$A^2_{\gcd(m,n)}$ ALWAYS DIVIDES $F_{m,n}$: MULTIPLE ROOTS OF THE BREMNER–ULAS QUADRINOMIAL DISCRIMINANTS

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. Bremner and Ulas reduce the divisibility of the quadrinomial $x^n + x^{n-m} + x^{n-2m} + a$ by a rational quadratic to the rational points of the hyperelliptic curve $s^2 = F_{m,n}(t)$, where $F_{m,n} = A^2_{n-m} - 4A_{n-2m}A_n$ is built from the sequence $A_k = A_k(1,t) \in \mathbb{Z}[t]$ of their Lemma 3.1, and they conjecture that $F_{m,n}$ has no multiple roots whenever $n > 2m$. We show that this is false and identify the obstruction exactly: $A^2_{\gcd(m,n)}$ divides $F_{m,n}$ for *all* m, n, over every commutative ring. Since A_d is a non-unit precisely for $d \geq 3$, the polynomial $F_{m,n}$ fails to be squarefree, and has a multiple complex root, for every pair with $n > 2m$ and $\gcd(m,n) \geq 3$; the smallest is $(m,n) = (3,9)$, where $F_{3,9} = (t-1)^2(4t^3 - 27t^2 + 18t - 3)$ although $9 > 2 \cdot 3$. We propose the repaired statement $\gcd(F_{m,n}, F'_{m,n}) = A_{\gcd(m,n)}$ up to a nonzero constant — equivalently, $F_{m,n}$ is squarefree if and only if $\gcd(m,n) \leq 2$ — and verify it for all 210 pairs with $3 \leq n \leq 30$, $0 < m$, $2m < n$ by an explicit Bézout certificate per pair, in which both exact divisions are checked rather than assumed and no polynomial gcd algorithm is trusted; an independent computation confirms it for all 1560 pairs with $n \leq 80$. Every theorem below is machine-checked in Lean 4; §8 says exactly what the machine checks and names the two steps that remain outside it. One caveat is stated in full in §1.1: the published version of the source is closed access, and the refutation is graded against its arXiv e-print.

1. INTRODUCTION

Let $f_{n,m,k}(a,x) = x^n + x^m + x^k + a$ with $n > m > k \geq 1$ and $a \in \mathbb{Q} \setminus \{0\}$. Reducibility of such quadrinomials is a classical subject, treated in general by Fried and Schinzel [3] (later corrected in [4]); [1] refers to [3] for background. The concrete question of which rational a, for a given triple of exponents, make $f_{n,m,k}(a,x)$ divisible by a quadratic is the subject of [1]: it is treated there in detail for $\deg f \leq 6$, and for $\deg f \geq 7$ it is reduced to a Diophantine problem on a curve.

Their Lemma 3.1 is the elementary observation that

$$x^n \bmod (x^2 + px + q) = A_n(p,q)\,x + B_n(p,q),$$

where $A_0 = 0$, $A_1 = 1$, $B_0 = 1$, $B_1 = 0$ and both sequences satisfy the same recurrence $A_n = -pA_{n-1} - qA_{n-2}$. Their Corollary 3.2 then says that if $f_{n,m,k}(a,x)$ is divisible by $x^2 + px + q$ with $a \neq 0$, then $A_n(p,q) + A_m(p,q) + A_k(p,q) = 0$ and $a = -B_n(p,q) - B_m(p,q) - B_k(p,q)$; [1] reads the first of these as a plane curve whose rational points carry the whole question. In §5 of [1] the exponents are taken in arithmetic progression, $f(a,x) = x^n + x^{n-m} + x^{n-2m} + a$; since $A_n(p,tp^2) = p^{n-1}A_n(1,t)$, writing $q = tp^2$ and $X = p^m$ turns that condition, for $p \neq 0$ and after removing the factor p^{n-2m-1}, into

$$A_n(1,t)X^2 + A_{n-m}(1,t)X + A_{n-2m}(1,t) = 0,$$

so that a rational solution forces the discriminant to be a square. This is their Theorem* of §5, and it produces the hyperelliptic curve

$$H_{n,n-m,n-2m}:\ s^2 = F_{m,n}(t), \qquad F_{m,n}(t) = A_{n-m}(1,t)^2 - 4A_{n-2m}(1,t)A_n(1,t),$$

with $s = \pm(2A_n(1,t)p^m + A_{n-m}(1,t))$. For $m = 1$ the curve has genus 2 exactly when $n = 7, 8$, according to [1], which prints those two curves explicitly,

$$H_{7,6,5}:\ s^2 = 4t^5 - 27t^4 + 72t^3 - 66t^2 + 24t - 3, \qquad H_{8,7,6}:\ s^2 = t^6 + 36t^5 - 138t^4 + 186t^3 - 111t^2 + 30t - 3,$$

resolving the first by a Chabauty computation and leaving the second unresolved. Section 5 then closes with a conjecture, which we quote verbatim from the e-print, together with the sentence that introduces it:

> Although we have not proved the following, it seems plausible:
>
> **Conjecture 5.2.** Let $m, n \in \mathbb{N}_+$ with $n > 2m$ and define the polynomial $F_{m,n}(t) = A_{n-m}(1,t)^2 - 4A_{n-2m}(1,t)A_n(1,t)$. Then $F_{m,n}$ has no multiple roots.

