = T\Big(\prod_{j=m}^{m+n-1} a_j^i, G_{m+1,n}\Big) \tag{2.6}$$

for any $i \geq 1$ such that $\lfloor ni/2 \rfloor \leq 2^{m-2} - 2$. For the remainder of the proof, fix such an i.

By Lemma 1.7(b) and the definition of $G_{m,n}$, for $n \nmid m-1$, we have

$$T\Big(\prod_{j=m-1}^{m+n-2} a_j^i, G_{m,n}\Big) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) T\Big(\prod_{j=m-1}^{m+n-2} a_j^i, a_{m+d-1} + a_{m-1}\Big).$$

In fact, by the same reasoning as in the proof of Lemma 1.9, the same equality also holds if $n \,|\, m-1$. Observe that for each $i \geq 0$ and $t \geq 1$, we have

$$a_{m+dt-1} \equiv -a_{m-1} \quad \text{and} \quad a_{m+i+dt} \equiv a_{m+i} \pmod{a_{m+d-1} + a_{m-1}},$$

and hence by Lemma 1.7(a), we have

$$(2.7) \qquad T\Big(\prod_{j=m-1}^{m+n-2} a_j^i, G_{m,n}\Big)$$
$$= \sum_{d|n} \mu\Big(\frac{n}{d}\Big) (-1)^{i((n/d)-1)} T\Big(\prod_{j=m-1}^{m+d-2} a_j^{ni/d}, a_{m+d-1} + a_{m-1}\Big)$$
$$= \sum_{d|n} \mu\Big(\frac{n}{d}\Big) (-1)^{i((n/d)-1)} (R_d + S_d),$$

where R_d and S_d are the quantities R and S from Lemma 2.8 for which

$$T\Big(\prod_{j=m-1}^{m+d-2} a_j^{ni/d}, a_{m+d-1} + a_{m-1}\Big) = R_d + S_d.$$

(That is, in the notation of Lemma 2.8, use d in place of n, set $k_0 = \cdots = k_{d-1} = ni/d$, and use $\ell = 0$. That lemma does indeed apply, because $d\lfloor ni/2d \rfloor \leq \lfloor ni/2 \rfloor \leq 2^{m-2} - 2$.)

Let $K_d = d\lfloor \frac{ni}{2d} \rfloor \leq 2^{m-2} - 2$, and let $A_{d,j}, B_{d,j} \in \mathbb{Z}$ be the integers in the sums defining R_d and S_d. Then S_d is

$$\sum_{j=0}^{K_d} B_{d,j} T\Big(c^j \prod_{s=m-1}^{m+d-2} a_s, a_{m+d-1} + a_{m-1}\Big)$$
$$= \sum_{j=0}^{K_d} B_{d,j} \Big(\frac{1}{2^d} - 1\Big) T(c^j, a_{m+d-1} + a_{m-1}),$$

by using Remark 1.12 for $j = 0$ (recalling that $m \geq 3$), and by using Lemma 2.7 for $j \geq 1$. Hence, setting $C_{d,j} = A_{d,j} + \big(\frac{1}{2^d} - 1\big) B_{d,j}$, equation (2.7) and the formulas defining R_d and S_d from Lemma 2.8 yield

$$T\Big(\prod_{j=m-1}^{m+n-2} a_j^i, G_{m,n}\Big) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)(-1)^{i((n/d)-1)} \sum_{j=0}^{K_d} C_{d,j} T(c^j, a_{m+d-1}+a_{m-1}).$$

Applying Lemmas 2.7 and 2.8 to $T(\prod_{j=m}^{m+n-1} a_j^i, G_{m+1,n})$ in the same fashion, we obtain

$$T\Big(\prod_{j=m}^{m+n-1} a_j^i, G_{m+1,n}\Big) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big)(-1)^{i((n/d)-1)} \sum_{j=0}^{K_d} C_{d,j} T(c^j, a_{m+d} + a_m),$$

using the same coefficients $C_{d,j}$, since the integer coefficients $A_{d,j}$ and $B_{d,j}$ in the sums defining R_d and S_d in Lemma 2.8 are independent of m.

