ROOTS OF UNITY AND RATIONAL ZEROS OF THE BERNOULLI-COEFFICIENT POLYNOMIALS $R_{k,\ell}$, UNIFORMLY IN ℓ

KOREA SUPERINTELLIGENCE LABS

ABSTRACT. For positive integers k and ℓ let $R_{k,\ell}(x) = \sum_{j=0}^{k+1}(-1)^{(\ell+1)j}\big(\frac{B_{2j}}{(2j)!}\,\frac{B_{2k+2-2j}}{(2k+2-2j)!}\big)^{\ell}x^j$, the two-parameter family of reciprocal polynomials introduced by Maji and Sarkar [2] and studied by Charan, Meher and Pathak [1], who prove that all zeros of $R_{k,\ell}$ except two real ones, $\alpha_{k,\ell} > 1$ and $1/\alpha_{k,\ell}$, lie on the unit circle. The concluding section of [1] asks which zeros of $R_{k,\ell}$ are roots of unity, reports that computation suggests none besides ± 1 when $\ell > 1$, and says that "a proof of this fact seems elusive"; it also asks whether $R_{k,\ell}$ is irreducible, noting that this would entail the irrationality of $\alpha_{k,\ell}$. For $\ell = 1$, where $R_{k,1}(x^2)$ is the Ramanujan polynomial, the roots-of-unity question is answered by a theorem of Murty, Smyth and Wang [3]; for $\ell > 1$ nothing appears to have been known. We prove three statements, each for *every* $\ell \geq 1$. First, for $k \in \{8, 11, 13, 14\}$ no cyclotomic polynomial Φ_d with $d \geq 3$ divides $R_{k,\ell}$ over $\mathbb{Q}$: an integral model whose dependence on ℓ sits entirely in the exponents of fixed integers lets Fermat's little theorem collapse ℓ to a residue modulo $p-1$, so finitely many evaluations in $\mathbb{F}_p$ certify all ℓ at once, and a lower bound $n \leq 2\varphi(n)^2$ for Euler's totient makes the set of candidate orders finite. Second, a 2-adic structure theorem: $v_2(c_{k,j}/c_{k,0}) = v_2\binom{k+1}{j} - 1$ for the coefficient bases $c_{k,j}$, so that the reduction modulo 2 of the integral model does not depend on ℓ at all; this sieve alone settles the roots-of-unity question at $k \in \{2, 26, 44\}$. Third, $R_{11,\ell}$ and $R_{13,\ell}$ have no rational zero, and every rational zero of $R_{8,\ell}$ and $R_{14,\ell}$ is ± 1; with the unit-circle theorem of [1] this gives the irrationality of $\alpha_{k,\ell}$ for $k \in \{8, 11, 13, 14\}$ — the consequence of irreducibility that [1] names, obtained without irreducibility. The three statements are machine-checked in Lean 4; the final step to $\alpha_{k,\ell}$ rests on the cited theorem of [1] and is not.

1. INTRODUCTION

Let $B_0, B_1, B_2, \ldots$ be the Bernoulli numbers. For positive integers k and ℓ put

$$R_{k,\ell}(x) \;:=\; \sum_{j=0}^{k+1}(-1)^{(\ell+1)j}\left(\frac{B_{2j}}{(2j)!}\cdot\frac{B_{2k+2-2j}}{(2k+2-2j)!}\right)^{\ell}x^j. \tag{1}$$

These polynomials were introduced by Maji and Sarkar [2], who conjectured that all non-real zeros of $R_{k,\ell}$ lie on the unit circle. For $\ell = 1$ the substitution $x \mapsto x^2$ turns (1) into the *Ramanujan polynomial* $R_{2k+1}(x) = R_{k,1}(x^2)$ of Murty, Smyth and Wang [3], so (1) is a genuine two-parameter deformation of a classical object.

Charan, Meher and Pathak [1] settle the Maji–Sarkar conjecture in a sharp form: except for two real zeros $\alpha_{k,\ell}$ and $1/\alpha_{k,\ell}$ with $\alpha_{k,\ell} > 1$, all zeros of $R_{k,\ell}$ lie on the unit circle, and all zeros are simple (their Theorem 1.1). Their concluding remarks then pose two new questions. We quote the passage as it stands in the arXiv v1 e-print of [1], whose internal numbering we use throughout:

> For instance, the irreducibility of $R_{k,\ell}(z)$ over $\mathbb{Q}$ when k is odd and that of $R_{k,\ell}(z)/(z-(-1)^{\ell})$ when k is even, is a natural question. Numerical evidence suggests that this is indeed the case. Note that a proof of such a fact would entail the irrationality of the real zero $\alpha_{k,\ell}$ of $R_{k,\ell}(z)$. A related problem is to identify whether any of the zeros of $R_{k,\ell}(z)$ are roots of unity. Preliminary computations suggest that except for ± 1, the other zeros of $R_{k,\ell}(z)$ are not roots of unity for $\ell > 1$, but a proof of this fact seems elusive.

The same paper says in its first section that "the roots of unity which may be zeros of $R_{k,\ell}(x)$ appear to be very subtle and involved in this generality. We relegate these investigations to future research."

The second question is the main subject of this paper. For $\ell = 1$ it is completely answered in [3]: reading their Theorem 6.1 through $R_{2k+1}(x) = R_{k,1}(x^2)$, the only cyclotomic factors of $R_{k,1}$ are $\Phi_2 = z+1$ when k is even and $\Phi_3 = z^2+z+1$ when $3 \mid k$, and there are no others. Their argument is archimedean — a resultant is a nonzero integer, together with an estimate on the unit circle — and is stated for the Ramanujan polynomial only. It does not survive raising the Bernoulli products to the power ℓ, and for $\ell > 1$ we are aware of no result at all; this is the state of affairs that the word "elusive" in [1] records.

The difficulty is that ℓ is a quantifier, not a parameter one may fix and compute with. Any finite computation settles finitely many ℓ. Our starting point is that (1) nevertheless carries an ℓ-free skeleton.

The ratios of the coefficient bases do not depend on ℓ.

Writing $c_{k,j} = \frac{B_{2j}}{(2j)!} \cdot \frac{B_{2k+2-2j}}{(2k+2-2j)!}$, so that $R_{k,\ell} = \sum_j (-1)^{(\ell+1)j} c_{k,j}^{\ell} x^j$, the quotients $c_{k,j}/c_{k,0}$ are rational numbers independent of ℓ. Clearing their common denominator once and dividing by the content gives coprime integers $b_0, \dots, b_{k+1}$ with $c_{k,j} b_0 = c_{k,0} b_j$, and then, for *every* $\ell \geq 0$,

$$R_{k,\ell} = \left(\frac{c_{k,0}}{b_0}\right)^{\ell} \cdot W_{\ell}, \qquad W_{\ell}(x) = \sum_{j=0}^{k+1} (-1)^{(\ell+1)j} b_j^{\ell} x^j \in \mathbb{Z}[x]. \tag{2}$$

All of the ℓ-dependence now sits in the exponents of *fixed* integers. Reducing (2) modulo an odd prime p and evaluating at an element $z \in \mathbb{F}_p$ of exact order d, Fermat's little theorem replaces b_j^{ℓ} by b_j^{r} with $r = 1 + ((\ell - 1) \bmod (p-1)) \in \{1, \dots, p-1\}$ — and $p-1$ is even, so the sign $(-1)^{(\ell+1)j}$ transports as well. Checking the $p-1$ residues r therefore certifies all $\ell \geq 1$ simultaneously. What remains is to make the order d range over a finite set, and for that we prove the classical totient lower bound $n \leq 2\varphi(n)^2$ (Section 5), which turns the degree constraint $\varphi(d) \leq k+1$ into $d \leq 2(k+1)^2$.

The first outcome is the following.

Theorem 1.1 (Theorem 6.1 below)**.** *Let $k \in \{8, 11, 13, 14\}$. For every $\ell \geq 1$ and every $d \geq 3$, the cyclotomic polynomial Φ_d does not divide $R_{k,\ell}$ in $\mathbb{Q}[x]$. Equivalently: if z is a root of unity and $R_{k,\ell}(z) = 0$, then $z = 1$ or $z = -1$.*

At $\ell = 1$ this reproves the Murty–Smyth–Wang statement at those four values of k (none of which is divisible by 3) by an entirely different, non-archimedean route; for $\ell \geq 2$ it is, to our knowledge, the first case of the question of [1] to be settled, and it is settled for all ℓ at once. The restriction $d \geq 3$ is necessary and not an artefact: for k even, Φ_1 or Φ_2 really does divide $R_{k,\ell}$, by Proposition 3.1 of [1] (Proposition 2.2 below). The restriction on k is likewise not a formality: at $k = 3$, $\ell = 1$ the conclusion is false, and we exhibit the factorisation (Proposition 7.1).

The reduction modulo 2 of the model (2) is special: since $b^{\ell} \equiv b$ and $-1 \equiv 1$ modulo 2 for $\ell \geq 1$, it does not depend on ℓ at all, and a 2-adic structure theorem (Theorem 8.1, from the von Staudt–Clausen theorem) identifies it in terms of the binary digits of $k+1$. Where the resulting sieve leaves no candidate order, the question is settled with no computation per order and none per ℓ:

Theorem 1.2 (Theorem 9.2 below)**.** *Let $k \in \{2, 26, 44\}$. For every $\ell \geq 1$ and every $d \geq 3$, Φ_d does not divide $R_{k,\ell}$ in $\mathbb{Q}[x]$; equivalently, the only zeros of $R_{k,\ell}$ that are roots of unity are ± 1.*

The same Fermat periodicity reaches the arithmetic consequence that [1] attaches to its first question. A rational zero of $R_{k,\ell}$ transports, modulo a prime not dividing b_{k+1}, to a zero of the reduced model in $\mathbb{F}_p$, and a certificate that there is none — or none beyond the predicted ± 1, with that zero simple — is again a finite check over the residues r.

Theorem 1.3 (Theorems 10.4 and 10.5 below)**.** *For every $\ell \geq 1$: $R_{11,\ell}$ and $R_{13,\ell}$ have no rational zero, and every rational zero of $R_{8,\ell}$ and of $R_{14,\ell}$ is 1 or -1. Consequently every real zero of $R_{11,\ell}$ and $R_{13,\ell}$, and every real zero of $R_{8,\ell}$ and $R_{14,\ell}$ other than ± 1, is irrational.*

Since $\alpha_{k,\ell} > 1$ is a real zero by [1, Theorem 1.1], the numbers $\alpha_{k,\ell}$ and $1/\alpha_{k,\ell}$ are irrational for $k \in \{8, 11, 13, 14\}$ and every $\ell \geq 1$ (Corollary 10.6). This is the consequence that [1] derives from an irreducibility it does not prove; here it is obtained without irreducibility, which remains untouched (Section 13).

A factorisation census over $1 \leq k \leq 80$, $1 \leq \ell \leq 10$ is recorded in Section 12 as a computation outside the machine-checked development. Section 13 says what the present methods do not reach.