No verification range is attached to it anywhere in the paper. (The e-print's LaTeX source carries, commented out at the end of its last section, an earlier form of the same conjecture, identical except that its hypothesis reads $n > m$; neither form mentions $\gcd(m,n)$.) The conjecture is not decorative: a multiple root of $F_{m,n}$ is a singular point of $H_{n,n-m,n-2m}$, and the genus computation and the Chabauty and descent arguments that [1] runs at $n = 7, 8$ all presuppose a smooth model. Any attempt to push §5 past $n = 8$ meets the conjecture immediately.

Results. The conjecture is false, and it fails for a reason that is visible without computation. Write $d = \gcd(m,n)$ and abbreviate $A_k := A_k(1,t) \in \mathbb{Z}[t]$. Then d divides each of $n-m$, $n-2m$ and n; the sequence $(A_k)_{k\geq 0}$ is a Lucas sequence, so it has the divisibility property $d \mid k \Rightarrow A_d \mid A_k$ of [5]; and therefore every term of $F_{m,n} = A_{n-m}^2 - 4A_{n-2m}A_n$ is divisible by A_d^2. We prove:

(1) $A_{\gcd(m,n)}^2$ divides $F_{m,n}$, for all m, n, over every commutative ring (Theorem 3.1).
(2) A_d is a non-unit exactly for $d \geq 3$, so for every pair with $0 < m$, $n > 2m$ and $\gcd(m,n) \geq 3$ the polynomial $F_{m,n}$ is not squarefree in $\mathbb{Z}[t]$ (Theorem 4.3) and has a multiple root in $\mathbb{C}$ (Theorem 4.4), which is the conjecture's literal wording. The refuting pairs form an infinite family, of which $F_{3,3k}$, $k \geq 3$, is the simplest subfamily.
(3) The smallest pair in the conjecture's range with $\gcd(m,n) \geq 3$ is $(m,n) = (3,9)$, where $9 > 2\cdot 3$ and
$$F_{3,9}(t) = 4t^5 - 35t^4 + 76t^3 - 66t^2 + 24t - 3 = (t-1)^2(4t^3 - 27t^2 + 18t - 3),$$
a double root at $t = 1$ (Theorem 4.1). The multiplicity there is exactly two (Proposition 4.5).
(4) Nothing else appears to go wrong. We conjecture that A_d^2 is the whole obstruction, in the sharp form $\gcd(F_{m,n}, F'_{m,n}) = A_{\gcd(m,n)}$ up to a nonzero constant — equivalently, $F_{m,n}$ is squarefree if and only if $\gcd(m,n) \leq 2$ — and verify this for all 210 pairs with $3 \leq n \leq 30$, $0 < m$, $2m < n$ (Theorem 5.1), with an independent confirmation for all 1560 pairs with $n \leq 80$.

So the correct dividing line is a gcd condition that the conjecture's statement does not mention, and the exceptional set is not sparse: on the window of Theorem 5.1 the conjecture fails at 37 of the 210 pairs, and since the pairs with $\gcd(m,n) = d$ have relative density $6/(\pi^2 d^2)$ in the cone $n > 2m > 0$, the asymptotic proportion of failing pairs is $1 - 15/(2\pi^2) \approx 24\%$. (That last count is an elementary observation, outside the formal development.) We also reproduce, from the recurrence alone, the two curves $H_{7,6,5}$ and $H_{8,7,6}$ that [1] prints (Theorem 6.1); this was done before any of the above was claimed, as a check that our transcription of §5 agrees with the source.

1.1. **Which text is refuted.** This must be said plainly. The e-print [1] has exactly one version, v1 of 20 October 2013; no later version was posted, and it carries no journal-reference field. The quotation above is from that e-print, fetched and read directly, and the conjecture is Conjecture 5.2 there (§5 is the fifth section, and the Theorem* preceding the conjecture is 5.1, all theorem-like environments sharing one counter numbered by section). *The body of the published version was not read*: the article is closed access, the publisher's page serving the title, the abstract, the reference list and the dates and then "a preview of subscription content"; no open-access location is recorded, no repository copy is attached, and no reviewing service quotes §5 — the zbMATH review summarises only the degree-≤ 6 classification.