Thus, to prove (2.6), it suffices to prove the equalities

$$2T(c^j, a_{m+d-1} + a_{m-1}) = T(c^j, a_{m+d} + a_m) \quad \text{for each } j = 0, 1, \ldots, K_d.$$

Equivalently, we must prove

(2.8)
$$T(c^j, (a_{m+d-1} + a_{m-1})^2) = T(c^j, a_{m+d} + a_m) \quad \text{for each } j = 0, 1, \ldots, K_d.$$

However, for every $d \geq 1$, observe that the coefficients of the 2^{m-2} highest-power terms of the degree-2^{m+d-1} polynomials $(a_{m+d-1}+a_{m-1})^2 \in \mathbb{Z}[c]$ and $a_{m+d} + a_m \in \mathbb{Z}[c]$ coincide. Indeed, since $a_s = a_{s-1}^2 + c$, their difference is

$$(a_{m+d-1}^2+2a_{m+d-1}a_{m-1}+a_{m-1}^2)-(a_{m+d-1}^2+a_{m-1}^2+2c) = 2a_{m+d-1}a_{m-1}-2c,$$

which has degree $2^{m+d-2} + 2^{m-2}$, too small to affect those highest-power terms. Therefore, because $K_d \leq 2^{m-2} - 2$, Newton's identities for symmetric polynomials immediately imply (2.8), and hence (2.6) follows. ∎

3. Proving that multiplier polynomials are 2-special. Theorem 2.1 makes possible the following result, which will be an essential tool in the proof of Theorem 0.3.

THEOREM 3.1. *Let $m \geq 2$, and $n \geq 1$. Suppose that*

$$v_2(\mathrm{tr}(P_{m+1,n})) \leq m + 1 + 3n/2.$$

If $P_{m,n}$ is 2-special, then $P_{m+1,n}$ is also 2-special.

Proof. Write $(P_{m,n}(x))^2 = x^k + \sum_{j=0}^{k-1} b_j x^j$, $P_{m+1,n}(x) = x^\ell + \sum_{j=0}^{\ell-1} c_j x^j$. By Proposition 1.5, we have $v_2(c_{\ell-j}) > nj$ for all $j \geq 1$. In particular, $v_2(c_{\ell-1}) > 1$, satisfying the first condition for $P_{m+1,n}$ to be 2-special.

By [3, Lemma 6.3] and the hypothesis that $P_{m,n}$ is 2-special, we deduce that $P_{m,n}^2$ is 2-special as well. In addition, for any index $j \geq 1$ such that $nj < 2^{m-1} - 2$, we have $\lfloor nj/2 \rfloor \leq 2^{m-2} - 2$, and hence $b_{k-j} = c_{\ell-j}$, by

Theorem 2.1. Therefore, if $2 \le j < (2^{m-1} - 2)/n$, then

$$v_2(c_{\ell-j}) = v_2(b_{k-j}) > v_2(b_{k-1}) = v_2(c_{\ell-1}).$$

It remains to prove $v_2(c_{\ell-j}) > v_2(c_{\ell-1})$ for $j \ge \max\{2, (2^{m-1} - 2)/n\}$. By hypothesis, we have $v_2(c_{\ell-1}) \le m + 1 + 3n/2$; and as noted above, we also have $v_2(c_{\ell-j}) > nj$. Thus, the desired result follows immediately if m and n satisfy

$$m + 1 + 3n/2 \le \max\{2n, 2^{m-1} - 2\}. \tag{3.1}$$

Inequality (3.1) holds if and only if

$$m + 1 \le n/2 \quad \text{or} \quad 3n/2 \le 2^{m-1} - m - 3,$$

and hence it fails if and only if

$$\tfrac{2}{3}(2^{m-1} - m - 3) < n < 2m + 2. \tag{3.2}$$

Observe that

$$\tfrac{2}{3}(2^{m-1} - m - 3) - (2m + 2) = \tfrac{2}{3}(2^{m-1} - 4m - 6),$$

which is positive for $m \ge 6$. Thus, (3.1) holds for all pairs (m, n) with $m \ge 6$. Hence, the only pairs (m, n) for which (3.1) fails are those for which $m = 2, 3, 4, 5$ and (3.2) holds. That is, it remains to consider $P_{m+1,n}$ for the finitely many cases

$$m = 2 \text{ and } 1 \le n \le 5, \quad m = 3 \text{ and } 1 \le n \le 7,$$
$$m = 4 \text{ and } 1 \le n \le 9, \quad m = 5 \text{ and } 6 \le n \le 11.$$