Changes from version 1. Version 1 of this paper contained Sections 2–7 as they stand here, the census of Section 12, the explicit form of the 2-adic structure theorem (Theorem 8.2) as a prose result, and the rational-root route to the irrationality of $\alpha_{k,\ell}$ as a suggestion only. New in this version: Theorem 8.1 (the 2-adic structure theorem, now machine-checked in its valuation form) and its sieve consequence Theorem 9.2 at $k \in \{2, 26, 44\}$ (Sections 8–9); Theorems 10.4 and 10.5 on rational zeros and irrationality at $k \in \{8, 11, 13, 14\}$, with Corollary 10.6 (Section 10); the controls for these two layers (Section 11); the corresponding updates to Remark 6.3, to Sections 13 and 14 and to the provenance paragraph; and Appendix A, which lists the formal statement of every machine-checked result. The title now names the second question as well. The numbering of [1] used here (Theorem 1.1, Theorem 1.2, Proposition 3.1 of the compiled v1 e-print) and the bibliographic data of [1] were already corrected in version 1 and are unchanged. Nothing proved in version 1 is weakened or withdrawn; the only refereed statement that changes is Remark 6.3, which is sharpened by Theorem 10.4.

2. The polynomials, and their behaviour at ± 1

Throughout, k and ℓ are positive integers, $n := k + 1$, and

$$c_{k,j} := \frac{B_{2j}}{(2j)!} \cdot \frac{B_{2k+2-2j}}{(2k+2-2j)!} \qquad (0 \leq j \leq k+1), \tag{3}$$

so that $R_{k,\ell}(x) = \sum_{j=0}^{k+1} a_{k,\ell,j} x^j$ with $a_{k,\ell,j} = (-1)^{(\ell+1)j} c_{k,j}^{\ell}$. Thus $\deg R_{k,\ell} \leq k+1$, with equality because $c_{k,k+1} = B_{2k+2}/(2k+2)! \neq 0$; the instance we use, $\deg R_{8,\ell} = 9$ for all ℓ, is verified in Proposition 7.1. We write Φ_d for the d-th cyclotomic polynomial, φ for Euler's totient and v_2 for the 2-adic valuation.

The first two statements are due to [1]; we record them because the main theorem is stated against them, and because the second is exactly the source of the ± 1 that the main theorem must exclude from its conclusion.

Proposition 2.1. *For all $k, \ell \geq 1$ and all $0 \leq j \leq k+1$,*

$$c_{k,\,k+1-j} = c_{k,j}, \qquad a_{k,\ell,\,k+1-j} = (-1)^{(\ell+1)(k+1)}\, a_{k,\ell,j}.$$

Proof. The first identity is the substitution $j \mapsto k+1-j$ in (3), which exchanges the two factors: $2(k+1-j) = 2k+2-2j$ and $2k+2-(2k+2-2j) = 2j$. The second follows by feeding it into $a_{k,\ell,j} = (-1)^{(\ell+1)j} c_{k,j}^{\ell}$ and comparing the two sign exponents modulo 2, using $(\ell+1)(k+1-j) + (\ell+1)j = (\ell+1)(k+1)$. □

Reading Proposition 2.1 off the coefficient list gives the reciprocity that [1] states in its first section ("It is easy to see that $R_{k,\ell}(x)$ is a reciprocal polynomial, that is $x^{k+1} R_{k,\ell}(1/x) = \pm R_{k,\ell}(x)$"), with the sign identified as $(-1)^{(\ell+1)(k+1)}$.

Proposition 2.2 ([1, Proposition 3.1])**.** *Let k be even. Then $R_{k,\ell}(1) = 0$ if ℓ is even, and $R_{k,\ell}(-1) = 0$ if ℓ is odd.*

Proof. For k even the involution $j \mapsto k+1-j$ of $\{0, 1, \ldots, k+1\}$ has no fixed point and reverses the parity of j, since $k+1$ is odd. Hence by Proposition 2.1 the sum $\sum_{j=0}^{k+1} (-1)^j c_{k,j}^{\ell}$ equals its own negative and therefore vanishes. For ℓ even, $(-1)^{(\ell+1)j} = (-1)^j$ and evaluating $R_{k,\ell}$ at 1 gives exactly that sum; for ℓ odd, $(-1)^{(\ell+1)j} = 1$ and evaluating at -1 gives it again. □

(The proof of [1, Proposition 3.1] proceeds instead through the rewriting of the coefficients in terms of $q_j = \zeta(2j)\zeta(2k+2-2j)/\zeta(2k+2)$; the reflection argument above is what we verified.)

3. An ℓ-free integral model

Fix k and let $B = (b_0, \dots, b_{k+1})$ be integers. Define

$$W_{B,\ell}(x) \;:=\; \sum_{j=0}^{k+1} (-1)^{(\ell+1)j} b_j^{\ell}\, x^j \;\in\; \mathbb{Z}[x]. \tag{4}$$

If $b_0 \neq 0$ then $W_{B,\ell} \neq 0$, because its constant coefficient is b_0^{ℓ}.

Lemma 3.1. *Suppose $b_0 \neq 0$, $c_{k,0} \neq 0$ and*

$$c_{k,j}\, b_0 = c_{k,0}\, b_j \qquad (0 \le j \le k+1). \tag{5}$$

Then for every $\ell \ge 0$, $R_{k,\ell} = \big(c_{k,0}/b_0\big)^{\ell} W_{B,\ell}$ in $\mathbb{Q}[x]$. Consequently, if Φ_d divides $R_{k,\ell}$ in $\mathbb{Q}[x]$ then Φ_d divides $W_{B,\ell}$ in $\mathbb{Z}[x]$.

Proof. By (5), $c_{k,j} = c_{k,0} b_j / b_0$, so $a_{k,\ell,j} = (c_{k,0}/b_0)^{\ell} \cdot (-1)^{(\ell+1)j} b_j^{\ell}$ coefficientwise, which is the asserted identity. The scalar $(c_{k,0}/b_0)^{\ell}$ is a nonzero rational, so $\Phi_d \mid R_{k,\ell}$ in $\mathbb{Q}[x]$ gives $\Phi_d \mid W_{B,\ell}$ in $\mathbb{Q}[x]$; since Φ_d is monic with integer coefficients and $\mathbb{Z} \to \mathbb{Q}$ is injective, the divisibility descends to $\mathbb{Z}[x]$ (Gauss). □

Only the existence of *some* integer vector B satisfying (5) is used; in practice one takes b_j coprime, obtained by clearing denominators in the rational numbers $c_{k,j}/c_{k,0}$ and dividing out the content. Note that $W_{B,\ell}$ is then primitive for every ℓ, since a prime dividing every b_j^{ℓ} divides every b_j.

Example 3.2. For $k = 8$ (so $n = 9$) one may take

$$\begin{aligned} B = (&438670,\ -1443183,\ -949620,\ -892772,\ -881790,\\ &-881790,\ -892772,\ -949620,\ -1443183,\ 438670), \end{aligned}$$

a palindrome, as Proposition 2.1 demands. For $k = 11, 13, 14$ the corresponding vectors have 13, 15 and 16 entries and leading terms 7090922730, 47498922058 and 17231682552010 respectively.

4. Fermat periodicity, and a certificate valid for all ℓ

Lemma 4.1 (periodicity)**.** *Let p be an odd prime, $z \in \mathbb{F}_p$, and B as above. Put*

$$E_{B,p,z}(r) \;:=\; \sum_{j=0}^{k+1} (-1)^{(r+1)j}\, \overline{b_j}^{\,r}\, z^j \;\in\; \mathbb{F}_p.$$

Then for every $\ell \ge 1$ one has $E_{B,p,z}(\ell) = E_{B,p,z}\big(1 + ((\ell-1) \bmod (p-1))\big)$.

Proof. Write $\ell = 1 + s + (p-1)q$ with $s = (\ell-1) \bmod (p-1)$. For each j: if $\overline{b_j} = 0$ then $\overline{b_j}^{\ell} = 0 = \overline{b_j}^{1+s}$, both exponents being positive; otherwise $\overline{b_j}^{\ell} = \overline{b_j}^{1+s} (\overline{b_j}^{\,p-1})^q = \overline{b_j}^{1+s}$ by Fermat. For the signs, $p-1$ is even, so $\ell \equiv 1 + s \pmod 2$ and hence $(\ell+1)j \equiv (1+s+1)j \pmod 2$ for every j. □

The point of Lemma 4.1 is that the map $\ell \mapsto E_{B,p,z}(\ell)$ takes at most $p-1$ values, all of them attained at $\ell \in \{1, \dots, p-1\}$. A finite check therefore controls an infinite family.

Lemma 4.2 (certificate)**.** *Let p be an odd prime, let $d \ge 1$, and let $z \in \mathbb{F}_p$ have exact order d, that is $z^d = 1$ and $z^m \neq 1$ for $0 < m < d$. If*

$$E_{B,p,z}(r) \neq 0 \qquad \text{for every } r \in \{1, 2, \dots, p-1\},$$

then Φ_d does not divide $W_{B,\ell}$ in $\mathbb{Z}[x]$, for any $\ell \ge 1$.

Proof. Suppose $\Phi_d \mid W_{B,\ell}$ over $\mathbb{Z}$ for some $\ell \ge 1$. Reducing mod p gives $\overline{\Phi_d} \mid \overline{W_{B,\ell}}$ in $\mathbb{F}_p[x]$, and $\overline{\Phi_d}$ is the d-th cyclotomic polynomial over $\mathbb{F}_p$. Since z has exact order d it is a primitive d-th root of unity in $\mathbb{F}_p$, hence a root of $\overline{\Phi_d}$, hence a root of $\overline{W_{B,\ell}}$. But $\overline{W_{B,\ell}}(z) = E_{B,p,z}(\ell)$, which by Lemma 4.1 equals $E_{B,p,z}(r)$ for some $r \in \{1, \dots, p-1\}$, and that is nonzero by hypothesis. □

5. A lower bound for Euler's totient

To apply Lemma 4.2 one must know that only finitely many orders d can occur. The degree of Φ_d is $\varphi(d)$, so $\Phi_d \mid W_{B,\ell}$ forces $\varphi(d) \le k+1$; what is needed is that this bounds d. The bound we use is classical, and sharp at $n = 2$.