Three facts indicate that the published text tracks the e-print. The publisher's abstract is word-identical to the arXiv abstract. The publisher's reference list is item-for-item the e-print's: the same nine works in the same order, nothing added and nothing removed. And the only work that OpenAlex

records as citing the published version, [2], restates the source's Lemma 3.1 with exactly the content of the e-print's Lemma 3.1 and derives its own Lemma 2.2 from "Corollary 3.2" of [1], so the numbering of §3 did not shift between preprint and journal. None of the three is evidence about §5 itself, and two details cut the other way: the publisher records the manuscript as received 9 September 2013 and revised and accepted 24 October 2013, four days *after* the e-print was posted, so the accepted text is contemporaneous with the e-print but not thereby identical to it; and the e-print's comments field names a journal other than the one in which the paper appeared.

If the published version carries a hypothesis $\gcd(m,n)=1$ that the e-print does not, then none of the mathematics below changes and only its relation to [1] does: our results then say that such a hypothesis is *necessary*, and that the exact threshold is $\gcd(m,n)\geq 3$ and not $\gcd(m,n)\geq 2$. In either reading, Theorems 3.1–5.1 stand as stated.

What is not proved. Theorem 5.1 is a verification on a finite window, not a proof: we do not prove the repaired law in general. Two independent statements remain open, and Remark 3.2 describes a route to the first. Nor do we say anything about the Diophantine problem [1] actually poses — the rational points of $H_{n,n-m,n-2m}$ — beyond the observation that for $\gcd(m,n)\geq 3$ the curve as written is singular, so that those questions must be asked of a desingularisation, or of the quotient $F_{m,n}/A^2_{\gcd(m,n)}$.

2. The sequence A_k and the polynomials $F_{m,n}$

Throughout, R is a commutative ring and $t\in R$.

Definition 2.1. $A\colon \mathbb{N}\to R$ is defined by $A_0=0$, $A_1=1$ and $A_{k+2}=-A_{k+1}-tA_k$.

This is $A_k(1,t)$ in the notation of [1, Lemma 3.1], specialised at $p=1$, $q=t$. Taking $R=\mathbb{Z}[t]$ with t the indeterminate gives the polynomials

$$A_1=1,\quad A_2=-1,\quad A_3=1-t,\quad A_4=2t-1,\quad A_5=t^2-3t+1,\quad A_6=-3t^2+4t-1,$$
$$A_7=-t^3+6t^2-5t+1,\quad A_8=4t^3-10t^2+6t-1,\quad A_9=t^4-10t^3+15t^2-7t+1.$$

Equivalently $A_k=(\alpha^k-\beta^k)/(\alpha-\beta)$ for the roots α,β of x^2+x+t, which is the closed form used in [1, §5]; that is, (A_k) is the Lucas sequence $U_k(-1,t)$.

Definition 2.2. For $m,n\in\mathbb{N}$, $F_{m,n}:=A^2_{n-m}-4A_{n-2m}A_n\in R$, where $n-m$ and $n-2m$ denote truncated subtraction in $\mathbb{N}$.

The truncation is a convenience that makes $F_{m,n}$ total; in the range $n>2m$ of Conjecture 5.2, which is the only range we draw conclusions about, both differences are the ordinary ones.

Remark 2.3. A short induction on the recurrence, outside the formal development and not needed for any theorem below, gives $\deg A_k=\lfloor (k-1)/2\rfloor$ with leading coefficient $(-1)^j$ for $k=2j+1$ and $(-1)^j j$ for $k=2j$. In particular $A_1=1$ and $A_2=-1$ are the only constants among the A_k with $k\geq 1$, and $\deg A_d\geq 1$ for $d\geq 3$. We do not use this: Lemma 4.2 obtains what we need from two evaluations instead, which is both shorter and easier to check.

Remark 2.4. Three slips in [1, §5] are worth recording, since we quote that section. Its Theorem* is displayed with the hypothesis $n>2m\geq 3$, yet the cases it then works out are $m=1$, $n=7,8$; inside its proof the display of $A_n(p,q)+A_{n-m}(p,q)+A_{n-2m}(p,q)$ carries $A_{n-1}(1,t)$ and $A_{n-2}(1,t)$ where $A_{n-m}(1,t)$ and $A_{n-2m}(1,t)$ are meant; and the formula for s accompanying $H_{n,n-m,n-2m}$ is written as it reads at $m=1$, with p in place of p^m. None of the three affects the conjecture, which is stated with the single hypothesis $n>2m$.

The two facts about (A_k) that we need are classical for Lucas sequences; we state them in the form in which they are proved, over an arbitrary commutative ring, since that is what makes Theorem 3.1 independent of any choice of coefficient domain.