Direct computation with Magma shows that $P_{m+1,n}$ is 2-special in all 27 of these cases. (Incidentally, [3, Theorem 7.2] also says that $P_{m,1}$ and $P_{m,2}$ are 2-special for all $m \ge 2$, covering the six cases above with $n = 1, 2$.) ∎

Proof of Theorem 0.3. The statement holds for $p = 2$ by [3, Theorem 7.2], so we can assume $3 \le p \le 1021$. By Proposition 1.2 and Theorem 1.4, it suffices to show that $P_{m,p}$ is 2-special for any $m \ge 2$. According to Corollary 2.2, we have

$$v_2(\mathrm{tr}(P_{m+1,p})) = v_2(\mathrm{tr}(P_{m,p})) + 1 \tag{3.3}$$

for any $m \ge 11$. Let α be a root of $G_{m,1} = (a_m + a_{m-1})/c$, which is irreducible over $\mathbb{Q}$ by [7, Corollary 1.1]. Setting $K = \mathbb{Q}(\alpha)$, Theorem 1.10 gives us

$$\mathrm{tr}(P_{m,p}) = 2^p\big(\mathrm{Tr}_{K/\mathbb{Q}}(a_{m-1}(\alpha)^p) + 2^{m+p-2} - 2^{m-2}\big). \tag{3.4}$$

Magma computations of $\mathrm{Tr}_{K/\mathbb{Q}}(a_{m-1}(\alpha)^p)$, together with (3.4), show that

$$v_2(\mathrm{tr}(P_{m,p})) < m + 3p/2 \tag{3.5}$$

for all primes $3 \le p \le 1021$ and all integers $2 \le m \le 10$. (See Section 4 for some of these trace valuations.) Therefore, applying equation (3.3) inductively, we find that the bound (3.5) holds for all primes $3 \le p \le 1021$ and *all* integers $m \geq 2$. By applying Theorem 3.1 inductively, it then suffices to show that $P_{2,p}$ is 2-special for every prime $3 \leq p \leq 1021$.

By Remark 1.11, we have

$$\mathrm{tr}(P_{2,p}) = 2^{2p} - 2^{p+1},$$

and hence $v_2(\mathrm{tr}(P_{2,p})) = p + 1$. On the other hand, by Proposition 1.5, writing $P_{2,p}(x) = x^k + \sum_{i=0}^{k-1} b_i x^i$, we have

$$v_2(b_{k-j}) > pj \geq 2p > p + 1 = v_2(\mathrm{tr}(P_{2,p})) \quad \text{for all } 2 \leq j \leq k,$$

showing that $P_{2,p}$ is 2-special. ∎

Table 1. Trace valuations of multiplier polynomials $P_{m,p}$ relative to $m + p$

(m,p)	$v_2(\mathrm{tr}(P_{m,p}))$	$m+p$	(m,p)	$v_2(\mathrm{tr}(P_{m,p}))$	$m+p$
$(10, 509)$	512	519	$(10, 503)$	511	513
$(10, 499)$	509	509	$(10, 491)$	496	501
$(10, 487)$	500	**497**	$(10, 479)$	486	489
$(10, 467)$	473	477	$(10, 463)$	470	473
$(10, 461)$	470	471	$(10, 457)$	465	467
$(9, 251)$	256	260	$(9, 241)$	249	250
$(9, 239)$	245	248	$(9, 233)$	240	242
$(9, 229)$	237	238	$(9, 227)$	236	236
$(9, 223)$	230	232	$(9, 211)$	219	220
$(9, 199)$	206	208	$(9, 197)$	202	206
$(8, 113)$	120	121	$(8, 109)$	112	117
$(8, 107)$	112	115	$(8, 103)$	109	111
$(8, 101)$	105	109	$(8, 97)$	102	105
$(8, 89)$	96	97	$(8, 83)$	91	91
$(8, 79)$	86	87	$(8, 73)$	78	81
$(7, 61)$	64	68	$(7, 59)$	65	66
$(7, 53)$	56	60	$(7, 47)$	54	54
$(7, 43)$	50	50	$(7, 41)$	45	48
$(7, 37)$	43	44	$(7, 31)$	32	38
$(7, 29)$	33	36	$(7, 23)$	31	**30**
$(6, 29)$	32	35	$(6, 23)$	30	**29**
$(6, 19)$	24	25	$(6, 17)$	21	23
$(6, 13)$	19	19	$(6, 11)$	16	17
$(6, 7)$	9	13	$(6, 5)$	9	11
$(6, 3)$	6	9	$(6, 2)$	6	8
$(5, 13)$	18	18	$(5, 11)$	15	16
$(5, 7)$	8	12	$(5, 5)$	8	10
$(5, 3)$	5	8	$(5, 2)$	5	7
$(4, 5)$	7	9	$(4, 3)$	4	7
$(4, 2)$	4	6	$(3, 2)$	3	5