Proposition 5.1. *For every $n \in \mathbb{N}$, $n \le 2\varphi(n)^2$. Consequently, if $\varphi(d) \le N$ then $d \le 2N^2$.*

Proof. Multiplicative induction, carrying the strengthened invariant

$$n \le 2\varphi(n)^2 \quad \text{and} \quad \big(n \text{ odd} \implies n \le \varphi(n)^2\big),$$

which is needed because the coprime step would otherwise lose a factor 2 each time. For an odd prime power p^a with $a \ge 1$ one has $p \le (p-1)^2$ (as $p \ge 3$) and $p^{a-1} \le (p^{a-1})^2$, so $p^a = p^{a-1} \cdot p \le (p^{a-1})^2(p-1)^2 = \varphi(p^a)^2$. For $p = 2$, $2^a \le 2^{2a-1} = 2 \cdot (2^{a-1})^2 = 2\varphi(2^a)^2$. If $n = ab$ with a, b coprime then at most one of a, b is even, and φ is multiplicative, so the two invariants multiply: the odd factor contributes its sharper bound and the single factor 2 is spent at most once. The cases $n = 0, 1$ are immediate. The consequence is $d \le 2\varphi(d)^2 \le 2N^2$. □

Lemma 5.2. *Let $b_0 \ne 0$ and let B have $k+2$ entries. If Φ_d divides $W_{B,\ell}$ in $\mathbb{Z}[x]$, then $\varphi(d) \le k+1$ and $d \le 2(k+1)^2$.*

Proof. $W_{B,\ell} \ne 0$ and $\deg W_{B,\ell} \le k+1$, so a divisor has degree at most $k+1$; $\deg \Phi_d = \varphi(d)$; and Proposition 5.1 converts the bound on $\varphi(d)$ into one on d. □

6. The main theorem

Theorem 6.1. *Let $k \in \{8, 11, 13, 14\}$. For every integer $\ell \ge 1$ and every integer $d \ge 3$, the cyclotomic polynomial Φ_d does not divide $R_{k,\ell}$ in $\mathbb{Q}[x]$.*

Proof sketch, with the finite computations named. Fix k and let B be the coprime integer vector of Example 3.2; the hypotheses of Lemma 3.1 are two finite verifications: $c_{k,0} \ne 0$, and the $k+2$ rational identities (5), each an exact computation with the Bernoulli numbers $B_0, \dots, B_{2k+2}$. Suppose $\Phi_d \mid R_{k,\ell}$ in $\mathbb{Q}[x]$ with $d \ge 3$ and $\ell \ge 1$. By Lemma 3.1, $\Phi_d \mid W_{B,\ell}$ in $\mathbb{Z}[x]$; by Lemma 5.2, $\varphi(d) \le k+1$ and $d \le 2(k+1)^2$. A sweep of φ over the range $d \le 2(k+1)^2$ — that is, over 162, 288, 392 and 450 values of d for $k = 8, 11, 13, 14$ — shows that d lies in the explicit list

$$\begin{aligned} k = 8: &\quad 3,4,5,6,7,8,9,10,12,14,15,16,18,20,24,30 \quad \text{(16 orders)},\\ k = 11,13,14: &\quad 3,4,5,6,7,8,9,10,11,12,13,14,15,16,\\ &\qquad 18,20,21,22,24,26,28,30,36,42 \qquad\qquad \text{(24 orders)}. \end{aligned}$$

(The lists for $k = 11, 13, 14$ coincide because no integer has totient 13, 14 or 15.) For each order d in the relevant list we supply a pair (p, z) with p an odd prime and $z \in \mathbb{F}_p$ of exact order d such that all $p-1$ values $E_{B,p,z}(r)$, $1 \le r \le p-1$, are nonzero; Lemma 4.2 then contradicts $\Phi_d \mid W_{B,\ell}$. There are $16 + 24 + 24 + 24 = 88$ such certificates. For $k = 8$ they are

d	3	4	5	6	7	8	9	10	12	14	15	16	18	20	24	30
p	13	37	691	13	43	41	37	691	37	29	31	97	73	41	73	31
z	3	6	149	4	21	3	7	371	8	4	7	70	18	2	52	3

and for $k = 11, 13, 14$ the largest primes used are 131, 691 and 593. The pairs were found by an exhaustive search over primes $p < 20000$ and, for each such p with $p \equiv 1 \pmod d$, over all elements of exact order d in $\mathbb{F}_p$; the search is heuristic, but its output is a certificate that is checked outright. □

Corollary 6.2. *Let $k \in \{8, 11, 13, 14\}$ and $\ell \ge 1$. If $z \in \mathbb{C}$ satisfies $z^m = 1$ for some $m \ge 1$ and $R_{k,\ell}(z) = 0$, then $z = 1$ or $z = -1$.*

Proof. Let $d = \operatorname{ord}(z)$ be the exact multiplicative order of z, so z is a primitive d-th root of unity. If $d \ge 3$ then Φ_d is the minimal polynomial of z over $\mathbb{Q}$, so $R_{k,\ell}(z) = 0$ forces $\Phi_d \mid R_{k,\ell}$, contradicting Theorem 6.1. Hence $d \in \{1, 2\}$, so $z^2 = 1$, so $(z-1)(z+1) = 0$. □

Corollary 6.2 is the form in which [1] asks the question. At $\ell = 1$ it agrees with [3, Theorem 6.1], which for k not divisible by 3 leaves no cyclotomic factor of $R_{k,1}$ beyond Φ_2 (k even); none of $8, 11, 13, 14$ is divisible by 3. For $\ell \geq 2$ we know of no earlier statement.

Remark 6.3. The conclusion of Corollary 6.2 cannot be sharpened to "no root of unity is a zero": for $k = 8$ and $k = 14$, Proposition 2.2 produces the zero 1 when ℓ is even and the zero -1 when ℓ is odd. For $k = 11$ and $k = 13$ the conclusion can be sharpened, and is: Theorem 10.4 below shows that $R_{11,\ell}$ and $R_{13,\ell}$ have no rational zero at all, so for these two k and every $\ell \geq 1$ no root of unity whatsoever is a zero. (At $\ell = 1$ this is also in [3, Theorem 6.1], which says that $R_{k,1}$ has no cyclotomic factor at all when k is odd and $3 \nmid k$.) The factorisation census of Section 12 is consistent with this: for k odd it finds the irreducible factor of degree $k+1$ that [1] expects at every (k, ℓ) in range except when $\ell = 1$ and $3 \mid k$, and in particular at $k = 11, 13$.

7. Sharpness and controls

The following collects the negative controls: each shows that some hypothesis above cannot be dropped, and the last two show that the statements are not vacuous.

Proposition 7.1. (i) *The hypothesis "k even" in Proposition 2.2 is needed:* $R_{1,1}(1) = \frac{1}{240} \neq 0$ *and* $R_{1,1}(-1) = -\frac{7}{720} \neq 0$.

(ii) *The parity of ℓ selects which of ± 1 vanishes:* $R_{2,1}(1) = -\frac{1}{6048} \neq 0$ *and* $R_{2,2}(-1) = \frac{53}{1828915200} \neq 0$.

(iii) *The restriction $d \geq 3$ in Theorem 6.1 is sharp:* $\Phi_1 \mid R_{8,2}$ *and* $\Phi_2 \mid R_{8,3}$.

(iv) *The restriction on k is not a formality:* $\Phi_3 \mid R_{3,1}$. *Explicitly, with* $B = (3, -10, -7, -10, 3)$ *one has* $c_{3,j} \cdot 3 = c_{3,0} \cdot b_j$ *and*

$$W_{B,1}(z) = 3 - 10z - 7z^2 - 10z^3 + 3z^4 = (1 + z + z^2)(3 - 13z + 3z^2),$$

so $R_{3,1} = (c_{3,0}/3)\, W_{B,1}$ *is divisible by* Φ_3.

(v) *The main theorem is not a statement about the zero polynomial:* $\deg R_{8,\ell} = 9$ *and* $R_{8,\ell} \neq 0$ *for every ℓ.*

Proof. (i), (ii) and (v) are exact rational computations from (1), the last using $c_{8,9} \neq 0$ together with $\deg R_{8,\ell} \leq 9$. (iii) is Proposition 2.2 with $(k, \ell) = (8, 2)$ and $(8, 3)$, since $\Phi_1 = z - 1$ and $\Phi_2 = z + 1$. For (iv), the bridge identities $c_{3,j} \cdot 3 = c_{3,0} \cdot b_j$ are four exact rational computations, the displayed factorisation is an identity in $\mathbb{Z}[x]$, and Lemma 3.1 transports it. □

Item (iv) deserves a word. It is precisely the Murty–Smyth–Wang cyclotomic factor of the Ramanujan polynomial at $3 \mid k$ [3, Theorem 6.1], recovered here from the integral model in one instance. That it is a *known* phenomenon is what makes it a useful control: Theorem 6.1 is a statement about particular k, and at $k = 3$, $\ell = 1$ the same statement is false. It also explains the shape of the obstruction our method meets. In the exhaustive certificate search over $1 \leq k \leq 16$ and primes $p < 20000$, an ℓ-uniform certificate was found for every admissible d exactly at $k = 8, 11, 13, 14$; at the other twelve values of k between 1 and 16, one to three orders d resist. The reason is structural. Suppose first that p divides none of the b_j. At $\ell \equiv 0 \pmod{p-1}$ the residue of Lemma 4.1 is $r = p - 1$, Fermat makes every $b_j^{p-1} \equiv 1$, and p is odd, so $E_{B,p,z}(p-1)$ collapses to the geometric sum $\sum_{j=0}^{n} (-z)^j$; here $-z \neq 1$ because $d \geq 3$, so that sum is $((-z)^{n+1} - 1)/(-z - 1)$ and vanishes whenever the order of $-z$ divides $n + 1 = k + 2$. That is a condition on d and k alone, so no *other* prime coprime to all the b_j repairs it. What does repair it is a prime dividing some b_j, which changes the degenerate value, and this is exactly what the certificates above do at the orders where the degeneracy bites: at $k = 8$ these orders are $d = 5$ and $d = 10$, and both use $p = 691$, which divides b_3 and b_6; at $k = 14$ they are $d = 4, 8, 16$, all three certified with $p = 593$. Where no such prime was found below 20000, the order resists. Relaxing the certificate from "all $\ell \geq 1$" to "$1 \leq \ell \leq 12$" removes the obstruction at every $k \leq 16$ with $3 \nmid k$, and fails only at $d = 3$ when $3 \mid k$ — which is exactly where $\Phi_3 \mid R_{k,1}$ genuinely holds. The search fails precisely where the statement is false. (These search statistics are measurements, not theorems; the ℓ-window certificates are not formalised here.)

8. A 2-adic structure theorem

The prime 2 plays no role in Sections 4–6, where p is odd because the sign $(-1)^{(\ell+1)j}$ has to be transported. Modulo 2 that sign is invisible, and so is the exponent ℓ: in $\mathbb{F}_2$ one has $b^\ell = b$ for every $\ell \geq 1$. The reduction of the integral model modulo 2 is therefore the same polynomial for every ℓ, and the von Staudt–Clausen theorem identifies it.

Theorem 8.1 (2-adic structure)**.** *Let $k \geq 1$ and $n = k+1$.*

(i) $v_2(B_{2m}) = -1$ *for every* $m \geq 1$.

(ii) $v_2\binom{2n}{2j} = v_2\binom{n}{j}$ *for* $0 \leq j \leq n$.