Lemma 2.5 (addition formula)**.** *For all $a,b\in\mathbb{N}$, $A_{a+1+b}=A_{a+1}A_{b+1}-t\,A_aA_b$.*

Proof. Induction on b, carried out for the pair of statements at b and $b+1$ simultaneously so that only the one-step recurrence of Definition 2.1 is needed. For $b = 0$ the first component is the identity $A_{a+1} = A_{a+1}A_1 - tA_aA_0$ and the second is $A_{a+2} = -A_{a+1} - tA_a = A_{a+1}A_2 - tA_aA_1$. The step rewrites $A_{a+1+(b+2)} = -A_{a+1+(b+1)} - t\,A_{a+1+b}$ by the recurrence and substitutes both halves of the inductive hypothesis. □

Lemma 2.6 (Lucas divisibility)**.** *If $d \mid k$ then $A_d \mid A_k$.*

Proof. It suffices to treat $k = dj$ and induct on j, the case $d = 0$ being trivial. Write $d = e + 1$. Then $A_{d(j+1)} = A_{e+1+dj} = A_{e+1}A_{dj+1} - t\,A_eA_{dj}$ by Lemma 2.5; the first term is divisible by $A_d = A_{e+1}$ and the second by A_{dj}, hence by A_d by the inductive hypothesis. □

3. The structural theorem

Theorem 3.1. *Let R be a commutative ring, $t \in R$ and $m, n \in \mathbb{N}$. Then*

$$A_{\gcd(m,n)}^2 \;\Big|\; F_{m,n}$$

in R. In particular $A_{\gcd(m,n)}(1,t)^2$ divides $F_{m,n}(t)$ in $\mathbb{Z}[t]$, and hence in $\mathbb{Q}[t]$ and $\mathbb{C}[t]$.

Proof. Put $d = \gcd(m, n)$. Then $d \mid m$ and $d \mid n$, so d divides each of $n - m$, $n - 2m$ and n (in $\mathbb{N}$, truncated subtraction included). By Lemma 2.6, A_d divides each of A_{n-m}, A_{n-2m} and A_n. Hence A_d^2 divides A_{n-m}^2 and also divides $4A_{n-2m}A_n$, and therefore divides their difference $F_{m,n}$. □

Two features of this statement deserve emphasis. It has *no hypothesis*: neither $n > 2m$ nor any coprimality, and no restriction on the ring. And its proof uses nothing about $F_{m,n}$ beyond the shape of its three indices $n - m$, $n - 2m$, n, all of which are congruent to 0 modulo $\gcd(m, n)$ — which is precisely the structure that the arithmetic progression of exponents in $x^n + x^{n-m} + x^{n-2m} + a$ puts there.

Remark 3.2. There is a second route to Theorem 3.1 that also says something about the multiplicity. Catalan's identity for the Lucas sequence (A_k), $A_r^2 - A_{r+s}A_{r-s} = t^{\,r-s}A_s^2$, taken at $r = n-m$, $s = m$, rewrites the discriminant as

$$F_{m,n} = 4t^{\,n-2m}A_m^2 - 3A_{n-m}^2,$$

from which $A_d^2 \mid F_{m,n}$ follows again, and which reduces the assertion "the multiplicity at a root θ of A_d is exactly two" to $4\theta^{\,n-2m}A_m(\theta)^2 \neq 3A_{n-m}(\theta)^2$. This identity is not part of the formal development; we verified it outside it, for all 870 pairs with $n \leq 60$, and record it as the route we would take to Conjecture A rather than as a result.

4. The counterexamples

The pairs in the range of Conjecture 5.2 with $\gcd(m, n) \geq 3$ are exactly the pairs where Theorem 3.1 bites, and the smallest of them is $(m, n) = (3, 9)$. Indeed $\gcd(m, n) \geq 3$ forces $m \geq 3$ and then $n > 2m$ forces $n \geq 7$; for $n = 7$ the only divisor $d \geq 3$ of n is 7, which would need $m \geq 7$, and for $n = 8$ the divisors $d \geq 3$ are 4 and 8, which would need $m \geq 4$ and hence $n \geq 9$; so $n \geq 9$, and at $n = 9$ only $m = 3$ satisfies both $3 \mid m$ and $2m < 9$.

Theorem 4.1. *Over every commutative ring,*

$$F_{3,9} = A_6^2 - 4A_3A_9 = 4t^5 - 35t^4 + 76t^3 - 66t^2 + 24t - 3 = (t-1)^2\,(4t^3 - 27t^2 + 18t - 3).$$

In particular, as an element of $\mathbb{Q}[t]$ it satisfies $F_{3,9}(1) = 0$ and $F'_{3,9}(1) = 0$, so it has a multiple root — although $(m, n) = (3, 9)$ satisfies the hypothesis $n > 2m$ of Conjecture 5.2, since $9 > 2 \cdot 3$.

