Mathematisches
Forschungsinstitut
Oberwolfach

Member of Leibniz Association

Oberwolfach Preprints

Number 2024-12

Christian Krattenthaler
Thomas W. Müller

The Congruence Properties of Romik's Sequence of Taylor Coefficients of Jacobi's Theta Function θ_3

November 2024

Oberwolfach Preprints (OWP)

The MFO publishes the Oberwolfach Preprints (OWP) as a series which mainly contains research results related to a longer stay in Oberwolfach, as a documentation of the research work done at the MFO. In particular, this concerns the Oberwolfach Research Fellows program (and the former Research in Pairs program) and the Oberwolfach Leibniz Fellows (OWLF), but this can also include an Oberwolfach Lecture, for example.

All information about the publication process can be found at
https://www.mfo.de/scientific-programme/publications/owp

All published Oberwolfach Preprints can be found at https://publications.mfo.de

ISSN 1864-7596

Mathematisches Forschungsinstitut Oberwolfach gGmbH (MFO)
Schwarzwaldstrasse 9-11
77709 Oberwolfach-Walke
Germany
https://www.mfo.de

DOI 10.14760/OWP-2024-12

THE CONGRUENCE PROPERTIES OF ROMIK'S SEQUENCE OF TAYLOR COEFFICIENTS OF JACOBI'S THETA FUNCTION θ_3

C. KRATTENTHALER† AND T. W. MÜLLER

ABSTRACT. In [*Ramanujan J.* **52** (2020), 275–290], Romik considered the Taylor expansion of Jacobi's theta function $\theta_3(q)$ at $q = e^{-\pi}$ and encoded it in an integer sequence $(d(n))_{n\ge0}$ for which he provided a recursive procedure to compute the terms of the sequence. He observed intriguing behaviour of $d(n)$ modulo primes and prime powers. Here we prove (1) that $d(n)$ eventually vanishes modulo any prime power p^e with $p \equiv 3 \pmod 4$, (2) that $d(n)$ is eventually periodic modulo any prime power p^e with $p \equiv 1 \pmod 4$, and (3) that $d(n)$ is purely periodic modulo any 2-power 2^e. Our results also provide more detailed information on period length, respectively from when on the sequence vanishes or becomes periodic. The corresponding bounds may not be optimal though, as computer data suggest. Our approach shows that the above congruence properties hold at a much finer, polynomial level.

1. Introduction

The focus of this article is on Jacobi's theta function θ_3 defined by (cf. [14, top of p. 464 with $z = 0$])

$$\theta_3(\tau) = \sum_{n=-\infty}^{\infty} q^{n^2}, \quad \text{with } q = e^{i\pi\tau}.$$

In [10], Romik considered the Taylor expansion of $\theta_3(\tau)$ at $\tau = i$ in the form (cf. [10, display below Eq. (8)])

$$\theta_3\left(i\frac{1+z}{1-z}\right) = \theta_3(i)(1-z)^{1/2} \sum_{n=0}^{\infty} \frac{d(n)}{(2n)!} \Phi^n z^{2n}, \tag{1.1}$$

where $\Phi = \Gamma^8(1/4)/(128\pi^4)$ and, as is well-known (cf. [3, p. 325, Entry 1(i)]), $\theta_3(i) = \pi^{1/4}/\Gamma(3/4)$. He showed that the sequence $\big(d(n)\big)_{n\ge0}$ is an integer sequence, and he provided a highly non-trivial recursive procedure for computing the coefficients $d(n)$ (see Section 2). The first few values turn out to be

$$1, 1, -1, 51, 849, -26199, 1341999, 82018251, 18703396449,$$
$$-993278479599, -78795859032801, 38711746282537251, -923351332174412751, \dots$$

The signs of these numbers seem very irregular. (In fact, Problem 5 in Section 8 of [10] asks for figuring out the pattern of signs. So far, there has been no progress on that question.) However, computer experiments led Romik [10, Conj. 13] to conjecture that

2020 *Mathematics Subject Classification.* Primary 11F37; Secondary 11B83 14K25.

Key words and phrases. Modular forms of half integer weight, Jacobi theta function, Taylor coefficients, congruences.

†Research partially supported by the Austrian Science Foundation FWF, grant S50-N15, in the framework of the Special Research Program "Algorithmic and Enumerative Combinatorics".