(iii) *For* $0 < j < n$,
$$v_2\left(\frac{c_{k,j}}{c_{k,0}}\right) = v_2\binom{n}{j} - 1.$$

(iv) *Let $B = (b_0, \dots, b_n)$ be integers with $b_0 \neq 0$ satisfying the identities* (5)*. Then for every $0 < j < n$ with $b_j \neq 0$,*
$$v_2(b_j) + 1 = v_2(b_0) + v_2\binom{n}{j}.$$

(v) *For every integer vector B and every $\ell \geq 1$, $W_{B,\ell} \equiv W_{B,1} \pmod 2$, coefficientwise.*

Proof. (i) By the von Staudt–Clausen theorem, $B_{2m} + \sum_{(p-1)\mid 2m} 1/p$ is an integer, the sum running over the primes p with $(p-1) \mid 2m$. The prime 2 always occurs in that sum, and every other prime occurring in it is odd. An integer plus a sum of fractions with odd denominators is a fraction with odd denominator, so $B_{2m} + \frac{1}{2} = a/b$ with b odd, whence $B_{2m} = (2a-b)/(2b)$ with $2a-b$ and b odd, and $v_2(B_{2m}) = -1$.

(ii) For a prime p and $m \geq 0$ one has $v_p\big((pm)!\big) = v_p(m!) + m$ (the multiples of p among $1, \dots, pm$ are $p\cdot 1, \dots, p\cdot m$). Writing $v_2\binom{N}{J} = v_2(N!) - v_2(J!) - v_2((N-J)!)$ at $(N, J) = (2n, 2j)$ and applying the identity at $p = 2$ to each factorial, $v_2\binom{2n}{2j} = \big(v_2(n!)+n\big) - \big(v_2(j!)+j\big) - \big(v_2((n-j)!)+n-j\big) = v_2\binom{n}{j}$. No carry count is needed.

(iii) Since $B_0 = 1$, $c_{k,0} = B_{2n}/(2n)!$, so $c_{k,j}/c_{k,0} = B_{2j}B_{2n-2j}\,(2n)!/\big((2j)!\,(2n-2j)!\,B_{2n}\big)$, and by (i) its valuation is $(-1) + (-1) - (-1) + v_2\binom{2n}{2j} = v_2\binom{2n}{2j} - 1$, which is $v_2\binom{n}{j} - 1$ by (ii).

(iv) By (5), $b_j/b_0 = c_{k,j}/c_{k,0}$; take v_2 and apply (iii).

(v) The coefficient of x^j in $W_{B,\ell}$ is $(-1)^{(\ell+1)j} b_j^\ell$, and in $\mathbb{F}_2$ one has $-1 = 1$ and $b^\ell = b$ for $\ell \geq 1$. □

Part (iii) says that the 2-adic profile of the coefficients of $R_{k,\ell}/c_{k,0}^\ell$ is ℓ times a quantity that does not involve ℓ, and part (iv) transports this to any integral model. The explicit description of the reduction that results is the following; it was proved in version 1 of this paper and is stated here in the same form. Its ingredients (i)–(iii) are now Theorem 8.1; what is *not* machine-checked is the passage from the valuations to the primitive form and to the closed formula for Q_n, and we therefore keep it separate from the verified development.

Theorem 8.2 (explicit form; not machine-checked)**.** *Let $n = k+1$ and let $P_{k,\ell} \in \mathbb{Z}[x]$ be the primitive integral multiple of $R_{k,\ell}$. Then $P_{k,\ell} \equiv Q_n \pmod 2$, where*
$$Q_n = \begin{cases} x^n + x^{n/2} + 1, & n = 2^a,\ a \geq 1, \\ \displaystyle\sum_{\substack{0<j<n \\ j \subseteq n}} x^j = (1+x)^n + 1 + x^n, & \text{otherwise}, \end{cases}$$
and $j \subseteq n$ denotes bitwise containment of binary digits. In particular Q_n does not depend on ℓ.

Proof. By Theorem 8.1(iii) the coefficient of x^j in $R_{k,\ell}/c_{k,0}^\ell$ has 2-adic valuation $\ell\big(v_2\binom{n}{j} - 1\big)$ for $0 < j < n$, and 0 at the two ends $j \in \{0, n\}$, where the ratio is 1. Passing to the primitive form subtracts the minimum of these valuations. If $n = 2^a$ then $\min_{0<j<n} v_2\binom{n}{j} = 1$, attained only at $j = n/2$, so the minimum over all j is 0 and exactly $j \in \{0, n/2, n\}$ survive modulo 2. Otherwise some

$\binom{n}{j}$ with $0 < j < n$ is odd, the minimum is $-\ell$, and exactly the j with $0 < j < n$ and $j \subseteq n$ survive (Lucas: $\binom{n}{j}$ is odd exactly when $j \subseteq n$). Finally $\sum_{j \subseteq n} x^j = \prod_i (1 + x^{2^i}) = (1+x)^n$ over $\mathbb{F}_2$, where i runs over the positions of the 1-digits of n. □

Theorem 8.2 was verified by exact rational arithmetic for all $1 \le k \le 60$, $1 \le \ell \le 8$ (and the intermediate identity of Theorem 8.1(iii) for $k \le 39$ before that identity was proved). In the machine-checked development the reduction of the coprime model $W_{B,1}$ modulo 2 is not taken from Theorem 8.2 but computed outright from the parities of the b_j; the three reductions so obtained, for $n = 3, 27, 45$, are the polynomials $x + x^2$, $\sum_j x^j$ over the fourteen j with $0 < j < 27$ and $j \subseteq 27 = 11011_2$, and the same over the fourteen j with $0 < j < 45$ and $j \subseteq 45 = 101101_2$, exactly as Theorem 8.2 predicts.

9. The 2-adic sieve, and $k \in \{2, 26, 44\}$

If $\Phi_d \mid R_{k,\ell}$ then $\Phi_d \mid W_{B,\ell}$ over $\mathbb{Z}$ (Lemma 3.1), hence $\overline{\Phi_d}$ divides $\overline{W_{B,\ell}} = \overline{W_{B,1}}$ in $\mathbb{F}_2[x]$ (Theorem 8.1(v)), and $\varphi(d) \le n$ (Lemma 5.2). The set of $d \ge 3$ passing both tests depends only on k. Where it is empty, the roots-of-unity question at that k is settled for every ℓ with no computation per ℓ and no certificate per order. Refuting $\overline{\Phi_d} \mid \overline{W_{B,1}}$ is the whole computation, and it is done without ever writing down a cyclotomic polynomial modulo 2.

Polynomials over $\mathbb{F}_2$ are encoded as non-negative integers: for $a \in \mathbb{N}$ let $\beta(a) = \sum_i x^i$, the sum over the positions i of the binary digits 1 of a. Then $\beta(a \oplus b) = \beta(a) + \beta(b)$, where $\oplus$ is bitwise exclusive or, and carry-less multiplication of integers realises the product of polynomials. A certificate is then an identity between integers.

Lemma 9.1 (Bezout certificate)**.** *Let B be an integer vector, $d \ge 1$, $t = \varphi(d) > 0$, and let $q \in \mathbb{N}$ satisfy $\beta(q) = \overline{W_{B,1}}$ in $\mathbb{F}_2[x]$. Suppose that $a, b, g \in \mathbb{N}$ satisfy*

$$\beta(a)\,\beta(q) + \beta(b)\,(x^d - 1) = \beta(g) \quad \text{in } \mathbb{F}_2[x], \qquad g \ne 0, \qquad g < 2^t.$$

Then Φ_d does not divide $W_{B,\ell}$ in $\mathbb{Z}[x]$, for any $\ell \ge 1$.

Proof. Suppose $\Phi_d \mid W_{B,\ell}$ over $\mathbb{Z}$. Reducing modulo 2 and using Theorem 8.1(v), $\overline{\Phi_d} \mid \overline{W_{B,1}} = \beta(q)$. Also $\overline{\Phi_d} \mid x^d - 1$, since $\Phi_d \mid x^d - 1$ over $\mathbb{Z}$. Hence $\overline{\Phi_d}$ divides $\beta(g)$, which is nonzero of degree $< t = \varphi(d)$, while $\overline{\Phi_d}$ is monic of degree $\varphi(d)$. Contradiction. □

In every certificate below $\beta(g)$ was chosen as $\gcd(\overline{W_{B,1}}, x^d - 1)$, and the arithmetic content of the sieve being empty at a given n is that this gcd has degree $< \varphi(d)$ for every admissible $d \ge 3$.

Theorem 9.2. *Let $k \in \{2, 26, 44\}$. For every integer $\ell \ge 1$ and every integer $d \ge 3$, the cyclotomic polynomial Φ_d does not divide $R_{k,\ell}$ in $\mathbb{Q}[x]$.*

Proof sketch, with the finite computations named. Fix k and let B be the coprime integer vector of Section 3: for $k = 2$ it is $B = (2, -7, -7, 2)$; for $k = 26$ it has 28 entries, the first being the 34-digit integer 3206495999837334866355993619396010; for $k = 44$ it has 46 entries of 76 or 77 decimal digits each. All three are palindromes. The hypotheses of Lemma 3.1 are the $k + 2$ identities (5), one exact rational computation with $B_0, \dots, B_{2k+2}$. Suppose $\Phi_d \mid R_{k,\ell}$ with $d \ge 3$, $\ell \ge 1$; then $\Phi_d \mid W_{B,\ell}$ over $\mathbb{Z}$, $\varphi(d) \le n$ and $d \le 2n^2$ (Lemmas 3.1 and 5.2). A sweep of φ over $d \le 2n^2$, i.e. over 18, 1458 and 4050 values of d, shows that d lies in an explicit list: $\{3, 4, 6\}$ for $n = 3$; a list of 51 orders from 3 to 90 for $n = 27$; a list of 86 orders from 3 to 150 for $n = 45$. The reduction $\overline{W_{B,1}}$ is computed from the parities of the b_j (it is $x + x^2$ at $n = 3$, and the fourteen-term polynomials described after Theorem 8.2 at $n = 27, 45$). For each order d in the relevant list we supply a certificate (a, b, g) as in Lemma 9.1; there are $3 + 51 + 86 = 140$ of them, and each is checked as an identity between natural numbers (a carry-less product, an exclusive or, and a comparison with $2^{\varphi(d)}$), together with the value $\varphi(d)$. For $k = 2$ the three certificates read, with $Q_3 = x + x^2 = x(1 + x)$,

$$(1+x)\,Q_3 + (x^3 - 1) = 1 + x, \qquad (1 + x + x^2)\,Q_3 + (x^4 - 1) = 1 + x, \qquad \Big(\sum_{i=0}^{4} x^i\Big) Q_3 + (x^6 - 1) = 1 + x$$

in $\mathbb{F}_2[x]$, and $\deg(1+x) = 1 < 2 = \varphi(d)$ for $d \in \{3,4,6\}$. □

Corollary 9.3. *Let $k \in \{2, 26, 44\}$ and $\ell \geq 1$. If $z \in \mathbb{C}$ satisfies $z^m = 1$ for some $m \geq 1$ and $R_{k,\ell}(z) = 0$, then $z = 1$ or $z = -1$.*

Proof. As for Corollary 6.2, with Theorem 9.2 in place of Theorem 6.1. □

Three remarks. First, all three values of k are even, so by Proposition 2.2 one of ± 1 really is a zero of $R_{k,\ell}$, and the conclusion is sharp. Second, at $\ell = 1$ Theorem 9.2 is again contained in [3, Theorem 6.1], none of $2, 26, 44$ being divisible by 3; for $\ell \geq 2$ we know of no earlier statement. Third, $k = 2$ is the smallest k at which the question has content: for $k = 1$ the polynomial has degree 2, and by [1, Theorem 1.1] its two zeros are the real numbers $\alpha_{1,\ell} > 1$ and $1/\alpha_{1,\ell}$, neither of which is a root of unity.