Proof. Expand A_3, A_6 and A_9 from Definition 2.1 — six applications of the recurrence — and compare coefficients; the factorisation is then a polynomial identity in $\mathbb{Z}[t]$, valid in R for every t by specialisation. The double root is read off the factored form. □

Lemma 4.2. *For $d \geq 3$, A_d is not a unit of $\mathbb{Z}[t]$, and A_d is not a constant polynomial over any field of characteristic zero.*

Proof. Two specialisations of the recurrence suffice. At $t = 0$ it degenerates to $A_{k+1} = -A_k$, so $A_{k+1}(1, 0) = (-1)^k$. At $t = -2$ the quadratic $x^2 + x - 2$ splits with roots $1, -2$, and the closed form gives, by a one-step induction,

$$3\,A_k(1, -2) = 1 - (-2)^k \qquad (k \geq 0).$$

Now the units of $\mathbb{Z}[t]$ are the constants ± 1; if $A_d = r$ with $r \in \{1, -1\}$, then $3r = 1 - (-2)^d$, so $(-2)^d \in \{-2, 4\}$, while $|(-2)^d| = 2^d \geq 8$ for $d \geq 3$. Over a field K of characteristic zero the same two evaluations give the second claim: if $A_d = c$ is constant, then $c = (-1)^{d-1}$ from $t = 0$ and $3c = 1 - (-2)^d$ from $t = -2$, whence $(-2)^d = 1 - 3(-1)^{d-1} \in \{-2, 4\}$ in K; as both sides are images of integers under $\mathbb{Z} \to K$, which is injective, the same contradiction applies. □

Theorem 4.3. *Let $m, n \in \mathbb{N}$ with $0 < m$, $2m < n$ and $\gcd(m, n) \geq 3$. Then $F_{m,n}$ is not squarefree in $\mathbb{Z}[t]$. In particular, for every $k \geq 3$ the polynomial $F_{3,3k}$ is not squarefree, so Conjecture 5.2 fails on an infinite family of pairs.*

Proof. By Theorem 3.1, $A_d \cdot A_d$ divides $F_{m,n}$ with $d = \gcd(m, n)$, and by Lemma 4.2 the factor A_d is not a unit of $\mathbb{Z}[t]$; squarefreeness would force it to be one. For the second claim take $m = 3$, $n = 3k$: then $2m = 6 < 3k$ exactly when $k \geq 3$, and $\gcd(3, 3k) = 3$. □

Theorem 4.4. *Let $m, n \in \mathbb{N}$ with $0 < m$, $2m < n$ and $\gcd(m, n) \geq 3$. Then there is $z \in \mathbb{C}$ with*

$$F_{m,n}(z) = 0 \qquad \text{and} \qquad F'_{m,n}(z) = 0,$$

that is, $F_{m,n}$ has a multiple root. This is the literal statement of Conjecture 5.2, refuted.

Proof. Put $d = \gcd(m, n)$. By Lemma 4.2, $A_d \in \mathbb{C}[t]$ is not constant, so it has a root $z \in \mathbb{C}$ because $\mathbb{C}$ is algebraically closed. Write $F_{m,n} = A_d^2 G$ using Theorem 3.1. Then $F_{m,n}(z) = 0$, and $F'_{m,n} = 2A_d A'_d G + A_d^2 G'$ also vanishes at z, both terms carrying a factor $A_d(z) = 0$. □

We record the negative control against the natural over-shoot of Theorem 3.1: already at $(3, 9)$ the exponent 2 cannot be raised to 3.

Proposition 4.5. *A_3^3 does not divide $F_{3,9}$ in $\mathbb{Q}[t]$; equivalently, the multiplicity of the root $t = 1$ of $F_{3,9}$ is exactly two.*

Proof. $A_3 = 1 - t$, and by Theorem 4.1 we have $F_{3,9} = (t - 1)^2 C$ with $C = 4t^3 - 27t^2 + 18t - 3$. If $(1 - t)^3$ divided $F_{3,9}$ then $t - 1$ would divide C, whereas $C(1) = 4 - 27 + 18 - 3 = -8 \neq 0$. □

5. The repaired law

Theorem 3.1 says that A_d^2 always divides $F_{m,n}$. It says nothing about whether anything *else* divides $F_{m,n}$ twice, and that missing half is exactly the content Conjecture 5.2 was trying to assert. Computation says the answer is no.