$\big(d(n)\big)_{n\ge0}$ is (eventually) periodic when taken modulo a prime p with $p \equiv 1 \pmod 4$, and that the sequence eventually vanishes when taken modulo a prime p with $p \equiv 3 \pmod 4$. More computer experiments suggest (cf. also [13, Conjecture 18(3)]) that analogous assertions hold modulo *any* prime *power* (including powers of 2). To be more precise, such experiments suggest that:

(1) $d(n)$ eventually vanishes modulo any prime power p^e with $p \equiv 3 \pmod 4$;
(2) $d(n)$ is eventually periodic modulo any prime power p^e with $p \equiv 1 \pmod 4$;
(3) $d(n)$ is purely periodic modulo any 2-power 2^e.

Item (1) was proved for primes (i.e., for $e = 1$) by Scherer [11]. He also obtained partial results on Items (2) and (3) by proving that $d(n) \equiv (-1)^{n+1} \pmod 5$ for $n \ge 1$, and that $d(n)$ is odd for all n. Guerzhoy, Mertens and Rolen [4] claim to have proved Item (2) in full, as a special case of a more general result for a whole family of modular forms of half integer weight.[1] In [13], Wakhare revisited Item (2) for primes (i.e., for $e = 1$). He showed that $d(n)$ is (eventually) periodic modulo any prime number p with

---

[1]The authors of the present article admit that they are not able to comprehend what the result(s) in [4] say about Romik's sequence $\big(d(n)\big)_{n\ge0}$. The first problem is that $\tilde\Omega$ in Theorem 1.3 of [4] is nowhere defined. One may guess that $\tilde\Omega^2 = \omega$, with the ω in the proof of Theorem 1.3 on pages 148/149 of [4]. We assume this guess in the following.

In the Remark on top of page 150 of [4], Romik's sequence is addressed explicitly. There, ω is computed as $\Gamma^2(1/4)/(8\pi)^{1/2}$.

In Theorem 1.3, the coefficients $\partial^n f(\tau_0)$ are considered. If, in the case of $f(\tau) = \Theta(\tau) = \theta_3(2\tau)$, we make the comparison of coefficients in (1-1) and (1-3) of [4], then we obtain the relation

$$(2\pi)^n \partial^n \Theta(i/2) = \Theta(i/2)\Phi^n D(n),$$

where we write $D(n)$ for the Taylor coefficients in Romik's series, that is, $D(2n) = d(n)$ and $D(2n+1) = 0$.

In order to apply Theorem 1.3 to Romik's sequence, we must choose $k = 1$ there. In particular, we should divide the above relation by $\tilde\Omega^{4n+1}$:

$$\frac{(2\pi)^n \partial^n \Theta(i/2)}{\tilde\Omega^{4n+1}} = \frac{\Theta(i/2)\Phi^n D(n)}{\tilde\Omega^{4n+1}}.$$

Now we use the assumption that $\tilde\Omega = \omega^{1/2}$ and the relation $\omega^2 = 2^{1/2}\pi\Phi$ from the Remark on top of page 150 of [4]. We substitute and get, after some cancellation,

$$\frac{(2\pi)^n \partial^n \Theta(i/2)}{\tilde\Omega^{4n+1}} = \frac{D(n)}{2^{n/2-1/4}\pi^{n+1/2}}.$$

Here is the first problem: π does not drop out.

This could be easily fixed: just change the normalisation by that power of π. However, that would create another, equally serious problem. Then the (re)normalised sequence equals Romik's sequence (with 0s for odd indexed coefficients) up to some power of $2^{1/2}$. Then Theorem 1.3, say with $A = 0$, predicts a period length of the (re)normalised sequence, taken modulo p, of $2(p-1)$. (The factor 2 comes from the period length of $2^{1/2}$ modulo p.) Translated to Romik's original sequence $\big(d(n)\big)_{n\ge0}$ (i.e., without 0s), this implies a period length of $p-1$. However, this is definitely wrong. For example, for $p = 13$, Romik's sequence, taken modulo 13, begins

$$1, 1, 12, 12, 4, 9, 9, 3, 10, 10, 12, 1, 1, 9, 4, 4, 10, 3, 3,\\ 1, 12, 12, 4, 9, 9, 3, 10, 10, 12, 1, 1, 9, 4, 4, 10, 3, 3, 1, 12, 12, 4, \dots$$

The period length is visibly 18 $(= (p-1)^2/8)$; see Conjecture 46(1) in Section 13. Despite correspondence with the authors of [4], these concerns were not dispelled.