Remark 9.4 (what the sieve says elsewhere; not machine-checked). Computing the set $\{d \geq 3 : \varphi(d) \leq n,\ \overline{\Phi_d} \mid Q_n\}$ for every $2 \leq n \leq 64$ shows it to be empty exactly at $n = 3, 27, 45$; at every other $n \leq 64$ some order survives and the sieve says nothing. The three values of k in Theorem 9.2 are therefore exactly those this route reaches below $k = 64$. The sieve is necessary and not sufficient: $d = 3$ appears in the admissible set for every $n \equiv 1 \pmod 3$ in the computed range, which is exactly where the Murty–Smyth–Wang factor occurs (Proposition 11.1(ii) exhibits $n = 4$), but also at other n. This consistency with Section 12 is a check on Theorem 8.2.

A refinement modulo 8 — where the reduction depends on ℓ only through its parity, for $\ell \geq 3$, because an odd square is 1 mod 8 while an even b_j has $b_j^\ell \equiv 0 \bmod 8$ — empties the admissible set for all odd $\ell \geq 3$ at $n \in \{2, 3, 4, 7, 8, 15, 16, 21, 27, 29, 31, 32, 37, 39, 41, 43, 45, 51, 57, 59\}$, that is at 20 of the values $2 \leq n \leq 61$ computed. This refinement is not machine-checked: over $\mathbb{Z}/8$ the Bezout argument of Lemma 9.1 is not available, and a certificate would have to be a remainder against an explicit integer form of Φ_d for each admissible d.

10. Rational zeros, and the irrationality of $\alpha_{k,\ell}$

[1] observes that the irreducibility of $R_{k,\ell}$ (for k odd; of $R_{k,\ell}/(z-(-1)^\ell)$ for k even) would entail the irrationality of $\alpha_{k,\ell}$. A much weaker property suffices: since by [1, Theorem 1.1] every zero other than $\alpha_{k,\ell}$ and $1/\alpha_{k,\ell}$ lies on the unit circle, a rational zero outside $\{\pm 1\}$ would have to be $\alpha_{k,\ell}$ or its inverse, so $\alpha_{k,\ell}$ is irrational as soon as $R_{k,\ell}$ has no rational zero besides the predicted ± 1. That is a rational-root statement, and the periodicity of Section 4 reaches it.

Lemma 10.1 (transfer)**.** *Let $P \in \mathbb{Z}[x]$ with $\deg P \leq N$, and let $q = u/v$ with u, v coprime integers, $v \neq 0$, be a zero of P. Then $\sum_{j=0}^{N} P_j u^j v^{N-j} = 0$ in $\mathbb{Z}$, where P_j is the coefficient of x^j. If p is a prime with $p \nmid P_N$, then $p \nmid v$, so $z := \overline{u}\,\overline{v}^{-1} \in \mathbb{F}_p$ is defined and $\overline{P}(z) = 0$ in $\mathbb{F}_p$.*

Proof. Multiply $P(u/v) = 0$ by v^N. Every term with $j < N$ contains the factor v, so if $p \mid v$ then $p \mid P_N u^N$, hence $p \mid u$, contradicting $\gcd(u, v) = 1$. Reducing the integer identity modulo p and dividing by $\overline{v}^N$ gives the last claim. □

Apply this to $P = W_{B,\ell}$, whose coefficient of x^n is $\pm b_n^\ell$; the condition is $p \nmid b_n$, and $b_n = b_0$ by Proposition 2.1. Then $\overline{W_{B,\ell}}(z) = E_{B,p,z}(\ell) = E_{B,p,z}(r)$ with $r = 1 + ((\ell - 1) \bmod (p-1))$, by Lemma 4.1. The derivative of $W_{B,\ell}$ transports in the same way: put

$$E'_{B,p,z}(r) := \sum_{j=1}^{n} j\,(-1)^{(r+1)j}\,\overline{b_j}^{\,r}\,z^{j-1} \in \mathbb{F}_p,$$

so that $\overline{W'_{B,\ell}}(z) = E'_{B,p,z}(\ell) = E'_{B,p,z}(r)$ by the same term-by-term argument as in Lemma 4.1.

Proposition 10.2 (odd step)**.** *Let k, B satisfy the hypotheses of Lemma 3.1, let $\ell \geq 1$, let p be an odd prime with $p \nmid b_n$, and let $r = 1 + ((\ell - 1) \bmod (p-1))$. If $E_{B,p,z}(r) \neq 0$ for every $z \in \mathbb{F}_p$, then $R_{k,\ell}$ has no rational zero.*

Proof. A rational zero of $R_{k,\ell}$ is a zero of $W_{B,\ell}$ (Lemma 3.1), and Lemma 10.1 produces $z \in \mathbb{F}_p$ with $E_{B,p,z}(r) = 0$. □

For k even no such certificate can exist, since Proposition 2.2 puts $\varepsilon := (-1)^\ell$ among the zeros. The statement to prove is then that ε is the only rational zero, and the certificate has two halves: no zero of the reduced model away from $\overline{\varepsilon}$, and $\overline{\varepsilon}$ a *simple* zero. Note that $r \equiv \ell \pmod 2$ because $p-1$ is even, so $\overline{\varepsilon} = (-1)^r$ is determined by r.

Proposition 10.3 (even step)**.** *Let k be even, let k, B, ℓ, p, r be as in Proposition 10.2, and put $\varepsilon_r = (-1)^r \in \mathbb{F}_p$. If $E_{B,p,z}(r) \neq 0$ for every $z \in \mathbb{F}_p$ with $z \neq \varepsilon_r$, and $E'_{B,p,\varepsilon_r}(r) \neq 0$, then every rational zero of $R_{k,\ell}$ is 1 or -1.*

Proof. Let $\varepsilon = (-1)^\ell \in \mathbb{Z}$. By Proposition 2.2 and Lemma 3.1, $W_{B,\ell}(\varepsilon) = 0$, so $W_{B,\ell} = (x-\varepsilon)V$ with $V \in \mathbb{Z}[x]$, $\deg V \leq n-1$, and V has the same leading coefficient as $W_{B,\ell}$. Let $q \in \mathbb{Q}$ be a zero of $R_{k,\ell}$ with $q \neq \varepsilon$; then $V(q) = 0$, and Lemma 10.1 applied to V gives $z \in \mathbb{F}_p$ with $\overline{V}(z) = 0$. If $z \neq \overline{\varepsilon}$ then $\overline{W_{B,\ell}}(z) = (z-\overline{\varepsilon})\overline{V}(z) = 0$, that is $E_{B,p,z}(r) = 0$ with $z \neq \varepsilon_r$, against the first hypothesis. If $z = \overline{\varepsilon}$ then, since $W'_{B,\ell} = V + (x-\varepsilon)V'$, one gets $\overline{W'_{B,\ell}}(\overline{\varepsilon}) = \overline{V}(\overline{\varepsilon}) = 0$, that is $E'_{B,p,\varepsilon_r}(r) = 0$, against the second. Hence $q = \varepsilon$. □

The argument shows $q = (-1)^\ell$; the statement we certify, and the only one we claim, is the weaker $q \in \{1, -1\}$.

A single prime p certifies the residues r for which its hypothesis holds; to cover every $\ell \geq 1$ one may combine several primes. If L is a common multiple of the numbers $p_i - 1$, the residue $r_i(\ell) = 1 + ((\ell-1) \bmod (p_i-1))$ at each prime p_i is a function of $\ell \bmod L$, namely $(\ell-1) \bmod (p_i-1) = \big((\ell \bmod L) + L - 1\big) \bmod (p_i - 1)$. A finite check over the L classes $c \in \{0, \ldots, L-1\}$ that, for each c, some p_i has r_i among its certified residues, therefore covers all ℓ.

Theorem 10.4. *For every integer $\ell \geq 1$:*

(a) *$R_{11,\ell}$ and $R_{13,\ell}$ have no rational zero;*
(b) *if $q \in \mathbb{Q}$ and $R_{8,\ell}(q) = 0$ or $R_{14,\ell}(q) = 0$, then $q = 1$ or $q = -1$.*

Proof sketch, with the finite computations named. The vectors B and the bridge identities are those of Example 3.2 and Theorem 6.1. The certificates are as follows; in each line, a prime is followed in parentheses by the number of residues r at which its hypothesis (Proposition 10.2 for k odd, Proposition 10.3 for k even) is certified, each certified residue costing p evaluations $E_{B,p,z}(r)$, $z \in \mathbb{F}_p$, plus one derivative evaluation when k is even.

k	L	primes (residues certified)
11	12	13 (12)
13	360	11 (7), 13 (8), 19 (4), 37 (3), 41 (2), 61 (1), 73 (1)
8	1380	11 (4), 13 (7), 31 (4), 47 (30), 61 (4), 139 (14), 277 (6), 461 (3), 691 (1), 1381 (1)
14	240	3 (1), 13 (5), 17 (3), 41 (3), 61 (2)

In every case L is the least common multiple of the $p-1$, none of the primes divides $b_n = b_0$, and the covering of the L classes is one finite check. At $k = 11$ the single prime 13 certifies all twelve residues, so no covering is needed: $E_{B,13,z}(r) \neq 0$ for all $z \in \mathbb{F}_{13}$ and all $1 \leq r \leq 12$, that is 156 evaluations. The certified residues at each prime are exactly those the covering uses, not all residues at which the hypothesis happens to hold; the primes and residues were found by a search over small primes, and no minimality is claimed. □

The shape of the coverings is explained by the degeneracy already met in Section 7. At the residue $r = p-1$, when p divides none of the b_j, Fermat makes every $\overline{b_j}^{\,r} = 1$ and $E_{B,p,z}(p-1) = \sum_{j=0}^{n} (-z)^j$, which vanishes at the z for which $-z$ has order $m > 1$ dividing $n+1 = k+2$, and at $z = -1$ if $p \mid k+2$. For k odd, $k+2$ is odd, so such a zero needs $\gcd(k+2, p-1) > 1$ or $p \mid k+2$. For k even, $m = 2$ gives $z = 1 = \varepsilon_{p-1}$, the predicted zero, which is harmless for the first half of Proposition 10.3 and only has to be simple; a further zero exists exactly when $\gcd(k+2, p-1)$ has a divisor ≥ 3 —

when $5 \mid p-1$ at $k=8$, when $4 \mid p-1$ at $k=14$ — or when $p \mid k+2$. A prime dividing some b_j with $0<j<n$ changes the collapsed value. In the coverings the class $\ell \equiv 0 \pmod{L}$, at which every prime is at its residue $p-1$, is served by $p=47$ at $k=8$ (where $5 \nmid 46$, $47 \nmid 10$, and 47 divides no b_j), by $p=11$ and $p=13$ at $k=13$, and by $p=13$ at $k=14$, the last three primes each dividing at least two of the b_j (two, eight and six respectively); at $k=11$ the single prime 13 divides ten of the b_j, and all twelve residues are certified. (These explanations are commentary on the certificates, which are checked outright.)