4. Appendix: Some trace data for multiplier polynomials. In the proof of Theorem 0.3 in Section 3, we had to rely on Magma computations of $v_2(\mathrm{tr}(P_{m,p}))$, the 2-adic valuation of the second-from-top coefficient of the multiplier polynomial $P_{m,p}$. The full set of those valuations, for all primes $3 \leq p \leq 1021$ and all integers $2 \leq m \leq 10$, would take up too much space here, but we include some of them in Table 1. We also include the values of $m+p$, since we found that $v_2(\mathrm{tr}(P_{m,p})) \leq m+p$ in almost all instances, thus certainly satisfying inequality (3.5). (But not always! As Table 1 shows, this sharper bound fails when (m,p) is $(6,23)$, $(7,23)$ or $(10,487)$, for example. We have marked all such instances in the table in boldface.)

Acknowledgements. The authors thank Joe Silverman for his helpful suggestions. The authors also thank the anonymous referee for their careful reading of the original manuscript of the paper, and for their detailed suggestions, which greatly improved the exposition.

Funding. The first author gratefully acknowledges the support of NSF grant DMS-2401172.

References

[1] M. Baker and L. DeMarco, *Special curves and postcritically finite polynomials*, Forum Math. Pi 1 (2013), art. e3, 35 pp.

[2] R. L. Benedetto and V. Goksel, *Misiurewicz polynomials and dynamical units, part I*, Int. J. Number Theory 19 (2023), 1249–1267.

[3] R. L. Benedetto and V. Goksel, *Misiurewicz polynomials and dynamical units, part II*, Res. Number Theory 10 (2024), no. 3, art. 58, 24 pp.

[4] X. Buff, *On postcritically finite unicritical polynomials*, New York J. Math. 24 (2018), 1111–1122.

[5] X. Buff, A. L. Epstein, and S. Koch, *Prefixed curves in moduli space*, Amer. J. Math. 144 (2022), 1485–1509.

[6] D. Ghioca, H. Krieger, K. D. Nguyen, and H. Ye, *The dynamical André–Oort Conjecture: unicritical polynomials*, Duke Math. J. 166 (2017), 1–25.

[7] V. Goksel, *On the orbit of a post-critically finite polynomial of the form x^d+c*, Funct. Approx. Comment. Math. 62 (2020), 95–104.

[8] V. Goksel, *A note on Misiurewicz polynomials*, J. Théor. Nombres Bordeaux 32 (2020), 373–385.

[9] B. H. Gross and D. B. Zagier, *On singular moduli*, J. Reine Angew. Math. 355 (1985), 191–220.

[10] B. Hutz and A. Towsley, *Misiurewicz points for polynomial maps and transversality*, New York J. Math. 21 (2015), 297–319.

[11] Y Li, *Singular units and isogenies between CM elliptic curves*, Compos. Math. 157 (2021), 1022–1035.

[12] J. Milnor, *Arithmetic of unicritical polynomial maps*, in: Frontiers in Complex Dynamics: In Celebration of John Milnor's 80th Birthday, Princeton Univ. Press, Princeton, NJ, 2014, 15–24.

[13] N. Patra, *Irreducibility of eventually 2-periodic curves in the moduli space of cubic polynomials*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (5), to appear.
[14] J. H. Silverman, *The Arithmetic of Dynamical Systems*, Springer, New York, 2007.

Robert L. Benedetto
Amherst College
Amherst, MA 01002, USA
E-mail: rlbenedetto@amherst.edu

Vefa Goksel
Towson University
Towson, MD 21252, USA
E-mail: vgoksel@towson.edu