$p \equiv 1 \pmod 4$ by proving the refinement (see [13, Theorem 2][2])

$$d\left(n + \tfrac{p-1}{2}\right) \equiv (-1)^{(p-5)/4}(3 \cdot 7 \cdot 11 \cdots (2p-3))^2 d(n) \pmod p,$$
$$\text{for } p \equiv 1 \pmod 4 \text{ and } n \geq \tfrac{p+1}{2}. \quad (1.2)$$

Since on the right-hand side of this congruence we have a square, $\frac{p-1}{2}$-fold iteration of this congruence in combination with Fermat's Little Theorem shows that $d(n)$ is (eventually) periodic modulo p with (not necessarily minimal) period length $\frac{(p-1)^2}{4}$.[3]

What all these authors did not notice is that periodicity was already (implicitly) known. Namely, Rodríguez Villegas and Zagier showed in [9, §§ 6, 7] that Taylor coefficients of entire modular forms at complex multiplication points[4] — suitably normalised — can be computed via a certain recursive (polynomial) scheme, and they indicated that this scheme can also be adapted to cover half-integral weights.[5] Moreover, O'Sullivan and Risager proved in [8, Theorem 6.1] (in a special case, but the argument is completely general) that integral number sequences that are produced by such a scheme are automatically periodic modulo any prime power. On the other hand, this argument only leads to very crude, super-exponential bounds on the period length, it cannot tell from when on periodicity occurs, and it also cannot predict whether such a sequence vanishes eventually modulo a prime power (thus producing a trivial period).

The purpose of the present article is to provide full proofs of all the above items that do include explicit statements about period lengths, respectively from when on periodicity or vanishing modulo a prime power holds. The theorem below collects our corresponding findings (see Theorems 23, 42, and 34).

Theorem 1. (1) *Let p be a prime number with $p \equiv 3 \pmod 4$, and let e be an integer with $e \geq 2$. Then $d(n) \equiv 0 \pmod{p^e}$ for $n \geq \left\lceil \frac{(e-1)p^2}{2} \right\rceil$.*

(2) *Let p be a prime number with $p \equiv 1 \pmod 4$, and let e be a positive integer. Then the sequence $\big(d(n)\big)_{n \geq e+1}$ is purely periodic modulo p^e with (not necessarily minimal) period length $\frac{1}{4}p^{e-1}(p-1)^2$.*

(3) *Let e be a positive integer. The sequence $(d(n))_{n \geq 0}$, when taken modulo any fixed 2-power 2^e with $e \geq 3$, is purely periodic with (not necessarily minimal) period length 2^{e-1}. Modulo 4, the sequence is purely periodic with period length 4, the first few values of the sequence (modulo 4) being given by*

$$1, 1, 3, 3, 1, \ldots.$$

[2] Wakhare did not simplify $-2^{(p-1)/2}$ modulo p on the right-hand side of the displayed congruence in [13, Theorem 1] to $(-1)^{(p-5)/4}$.

[3] Wakhare concludes a period length of only $\frac{(p-1)^2}{2}$. The reason is probably the missed simplification pointed out in Footnote 2.

[4] $\tau = i$ is such a "complex multiplication point" for θ_3

[5] We have worked out such a recursive scheme for producing the Taylor coefficients $d(n)$: let the polynomials $p_n(t)$, $n \geq 0$, be given by

$$p_{n+1}(t) = (\tfrac{1}{6} - 96t^2)p_n'(t) + 16(4n+1)tp_n(t) - n(n - \tfrac{1}{2})(256t^2 + \tfrac{4}{3})p_{n-1}(t),$$

with $p_{-1}(t) = 0$ and $p_0(t) = 1$. Then $p_{2n+1}(0) = 0$ and

$$d(n) = 2^{-n}p_{2n}(0)$$

for all $n \geq 0$.

Our proof of Item (2) in fact generalises the congruence (1.2) to prime powers; see (12.3). We remark that Larson and Smith [6] prove a result analogous to Theorem 1(1) for Taylor expansions of modular forms of integral weight at complex multiplication points in some imaginary quadratic number field, for primes $p \geq 5$.

The proofs of the congruence properties of $d(n)$ listed in Theorem 1 that we provide here are elementary throughout. They do however reveal that these congruences hold at a much finer, polynomial level; see Remarks 10, 12, 18, 20, Theorems 31–33, and 41.

More specifically, our proofs require a careful p-adic analysis of the earlier mentioned recursive procedure of computation of the numbers $d(n)$. This procedure involves two further sequences, namely $\big(u(n)\big)_{n\ge0}$ and $\big(v(n)\big)_{n\ge0}$, and a lower triangular matrix $\big(r(n,k)\big)_{n,k\ge0}$. We refer the reader to Section 2 for the corresponding definitions. In order to accomplish the proofs of the congruence assertions in Theorem 1, we must first analyse $u(n)$, $v(n)$, and $r(n,k)$ modulo the three families of prime powers that feature in the theorem, before we can make conclusions about $d(n)$.