Theorem 10.5. *For every integer $\ell \geq 1$: every real zero of $R_{11,\ell}$ and of $R_{13,\ell}$ is irrational, and every real zero of $R_{8,\ell}$ and of $R_{14,\ell}$ other than 1 and -1 is irrational.*

Proof. A rational real zero would be a rational zero of the same polynomial, which Theorem 10.4 excludes, or confines to $\{1,-1\}$. □

Corollary 10.6 (not machine-checked; uses [1, Theorem 1.1])**.** *For $k \in \{8,11,13,14\}$ and every $\ell \geq 1$, the real zeros $\alpha_{k,\ell}$ and $1/\alpha_{k,\ell}$ of $R_{k,\ell}$ are irrational.*

Proof. By [1, Theorem 1.1], $\alpha_{k,\ell} > 1$ and $1/\alpha_{k,\ell} \in (0,1)$ are real zeros of $R_{k,\ell}$; neither is ± 1, so Theorem 10.5 applies. □

The identification of the real zeros off the unit circle with $\alpha_{k,\ell}$ and its inverse is the theorem of [1] and is cited, not re-proved; what is machine-checked is Theorem 10.5. For a *fixed* pair (k,ℓ) the content of Theorem 10.4 is a routine rational-root computation, and the census of Section 12 performs it 800 times; the content of the theorem is its uniformity in ℓ, which no finite list of factorisations yields. We also record that the 2-adic information of Theorem 8.1 does not settle rational zeros on its own: at $k=8$ the coefficient valuations $\ell\big(v_2\binom{9}{j}-1\big)+\ell$ of the primitive model are $\ell, 0, 2\ell, 2\ell, \ell, \ell, 2\ell, 2\ell, 0, \ell$ for $j=0,\dots,9$, so the lower convex hull of the Newton polygon has vertices $(0,\ell),(1,0),(8,0),(9,\ell)$ and permits rational zeros of 2-adic valuation ℓ, 0 and $-\ell$; an archimedean or mod-p input is needed, and the certificates above supply it.

11. Controls for the two new layers

Proposition 11.1. (i) *Theorem 8.1(iv) is not vacuous: for $B=(2,-7,-7,2)$ at $k=2$, $j=1$ it asserts $v_2(-7)+1 = v_2(2)+v_2\binom{3}{1}$, and the instance has content — $b_1=-7$ is odd, $b_0=2$ is even and $\binom{3}{1}=3$ is odd, so the "-1" in Theorem 8.1(iii) is doing work.*

(ii) *The sieve of Section 9 is necessary and not sufficient: at $n=4$ ($k=3$) the reduction is $Q_4 = x^4+x^2+1 = (x^2+x+1)^2$ in $\mathbb{F}_2[x]$, so $\overline{\Phi_3}$ divides it — as it must, since $\Phi_3 \mid R_{3,1}$ (Proposition 7.1(iv)). In bitmask form, $111_2 \cdot 111_2 = 10101_2$.*

(iii) *The hypothesis $\ell \geq 1$ in Theorem 8.1(v) is needed: for $B=(2,-7,-7,2)$ the reduction of $W_{B,0}$ is $1+x+x^2+x^3$, not $Q_3 = x+x^2$.*

(iv) *"No rational zero" is false for k even: $R_{8,2}(1)=0$. This is why Theorem 10.4(b) reads $q=\pm 1$ and why Proposition 10.3 has to deflate.*

(v) *Theorem 10.5 is not about the empty set: with B the vector of Example 3.2 for $k=11$, $W_{B,1}(4) = -163091222790 < 0$ and $W_{B,1}(5) = 407085510363880330 > 0$, so $R_{11,1}$ has a real zero in $(4,5)$.*

Proof. (i) is Theorem 8.1(iv) applied to the $k=2$ model, whose bridge identities are one exact rational computation, followed by three parity checks. (ii) and (iii) are identities in $\mathbb{F}_2[x]$, checked as identities between bitmasks. (iv) is Proposition 2.2 at $(k,\ell)=(8,2)$. (v) is two integer evaluations; the formal statement records the two signs, the values are ours. □

By [1, Theorem 1.1] the zero in (v) is $\alpha_{11,1}$, the only real zero of $R_{11,1}$ greater than 1. Bisection on $W_{B,1}$ in exact rational arithmetic gives $\alpha_{11,1} = 4.0000044448387487\ldots$. We record one consequence of this value. [1, Theorem 1.2], for ℓ odd and $k \geq 3$, places $\alpha_{k,\ell}$ in the interval $\big((2\zeta(2)\zeta(2k)/\zeta(2k+2))^\ell,\ (2\zeta(2))^\ell \tfrac{2}{\zeta(2)}(1+3d_\ell/4^k)\big)$ with $d_\ell = ((1.75)^\ell - 1)/0.75$, as we read it in the compiled v1 e-print;

at $k = 11$, $\ell = 1$ the interval is $(2\zeta(2)\zeta(22)/\zeta(24),\ 4(1 + 3 \cdot 4^{-11})) \approx (3.28987,\ 4.0000029)$. The lower bound holds, but $W_{B,1}(4 + 12 \cdot 4^{-11}) < 0 < W_{B,1}(5)$ — two integer evaluations — so $\alpha_{11,1}$ lies *above* the upper bound. The same two-evaluation check at $\ell = 1$ gives $\alpha_{k,1} > 4(1 + 3 \cdot 4^{-k})$ for each $7 \le k \le 14$, and $\alpha_{k,1} < 4(1 + 3 \cdot 4^{-(k-1)})$ for $3 \le k \le 14$. Nothing in this paper depends on Theorem 1.2; we report the computation and do not pursue it. (The evaluations in this paragraph are ours and are not machine-checked.)

12. A factorisation census, outside the machine-checked development

Factoring the primitive integral multiple of $R_{k,\ell}$ over $\mathbb{Q}$ for all 800 pairs with $1 \le k \le 80$ and $1 \le \ell \le 10$ (PARI/GP [12], using `bernfrac` and `factor`; 13.0 CPU-seconds in total) gives exactly the pattern predicted in [1] — one irreducible factor of degree $k+1$ when k is odd, and $(z - (-1)^\ell)$ times one irreducible factor of degree k when k is even — with exactly 26 exceptions. Every exception has $\ell = 1$ and $3 \mid k$, that is $k \in \{3, 6, \dots, 78\}$; these are precisely the Murty–Smyth–Wang factor Φ_3 [3, Theorem 6.1]. So the census confirms rather than extends the $\ell = 1$ theory; its content is that the "preliminary computations" cited in [1] for $\ell > 1$ continue to hold two orders of magnitude further in k. This computation is not part of the machine-checked development.

13. What is not settled

Three limitations are worth stating precisely.

The irreducibility question of [1] *is untouched.* Nothing above bears on whether $R_{k,\ell}$ is irreducible for k odd, or $R_{k,\ell}/(z - (-1)^\ell)$ for k even; Theorem 10.4 excludes linear factors over $\mathbb{Q}$ beyond the predicted one, and nothing more. A certificate route would need an irreducibility test over $\mathbb{F}_p$ of Rabin type — $x^{p^m} \equiv x \bmod f$ together with $\gcd(x^{p^i} - x, f) = 1$ for the relevant i — developed to the same standard as Lemma 4.2; and, unlike the cyclotomic question, irreducibility mod p is a sufficient but not necessary condition, so a failure at one prime certifies nothing. The concluding remarks of [1] also observe that, granted irreducibility, $\alpha_{k,\ell}$ for $k \ge 4$ would have the configuration of Galois conjugates of a Salem number while being an algebraic number rather than an algebraic integer; Corollary 10.6 is far short of that.

The values of k. Theorem 6.1 is proved at $k = 8, 11, 13, 14$, Theorem 9.2 at $k = 2, 26, 44$, and Theorem 10.4 at $k = 8, 11, 13, 14$, and nowhere else. The obstruction to Theorem 6.1 at other small k is described after Proposition 7.1; the 2-adic sieve is empty at no other $n \le 64$ (Remark 9.4), and whether it is empty at any larger n is a question of computation we have not pursued; extending Theorem 10.4 to a further k costs a search for primes and a covering, which is not guaranteed to succeed. None of this produces a statement uniform in k, and no argument here suggests one.

What is not machine-checked. Theorem 8.2 in its explicit form, the sieve computation of Remark 9.4, the mod-8 refinement, the census, the search statistics after Proposition 7.1, the value of $\alpha_{11,1}$ and the comparison with [1, Theorem 1.2] after Proposition 11.1, and Corollary 10.6 (which rests on [1, Theorem 1.1]) are stated on the authority of the computations and citations named, not of the formal development.

14. Verification

Every statement of Sections 2–7 and 8–11 other than Theorem 8.2, Remark 9.4, the mod-8 paragraph and Corollary 10.6 — Propositions 2.1, 2.2, 5.1, 7.1, 10.2, 10.3 and 11.1, Lemmas 3.1, 4.1, 4.2, 5.2, 9.1 and 10.1, Theorems 6.1, 8.1, 9.2, 10.4 and 10.5, and Corollaries 6.2 and 9.3 — has been machine-checked in Lean 4 [10] against Mathlib [11], with no `sorry` anywhere. Appendix A lists, verbatim, the formal statement of each of the 53 declarations that carry the numbered results; the supporting Lemmas 3.1, 4.1, 4.2, 5.2 and 10.1 and Propositions 10.2 and 10.3 are proved in the same modules but are not listed there. The axiom closure of every declaration concerned was printed and is as stated here. The reasoning layer is kernel-clean in the ordinary sense (its axiom closure is exactly propositional extensionality, quotient soundness and choice): this includes Propositions 2.1, 2.2 and 5.1, all of Sections 3–5, all five parts of Theorem 8.1, Lemmas 9.1 and 10.1, Propositions 10.2 and 10.3,

and items (ii)–(v) of Proposition 11.1 (item (ii), and the parity checks of item (i), need propositional extensionality only). The finite computations are discharged by compiled evaluation (`native_decide`), each occurrence contributing one further axiom. For Theorem 6.1 and Corollary 6.2 there are 19 of these for $k = 8$ and 27 for each of $k = 11, 13, 14$: the 16 or 24 certificates, the $k+2$ bridge identities (5) as a single check, the non-vanishing of $c_{k,0}$, and the sweep of φ over $d \le 2(k+1)^2$. For Theorem 9.2 and Corollary 9.3 there are exactly 2 for each of $k = 2, 26, 44$: the bridge identities and the totient sweep; the 140 Bezout certificates of Lemma 9.1 and the 140 values of φ they use are checked by the kernel's own evaluation (`decide`) on natural numbers and contribute no axiom. For Theorems 10.4 and 10.5 there are 2 for $k = 11$ (the bridge identities and the certificate at $p = 13$), 8 for $k = 13$, 11 for $k = 8$ and 6 for $k = 14$ (the bridge identities and one certificate per prime); the coverings of the L classes are kernel `decide`s. The computational items of Proposition 7.1 rest on one such evaluation each, except item (iii), which is a deduction from Proposition 2.2; item (i) of Proposition 11.1 rests on one (the $k = 2$ bridge identities), and items (ii)–(v) on none. Each compiled evaluation is a genuinely finite one: a sum over $p - 1$ residues or over p points in $\mathbb{F}_p$ with $p \le 1381$, a rational identity over $k + 2$ indices, or a totient sweep over $d \le 2(k+1)^2$. Because Mathlib's Bernoulli numbers are defined by an unmemoised recursion and cannot be evaluated directly, the development also contains a computable list of Bernoulli numbers proved equal to them, which is what the finite checks run on. Theorem 8.2, Remark 9.4, the mod-8 refinement, the census of Section 12, the search statistics reported after Proposition 7.1, the evaluations reported after Proposition 11.1 and Corollary 10.6 are *not* machine-checked. Repository reference to be added at submission.