Conjecture A. Let $m, n \in \mathbb{N}$ with $0 < m$ and $2m < n$. Then, in $\mathbb{Q}[t]$ and up to a nonzero constant factor,

$$\gcd\big(F_{m,n},\, F'_{m,n}\big) = A_{\gcd(m,n)}.$$

Equivalently: $F_{m,n}$ is squarefree if and only if $\gcd(m, n) \leq 2$, and when it is not, its non-squarefree part is exactly $A_{\gcd(m,n)}$.

The equivalence is the standard criterion — a nonzero $F \in K[t]$ over a field of characteristic zero is squarefree if and only if $\gcd(F, F')$ is a nonzero constant — read against $\deg A_d = \lfloor (d-1)/2 \rfloor$, which vanishes exactly for $d \leq 2$ (Remark 2.3); on the window of Theorem 5.1 that dichotomy is verified directly, pair by pair, rather than through the degree formula. Note that Conjecture A implies the corrected form of Conjecture 5.2, namely that $F_{m,n}$ has no multiple root when $\gcd(m, n) \leq 2$, and by Theorem 4.4 the condition $\gcd(m, n) \leq 2$ is necessary.

Theorem 5.1. *Conjecture A holds for every pair (m,n) with $3 \le n \le 30$, $0 < m$ and $2m < n$ — all 210 of them, of which 37 have $\gcd(m,n) \ge 3$ and 173 have $\gcd(m,n) \le 2$. In particular, on that window $F_{m,n}$ is squarefree if and only if $\gcd(m,n) \le 2$.*

Proof (exhaustive verification). The verification is by an explicit certificate for each of the 210 pairs, and the certificate is checked, not the conclusion. Fix a pair, put $d = \gcd(m,n)$, and let $p, q \in \mathbb{Z}[t]$ be the outputs of a synthetic division of $F_{m,n}$ and $F'_{m,n}$ by A_d that truncates its integer quotients; nothing is assumed about that division, and the first two identities below are what make it exact. The stored data are two polynomials $u, v \in \mathbb{Z}[t]$ and an integer c, and what is checked is

$$A_d\, p = F_{m,n}, \qquad A_d\, q = F'_{m,n}, \qquad up + vq = c, \qquad c \neq 0,$$

all four as identities of integer coefficient vectors. The first two turn the divisions from assumptions into facts: the quotients are recomputed and multiplied back, so a division that was not exact cannot pass. The third is a Bézout identity: every common divisor of p and q in $\mathbb{Q}[t]$ divides the constant $c \neq 0$, hence is a unit, so $\gcd(p,q) = 1$ and

$$\gcd(F_{m,n}, F'_{m,n}) = \gcd(A_d p,\, A_d q) = A_d \cdot \gcd(p,q) = A_d$$

up to a nonzero constant. No polynomial gcd algorithm, resultant or factorisation routine is trusted anywhere: per pair, and on top of forming $F_{m,n}$ and $F'_{m,n}$ from the recurrence, the checked computation is two divisions, four multiplications, one addition, three equality tests between coefficient vectors and one test $c \neq 0$. A separate check confirms that the certificate table covers exactly the 210 pairs of the window and no others, and a further evaluation over the same window records that $A_{\gcd(m,n)}$ is a constant exactly when $\gcd(m,n) \le 2$; that is what turns the gcd equality into the squarefreeness dichotomy.

For instance, at the smallest pair $(m,n) = (1,3)$ one has $F_{1,3} = 4t - 3$, $F'_{1,3} = 4$, $A_1 = 1$ and the certificate $(u,v,c) = (0,1,4)$. At the smallest failing pair $(m,n) = (3,9)$ one has $A_3 = 1 - t$,

$$p = -4t^4 + 31t^3 - 45t^2 + 21t - 3, \qquad q = -20t^3 + 120t^2 - 108t + 24,$$

and the stored certificate is $u = 2040t^2 - 11420t + 6456$, $v = -408t^3 + 2998t^2 - 3391t + 819$, $c = 288$.

The Bézout data were produced outside the formal development; only the four displayed identities are verified inside it. The passage from them to the displayed gcd equality is the one-line argument just given, which is not itself formalised. □

Proposition 5.2. *On the window of Theorem 5.1: the 210 pairs split as 37 with $\gcd(m,n) \ge 3$ and 173 with $\gcd(m,n) \le 2$, so neither side of the dichotomy is vacuous. Moreover $A_1 = 1$ and $A_2 = -1$ are constant while $A_3 = 1 - t$ is not, so the threshold in Theorem 4.3 is $\gcd(m,n) \ge 3$ and cannot be lowered to $\gcd(m,n) \ge 2$; and the values of $F_{1,7}$ and $F_{1,8}$ and the factorisation of $F_{3,9}$ come out the same in the second, independent implementation of the polynomial arithmetic as in the first.*

Proof. Each assertion is a finite evaluation over the window, or over the single indices $1, 2, 3$; see §7. □

The pair $(m,n) = (1,7)$ is worth singling out as the control in the other direction: it lies in the conjecture's range, $\gcd(1,7) = 1$, and $F_{1,7}$ *is* squarefree. So Conjecture 5.2 is not false everywhere — it is false exactly where $\gcd(m,n) \ge 3$, as far as computation reaches.

6. The two curves printed in the source

Before making any of the claims above we recomputed, from Definition 2.1 alone, the two curves that [1, §5] prints, as a check on our reading of the source.

Theorem 6.1. *Over every commutative ring,*

$$F_{1,7} = A_6^2 - 4A_5A_7 = 4t^5 - 27t^4 + 72t^3 - 66t^2 + 24t - 3,$$
$$F_{1,8} = A_7^2 - 4A_6A_8 = t^6 + 36t^5 - 138t^4 + 186t^3 - 111t^2 + 30t - 3.$$

These are the right-hand sides of the curves $H_{7,6,5}$ and $H_{8,7,6}$ as printed in [1, §5].

Proof. Expand $A_5, \dots, A_8$ by the recurrence and compare coefficients. □

Both agree with the source exactly. The two polynomials have degrees 5 and 6, and both pairs $(1, 7)$ and $(1, 8)$ lie in the window of Theorem 5.1 with gcd = 1, so both are squarefree — consistent with the genus-2 claim of [1] for those curves.

7. The extent of the computation

We state precisely which assertions rest on exhaustive computation and how large each search was.

- Theorems 3.1, 4.3, 4.4 and Lemmas 2.5, 2.6, 4.2 rest on no computation at all: they are proofs by induction and by two specialisations, uniform in m, n and the ring.
- Theorems 4.1 and 6.1 and Proposition 4.5 are fixed polynomial identities in one or two variables, expanded symbolically.
- Theorem 5.1 is the only exhaustive claim. The search is the complete set of 210 pairs (m, n) with $3 \le n \le 30$, $0 < m$, $2m < n$ — the conjecture's whole hypothesis range up to $n = 30$ — and for each pair the four identities displayed in its proof are evaluated over $\mathbb{Z}$; a second evaluation over the same window records the constancy dichotomy for $A_{\gcd(m,n)}$, and a third checks that the table of certificates covers exactly those 210 pairs. The certificate table holds 6 715 integers, the largest of 77 decimal digits.
- Outside the formal development, and only as corroboration, the same law $\gcd(F_{m,n}, F'_{m,n}) = A_{\gcd(m,n)}$ was checked in PARI/GP [6] for every pair with $n \le 80$ — 1560 pairs — with no anomaly, using that system's own polynomial gcd; and the identity of Remark 3.2 was checked there for all 870 pairs with $n \le 60$.
- Proposition 5.2 is five finite evaluations: the count of the window, and four at fixed indices (A_1, A_2, A_3, and $F_{1,7}$, $F_{1,8}$, $F_{3,9}$ in the second implementation).

The window stops at $n = 30$ for a reason that has nothing to do with the arithmetic, and we record it because it is the frontier for anyone extending this. The certificate string for $n \le 30$ is 209 179 characters long; the corresponding data for $n \le 40$ (380 pairs) is about 749 KB and for $n \le 50$ about 2.1 MB. Generating them is seconds of work at any of these sizes. The obstruction is the proof assistant's handling of the literal: at $n \le 40$ the evaluation exhausts memory, at 1.56 GB after 4.8 CPU-seconds, in the interpreter that decodes the table — not in the arithmetic, which is trivial. Even at $n \le 30$ the table had to be encoded as a single whitespace-separated decimal *string*, decoded by a hand-written scanner, rather than as a nested array literal of the same data (which needs 6 295 numerals, the per-pair lengths being implicit in the nesting): the nested literal did not finish elaborating in nine wall-clock minutes, with memory flat, i.e. the cost was in the nesting of the literal and not in its size. Flattening the table to one scalar sequence and decoding it inside the development removed that cost entirely.

8. Verification

Every statement above — Definitions 2.1 and 2.2, Lemmas 2.5, 2.6 and 4.2, Theorems 3.1, 4.1, 4.3, 4.4, 5.1 and 6.1, and Propositions 4.5 and 5.2 — has been machine-checked in Lean 4 [7] against Mathlib [8]. The development is three files. The first carries the whole refutation, Theorems 3.1–4.4 together with Theorems 4.1 and 6.1 and Proposition 4.5, inside Mathlib's polynomial ring; it is kernel-clean, with no appeal to compiled evaluation anywhere, and the axiom closure of each of its theorems is the standard one: propositional extensionality and quotient soundness, with the axiom of choice appearing in exactly those theorems stated inside a Mathlib polynomial ring rather than over an arbitrary commutative ring. The second file is an independent, import-free implementation of integer polynomials as coefficient arrays, on which the certificate check of Theorem 5.1 is defined; the third holds the certificate table and the theorems that evaluate it, each of which carries in addition a single native-evaluation axiom recording that compiled evaluation. The separation is deliberate: everything that refutes Conjecture 5.2 is kernel-checked, and the trusted computational input is confined to the finite window of §7. Two limitations should be stated. The array layer is a transcription of polynomial