Provenance of the novelty claims

We state what was searched, since the claims of Theorems 6.1, 9.2 and 10.4 are claims about the literature as well as about polynomials. All of it was done on 3 September 2026, and the online channels were re-queried on that date after the paper was drafted. The arXiv record of [1] carries a single version, v1 of 16 July 2025; the paper has since appeared in the *Proceedings of the American Mathematical Society*. Both of its OpenAlex records — the preprint and the published article — have a citation count of 0, and the OpenAlex query for works citing either returns nothing; the Semantic Scholar citation listing, queried both by arXiv identifier and by DOI, is likewise empty in each case. Of the two OpenAlex records for the paper [2] that poses the underlying conjecture, one has no citations at all and the other has exactly one citer, namely [1]; the LaTeX source of [2] contains no occurrence of "irreducib" and none of "roots of unity". Three conjunction queries against the arXiv API — `"Ramanujan polynomial"` together with each of `cyclotomic`, `"roots of unity"` and `irreducible` — return no hits at all, against 18 items ever matching `"Ramanujan polynomial"` and 4 for the positive control `"Ramanujan polynomial"` with `Bernoulli`. A full-text scan of a local mirror of the arXiv (mathematics and computer science, through August 2026; quantum physics is not mirrored) for papers matching "Ramanujan polynomial" together with "irreducib", or with "roots of unity" and "cyclotomic", returned 13 papers, one of which is [1] itself; the titles of the other twelve were all read and none concerns the polynomials (1). Searches of the OEIS for the relevant phrases return nothing bearing on them. A zbMATH free-text search for the same phrase pairs was run and its leading hits read; the only one about cyclotomic factors of a family of polynomials attached to modular forms is Heim, Luca and Neuhauser, *On cyclotomic factors of polynomials related to modular forms*, Ramanujan J. **48** (2019), 445–458, whose family is the one defined by $\prod_{m\ge1}(1-q^m)^{-z} = \sum_{n\ge0} P_n(z)q^n$ and not (1).

For the two claims new in this version the search was widened in two directions. On the 2-adic side, the texts of [3], [5], [4], [6], [7] (whose Section 3.5 concerns Ramanujan polynomials), [2] and [1] were converted to text and searched for the strings "p-adic", "2-adic", "Staudt", "Newton polygon", "Eisenstein criterion" and "divisib": every count is zero. The nearest published method we found is [8], which combines the von Staudt–Clausen theorem with Dumas's criterion on the 2-adic Newton polygon to prove irreducibility — but for Faber polynomials of Eisenstein series, and that paper contains no occurrence of "Ramanujan polynomial" and none of "cyclotom". On the irrationality side,

we found no paper that proves the irrationality or transcendence of the real zero of a Ramanujan polynomial, and none that proves the irreducibility of R_{2k+1} for any k, even at $\ell = 1$: [3] contains no occurrence of "irreducib" and none of "irrational"; the Ramanujan-polynomial section of [7] has no irreducibility content; and [4] say of the analogous irrationality question for $\zeta(3)/\pi^3$ that "such a theorem is well beyond the scope of this paper". A second conjunction scan of the local mirror, for "Ramanujan polynomial" together with "irrational" or "irreducib" or with one of "2-adic", "two-adic", "Staudt", "Kummer", "mod 2", "modulo 2", returned 32 papers, whose titles were all read; none concerns (1) (they are about Ramanujan class polynomials and class invariants, q-trinomial identities, identities for zeta values, combinatorial Ramanujan polynomials counting labelled trees, Ramanujan cubics, the papers already named above, and the two source papers themselves). One item is recorded as not read: [9], located through a citation listing of [3]. Its text was not obtained (the publisher's page is not served to us); what was obtained is its zbMATH record — subject classes 11A25, 11L03, 12D10, 30C10, 30C15, and a reference list on gcd-sum functions and the Fourier transform of the greatest common divisor, together with [3] and [5] — and its dates: it appeared online in July 2014, nine years before [2] introduced $R_{k,\ell}$. Its family, polynomials with gcd powers as coefficients in the words of its title, is therefore not (1), and it cannot concern $R_{k,\ell}$ for $\ell \geq 2$; whether it says anything about the Ramanujan polynomial itself beyond citing [3] we cannot say. What was *not* searched: MathSciNet, Google Scholar, Semantic Scholar's free-text search endpoint (its citation endpoint is what was queried above), theses and MathOverflow. The paper [3] is not on the arXiv and was found by web search and read from the second author's homepage; the $\ell = 1$ case is theirs and is credited as such throughout. The published text of [1] is behind a paywall and was not obtained, so the passages quoted from it are certified against the arXiv v1 e-print only.

References

[1] Mrityunjoy Charan, Jaban Meher and Siddhi Pathak, *Variant of Ramanujan polynomials and a conjecture of Maji & Sarkar*, Proc. Amer. Math. Soc. **154** (2026), no. 1, 283–298; DOI 10.1090/proc/17438 (published electronically 4 December 2025). Preprint: arXiv:2507.12080v1 [math.NT], submitted 16 July 2025, the only version on the arXiv. All numbered references above — Conjecture 1.1 (the definition of $R_{k,\ell}$), Theorem 1.1, Theorem 1.2, Proposition 3.1 and the concluding remarks — are to the compiled v1 e-print, which is what we read; the journal version is behind a paywall and its numbering was not checked against it.

[2] Bibekananda Maji and Tithi Sarkar, *Zeros of Ramanujan-type Polynomials*, arXiv:2306.10283v1 [math.NT], submitted 17 June 2023, the only version. The source of the conjecture settled in [1].

[3] M. Ram Murty, Chris Smyth and Rob J. Wang, *Zeros of Ramanujan polynomials*, J. Ramanujan Math. Soc. **26** (2011), no. 1, 107–125. Theorem 6.1 and Proposition 6.2 are cited above; both were read from the second author's copy at `webhomes.maths.ed.ac.uk/~chris/papers/msw10.pdf`. Theorem 6.1 is stated there for $M_{2k+1} = ((2k+2)!/B_{2k+2})\,R_{2k+1}$, "the monic companion of $R_{2k+1}(z)$" in their words, and then restated for R_{2k+1} itself: "the only cyclotomic factors of R_{2k+1} are z^2+1 when k is even, and $(z^2+z+1)(z^2-z+1)$ when k is a multiple of 3". The two forms say the same thing, the scalar being nonzero, and it is the second that we use.

[4] Matilde Lalín and Mathew Rogers, *Variations of the Ramanujan polynomials and remarks on* $\zeta(2j+1)/\pi^{2j+1}$, arXiv:1106.1189v1.

[5] Matilde N. Lalín and Chris J. Smyth, *Unimodularity of zeros of self-inversive polynomials*, Acta Math. Hungar. **138** (2013), no. 1–2, 85–101; DOI 10.1007/s10474-012-0225-4. Preprint: arXiv:1201.0774v1, the text searched above.

[6] Matthew C. Lettington, *A trio of Bernoulli relations, their implications for the Ramanujan polynomials and the zeta constants*, arXiv:1203.1753v2, the text searched above; published, under the title *A trio of Bernoulli relations, their implications for the Ramanujan polynomials and the special values of the Riemann zeta function*, in Acta Arith. **158** (2013), no. 1, 1–31; DOI 10.4064/aa158-1-1.

[7] Atul Dixit, *Recent developments pertaining to Ramanujan's formula for odd zeta values*, Expo. Math. **42** (2024), no. 5, 125602; DOI 10.1016/j.exmath.2024.125602. Preprint: arXiv:2312.15501v1 (December 2023), the text searched above; its Section 3.5, *Ramanujan polynomials and their cousins*, is the section cited.

[8] Liubomir Chiriac and Andrei Jorza, *Lacunary recurrences and 2-adic properties of Eisenstein series*, preprint (2026), arXiv:2605.09738v2; title and authors verified against the arXiv record.

[9] Karl Dilcher and Sinai Robins, *Zeros and irreducibility of polynomials with gcd powers as coefficients*, Ramanujan J. **36** (2015), no. 1–2, 227–236; DOI 10.1007/s11139-014-9579-2 (published online 29 July 2014, in print February 2015; volume, issue, pages and dates from Crossref, matched by zbMATH 1308.12001). Text not obtained; see the provenance paragraph.

[10] 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.

[11] 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.
[12] The PARI Group, *PARI/GP*, version 2.13.3, Univ. Bordeaux, 2021 (stable release announced 25 October 2021), `https://pari.math.u-bordeaux.fr/`. Used for the factorisation census of Section 12.

Appendix A. The formal statements

The following are the statements, verbatim from the source files of the development, of every machine-checked result of this paper, grouped by the result of the text they establish. Notation of the development: `cbase k j` is $c_{k,j}$; `rcoef k l j` is $a_{k,\ell,j}$; `Rkl k l` is $R_{k,\ell} \in \mathbb{Q}[x]$; `Wp B l` is $W_{B,\ell} \in \mathbb{Z}[x]$ for an integer list `B`, whose j-th entry is `B.getD j 0`; `B2`, `B8`, `B11`, `B13`, `B14`, `B26`, `B44` are the coprime vectors of Sections 3 and 9; `wEval B p z r` is $E_{B,p,z}(r)$ and `wEvalD` its derivative version E'; `bp a` is $\beta(a)$, `clm f a b` the carry-less product (with a fuel parameter `f` bounding the bit length), and `^^^` bitwise exclusive or; `cyclotomic d K` is Φ_d over K; `padicValRat 2`, `padicValInt 2`, `padicValNat 2` are v_2; `Nat.totient` is φ; `ZMod p` is $\mathbb{F}_p$ for p prime, and `Int.castRingHom (ZMod 2)` reduction modulo 2; `aeval z P` is $P(z)$; `IsPrimitiveRoot z d` says that z has exact order d; `bernoulli` is Mathlib's Bernoulli number. In every statement `l` is ℓ and `Finset.range (k + 2)` is $\{0, \dots, k+1\}$.

Proposition 2.1 (reciprocity). Module `Defs.lean`.

```
theorem cbase_symm {k j : ℕ} (hj : j ≤ k + 1) : cbase k (k + 1 - j) = cbase k j

theorem rcoef_symm {k l j : ℕ} (hj : j ≤ k + 1) :
    rcoef k l (k + 1 - j) = (-1) ^ ((l + 1) * (k + 1)) * rcoef k l j
```

Proposition 2.2 (the zeros at ± 1). Module `Defs.lean`.

```
theorem Rkl_eval_one_eq_zero (k l : ℕ) (hk : Even k) (hl : Even l) : (Rkl k l).eval 1 = 0

theorem Rkl_eval_neg_one_eq_zero (k l : ℕ) (hk : Even k) (hl : Odd l) :
    (Rkl k l).eval (-1) = 0
```

Proposition 5.1 (totient bound). Module `Totient.lean`.

```
theorem nat_le_two_mul_totient_sq (n : ℕ) : n ≤ 2 * (Nat.totient n) ^ 2

theorem le_of_totient_le {d N : ℕ} (h : Nat.totient d ≤ N) : d ≤ 2 * N ^ 2
```

Theorem 6.1 ($k \in \{8, 11, 13, 14\}$, no cyclotomic factor). Modules `K11.lean`, `K13.lean`, `K14.lean`, `K8.lean`.

```
theorem k8_no_cyclotomic_factor {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) :
    ¬ (cyclotomic d ℚ ∣ Rkl 8 l)

theorem k11_no_cyclotomic_factor {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) :
    ¬ (cyclotomic d ℚ ∣ Rkl 11 l)

theorem k13_no_cyclotomic_factor {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) :
    ¬ (cyclotomic d ℚ ∣ Rkl 13 l)

theorem k14_no_cyclotomic_factor {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) :
    ¬ (cyclotomic d ℚ ∣ Rkl 14 l)
```

Corollary 6.2 (roots of unity, $k \in \{8, 11, 13, 14\}$). Modules `K11.lean`, `K13.lean`, `K14.lean`, `K8.lean`.

```
theorem k8_not_root_of_primitiveRoot {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) (z : ℂ)
    (hz : IsPrimitiveRoot z d) : aeval z (Rkl 8 l) ≠ 0

theorem k8_root_of_unity_zero {l : ℕ} (hl : 1 ≤ l) (z : ℂ) {n : ℕ} (hn : 0 < n)
    (hzn : z ^ n = 1) (hroot : aeval z (Rkl 8 l) = 0) : z = 1 ∨ z = -1

theorem k11_not_root_of_primitiveRoot {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) (z : ℂ)
    (hz : IsPrimitiveRoot z d) : aeval z (Rkl 11 l) ≠ 0

theorem k11_root_of_unity_zero {l : ℕ} (hl : 1 ≤ l) (z : ℂ) {n : ℕ} (hn : 0 < n)
```

```
    (hzn : z ^ n = 1) (hroot : aeval z (Rkl 11 l) = 0) : z = 1 ∨ z = -1

theorem k13_not_root_of_primitiveRoot {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) (z : ℂ)
    (hz : IsPrimitiveRoot z d) : aeval z (Rkl 13 l) ≠ 0

theorem k13_root_of_unity_zero {l : ℕ} (hl : 1 ≤ l) (z : ℂ) {n : ℕ} (hn : 0 < n)
    (hzn : z ^ n = 1) (hroot : aeval z (Rkl 13 l) = 0) : z = 1 ∨ z = -1

theorem k14_not_root_of_primitiveRoot {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) (z : ℂ)
    (hz : IsPrimitiveRoot z d) : aeval z (Rkl 14 l) ≠ 0

theorem k14_root_of_unity_zero {l : ℕ} (hl : 1 ≤ l) (z : ℂ) {n : ℕ} (hn : 0 < n)
    (hzn : z ^ n = 1) (hroot : aeval z (Rkl 14 l) = 0) : z = 1 ∨ z = -1
```

Proposition 7.1 (controls). Module `Controls.lean`.

```
theorem control_k_odd_eval_one : (Rkl 1 1).eval 1 ≠ 0

theorem control_k_odd_eval_neg_one : (Rkl 1 1).eval (-1) ≠ 0

theorem control_l_odd_eval_one : (Rkl 2 1).eval 1 ≠ 0

theorem control_l_even_eval_neg_one : (Rkl 2 2).eval (-1) ≠ 0

theorem control_cyclotomic_one_dvd : cyclotomic 1 ℚ ∣ Rkl 8 2

theorem control_cyclotomic_two_dvd : cyclotomic 2 ℚ ∣ Rkl 8 3

theorem control_cyclotomic_three_dvd_Rkl_3_1 : cyclotomic 3 ℚ ∣ Rkl 3 1

theorem control_Rkl_8_natDegree (l : ℕ) : (Rkl 8 l).natDegree = 9

theorem control_Rkl_8_ne_zero (l : ℕ) : Rkl 8 l ≠ 0
```

Theorem 8.1 (the two-adic structure theorem). Module `TheoremA.lean`.

```
theorem padicValRat_two_bernoulli {m : ℕ} (hm : 1 ≤ m) :
    padicValRat 2 (_root_.bernoulli (2 * m)) = -1

theorem padicValNat_choose_two_mul {n j : ℕ} (hj : j ≤ n) :
    padicValNat 2 ((2 * n).choose (2 * j)) = padicValNat 2 (n.choose j)

theorem cbase_ratio_padicValRat {k j : ℕ} (h0 : 0 < j) (hj : j < k + 1) :
    padicValRat 2 (cbase k j / cbase k 0)
      = (padicValNat 2 ((k + 1).choose j) : ℤ) - 1

theorem model_two_adic {k j : ℕ} {B : List ℤ} (h0 : B.getD 0 0 ≠ 0) (hbj : B.getD j 0 ≠ 0)
    (hbr : ∀ i ∈ Finset.range (k + 2),
      cbase k i * ((B.getD 0 0 : ℤ) : ℚ) = cbase k 0 * ((B.getD i 0 : ℤ) : ℚ))
    (hj0 : 0 < j) (hjn : j < k + 1) :
    (padicValInt 2 (B.getD j 0) : ℤ) + 1
      = (padicValInt 2 (B.getD 0 0) : ℤ) + (padicValNat 2 ((k + 1).choose j) : ℤ)

theorem Wp_map_two_eq (B : List ℤ) {l : ℕ} (hl : 1 ≤ l) :
    (Wp B l).map (Int.castRingHom (ZMod 2)) = (Wp B 1).map (Int.castRingHom (ZMod 2))
```

Lemma 9.1, Theorem 9.2 and Corollary 9.3 ($k \in \{2, 26, 44\}$). Module `TheoremA.lean`.

```
theorem not_cyclotomic_dvd_of_two_adic_cert {B : List ℤ} {d q : ℕ} (f a b g t : ℕ)
    (hd : 0 < d) (ht : d.totient = t) (htp : 0 < t)
    (hq : (Wp B 1).map (Int.castRingHom (ZMod 2)) = bp q)
    (ha : a < 2 ^ f) (hb : b < 2 ^ f)
    (hbez : (clm f a q) ^^^ (clm f b (2 ^ d ^^^ 1)) = g)
    (hg : g ≠ 0) (hgt : g < 2 ^ t)
    {l : ℕ} (hl : 1 ≤ l) : ¬ (cyclotomic d ℤ ∣ Wp B l)
```

```
theorem k2_no_cyclotomic_factor {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) :
    ¬ (cyclotomic d ℚ ∣ Rkl 2 l)

theorem k2_root_of_unity_zero {l : ℕ} (hl : 1 ≤ l) (z : ℂ) {m : ℕ} (hm : 0 < m)
    (hzm : z ^ m = 1) (hroot : aeval z (Rkl 2 l) = 0) : z = 1 ∨ z = -1

theorem k26_no_cyclotomic_factor {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) :
    ¬ (cyclotomic d ℚ ∣ Rkl 26 l)

theorem k26_root_of_unity_zero {l : ℕ} (hl : 1 ≤ l) (z : ℂ) {m : ℕ} (hm : 0 < m)
    (hzm : z ^ m = 1) (hroot : aeval z (Rkl 26 l) = 0) : z = 1 ∨ z = -1

theorem k44_no_cyclotomic_factor {l d : ℕ} (hl : 1 ≤ l) (hd : 3 ≤ d) :
    ¬ (cyclotomic d ℚ ∣ Rkl 44 l)

theorem k44_root_of_unity_zero {l : ℕ} (hl : 1 ≤ l) (z : ℂ) {m : ℕ} (hm : 0 < m)
    (hzm : z ^ m = 1) (hroot : aeval z (Rkl 44 l) = 0) : z = 1 ∨ z = -1
```

Theorems 10.4 and 10.5 (rational zeros; irrationality). Module `Irrational.lean`.

```
theorem k11_no_rational_zero {l : ℕ} (hl : 1 ≤ l) (q : ℚ) : (Rkl 11 l).eval q ≠ 0

theorem k11_irrational {l : ℕ} (hl : 1 ≤ l) (x : ℝ)
    (hx : Polynomial.aeval x (Rkl 11 l) = 0) : Irrational x

theorem k13_no_rational_zero {l : ℕ} (hl : 1 ≤ l) (q : ℚ) : (Rkl 13 l).eval q ≠ 0

theorem k13_irrational {l : ℕ} (hl : 1 ≤ l) (x : ℝ)
    (hx : Polynomial.aeval x (Rkl 13 l) = 0) : Irrational x

theorem k8_rational_zero_eq {l : ℕ} (hl : 1 ≤ l) (q : ℚ) (hq : (Rkl 8 l).eval q = 0) :
    q = 1 ∨ q = -1

theorem k8_irrational {l : ℕ} (hl : 1 ≤ l) (x : ℝ)
    (hx : Polynomial.aeval x (Rkl 8 l) = 0) (h1 : x ≠ 1) (h2 : x ≠ -1) :
    Irrational x

theorem k14_rational_zero_eq {l : ℕ} (hl : 1 ≤ l) (q : ℚ) (hq : (Rkl 14 l).eval q = 0) :
    q = 1 ∨ q = -1

theorem k14_irrational {l : ℕ} (hl : 1 ≤ l) (x : ℝ)
    (hx : Polynomial.aeval x (Rkl 14 l) = 0) (h1 : x ≠ 1) (h2 : x ≠ -1) :
    Irrational x
```

Proposition 11.1 (controls for the new layers). Modules `Irrational.lean`, `TheoremA.lean`.

```
theorem control_model_two_adic_k2 :
    (padicValInt 2 ((B2).getD 1 0) : ℤ) + 1
      = (padicValInt 2 ((B2).getD 0 0) : ℤ) + (padicValNat 2 ((2 + 1).choose 1) : ℤ)

theorem control_B2_parities :
    (B2).getD 1 0 % 2 = 1 ∧ (B2).getD 0 0 % 2 = 0 ∧ (2 + 1).choose 1 % 2 = 1

theorem control_sieve_not_sufficient : clm 8 7 7 = 21

theorem control_l_zero_differs : (Wp (B2) 0).map (Int.castRingHom (ZMod 2)) = bp 15

theorem control_even_k_has_rational_zero : (Rkl 8 2).eval 1 = 0

theorem control_sign_change :
    (Wp (B11) 1).eval 4 < 0 ∧ 0 < (Wp (B11) 1).eval 5
```