arithmetic, and its agreement with the polynomial layer is not proved but cross-checked, on $F_{1,7}$, $F_{1,8}$ and the factorisation of $F_{3,9}$ (Proposition 5.2); and the deduction of the gcd equality from the four verified identities, given in the proof of Theorem 5.1, is a paper argument. There is no `sorry` anywhere in the development. Repository reference to be added at submission.

9. What remains

Conjecture A splits into two independent halves, and Theorem 3.1 settles neither.

(1) *The multiplicity is exactly two*: $A_d^3 \nmid F_{m,n}$ for $d = \gcd(m,n) \geq 3$. Proposition 4.5 proves this at $(3,9)$ only. Remark 3.2 reduces it to showing $4\theta^{n-2m}A_m(\theta)^2 \neq 3A_{n-m}(\theta)^2$ at every root θ of A_d; and since a short computation from the closed form shows the roots of A_k to be the values $\zeta/(1+\zeta)^2$ at the k-th roots of unity $\zeta \notin \{1,-1\}$, this is a statement about roots of unity. The ingredient still to be formalised is Catalan's identity for (A_k), for which Lemma 2.5 together with d'Ocagne's identity $A_{b+c}A_{b+1} - A_{b+c+1}A_b = t^b A_c$ — one induction on b — is enough.

(2) *Nothing else repeats*: $F_{m,n}/A_d^2$ is squarefree and coprime to A_d. This is the original assertion of Conjecture 5.2 with the obstruction divided out, and it is open; we have only the verification of Theorem 5.1 and the corroboration to $n \leq 80$.

Finally, [1] contains, commented out in the LaTeX source of the e-print and so not part of its text, the analogous reduction for exponents $x^{n+m} + x^n + x^{n-m} + a$ in arithmetic progression, with curve $H_{n+m,n,n-m} : s^2 = A_n^2 - 4A_{n-m}A_{n+m}$. That discriminant is $F_{m,n+m}$ in the notation of Definition 2.2, so Theorem 3.1 applies to it verbatim, with the same threshold $\gcd(m, n+m) = \gcd(m,n) \geq 3$.

References

[1] A. Bremner and M. Ulas, *Some observations concerning reducibility of quadrinomials*, Acta Math. Hungar. **145** (2015), no. 2, 320–349; DOI 10.1007/s10474-015-0478-9. Cited here in the arXiv e-print arXiv:1310.5346v1 [math.NT] (20 October 2013), which is its only version; Lemma 3.1, Corollary 3.2, §5 (Theorem*, the curves $H_{7,6,5}$ and $H_{8,7,6}$) and Conjecture 5.2. See §1.1 for what could and could not be read.

[2] Y. Zhang and H. Zhu, *On the reducibility of some special quadrinomials*, arXiv:1605.01294v2 [math.NT] (21 May 2016). Cited as an e-print: no journal version is recorded by Crossref, and zbMATH indexes it as a preprint. It uses Lemma 3.1 and Corollary 3.2 of [1], citing the published version; it does not discuss $F_{m,n}$ or Conjecture 5.2.

[3] M. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith. **21** (1972), 153–171; DOI 10.4064/aa-21-1-153-171.

[4] M. Fried and A. Schinzel, *Corrigendum and addendum to the paper "Reducibility of quadrinomials"*, Acta Arith. **99** (2001), 409–410; DOI 10.4064/aa99-4-7.

[5] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), in three instalments: no. 2, 184–196; no. 3, 197–240; no. 4, 289–321. The source of the divisibility property used in Lemma 2.6; our proof of that lemma is self-contained from the recurrence.

[6] The PARI Group, *PARI/GP*, version 2.13.3, Univ. Bordeaux; `http://pari.math.u-bordeaux.fr/`. Used only for the corroborating computations of §7 and to produce the Bézout data that the formal development verifies.

[7] L. de Moura and S. Ullrich, *The Lean 4 theorem prover and programming language*, in: Automated Deduction — CADE 28, Lecture Notes in Computer Science 12699, Springer, 2021, 625–635; DOI 10.1007/978-3-030-79876-5_37.

[8] The mathlib Community, *The Lean mathematical library*, in: Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs (CPP 2020), ACM, 2020, 367–381; DOI 10.1145/3372885.3373824.