Accordingly, our article is organised as follows. In the next section, we review Romik's recursive procedure to compute the Taylor coefficients $d(n)$. This section contains in fact a notable novelty that is crucial for our proofs. Briefly, Romik defines a sequence $\big(v(n)\big)_{n\ge0}$ and shows that it equals the product of the matrix $\big(r(n,k)\big)_{n,k\ge0}$ — which in its definition involves the sequence $\big(u(n)\big)_{n\ge0}$ — and the sequence $\big(d(n)\big)_{n\ge0}$ (seen as column vector). At this point, one wants to invert this relation to have direct access to the numbers $d(n)$. This requires the computation of the *inverse* of the matrix $\big(r(n,k)\big)_{n,k\ge0}$. In all previous papers, this point is somehow by-passed. However, as it turns out, Lagrange inversion permits one to give a compact formula for the entries of this inverse matrix, again in terms of the sequence $\big(u(n)\big)_{n\ge0}$; see (2.11). More specifically, we extend the matrix $\big(r(n,k)\big)_{n,k\ge0}$ to the larger matrix $\mathbf{R} = \big(R(n,k)\big)_{n,k\ge0}$ in which the former matrix is embedded as the submatrix indexed by even labelled rows and columns; that is, $r(n,k) = R(2n,2k)$ for all n and k. Our inversion result then applies to this larger matrix which, in view of the Lagrange inversion formula, is the one that should be looked at.

In Section 3, we recall the standard results from elementary number theory concerning the divisibility of factorials and binomial coefficients by prime powers that we use ubiquitously in our article.

Subsequently, we embark on the p-adic analysis of our sequences. Section 4 is devoted to the proof that $u(n)$ vanishes modulo any fixed odd prime prime power p^e for large enough n. It contains two main results: Theorem 9 treats the case where $p \equiv 3 \pmod 4$, while Theorem 11 contains the (significant) improvement for the case where $p \equiv 1 \pmod 4$. The corresponding results for $v(n)$ modulo odd prime powers are presented in Section 5. Again there are two main results: Theorem 17 treats the "generic case", while Theorem 19 contains the (significant) improvement for the case where $p \equiv 1 \pmod 4$. The final preparations for our first main result on $d(n)$ is done in Section 6, where we prove a p-divisibility result for the matrix entries of the *inverse* of the matrix $\mathbf{R}$ for primes p with $p \equiv 3 \pmod 4$; see Theorem 22. Theorem 23 in Section 7 is then our first main result for the sequence $\big(d(n)\big)_{n\ge0}$. It says that $d(n)$ is divisible by prime powers p^e with $p \equiv 3 \pmod 4$ for $n \geq \lceil (e-1)p^2/2 \rceil$ and $e \geq 2$, thus establishing Part (1) of Theorem 1.

The next sections are devoted to the analysis of our sequences and our matrix $\mathbf{R}$ modulo powers of 2. The subject of Section 8 is to show that the sequence $(v(n))_{n\ge0}$ is purely periodic modulo any fixed power of 2, together with a precise statement concerning the period length. As a matter of fact, Theorems 31 and 32 contain a polynomial refinement of these assertions. In Section 9 we establish a periodicity result for the entries of the *inverse* of the matrix $\mathbf{R}$ modulo powers of 2; see Theorem 33. These findings are then put together to obtain our second main result for the sequence $\big(d(n)\big)_{n\ge0}$. Namely, $\big(d(n)\big)_{n\ge0}$ is purely periodic modulo 2^e with (not necessarily minimal) period length 2^{e-1} for $e\ge3$, while modulo 4 it starts with $1,1,3,3$ and then repeats itself; see Theorem 34 in Section 10. These results establish Part (3) of Theorem 1.

The purpose of Sections 11 and 12 is to prove periodicity of $\big(d(n)\big)_{n\ge0}$ modulo prime powers p^e with $p\equiv1\pmod 4$, accompanied by a precise statement on the period length. The preparatory work in the former section concerns the analysis of the entries of the *inverse* of the matrix $\mathbf{R}$ modulo these prime powers; see Theorem 41. Again, this theorem actually contains a polynomial refinement. This is then used to prove our third main result on $d(n)$, namely that $\big(d(n)\big)_{n\ge e+1}$ is purely periodic modulo p^e with $p\equiv1\pmod 4$ with (not necessarily minimal) period length $\frac14p^{e-1}(p-1)^2$, thus establishing Part (2) of Theorem 1; see Theorem 42 in Section 12.

The final section, Section 13, addresses the question of whether our results can be improved concerning period length, respectively point of vanishing. As is reported in that section, (computer) data suggest that our results are not far from being optimal, but that it may be possible to improve them by — roughly — a factor of 2. (Our result on $d(n)$ modulo powers of 2 in Theorem 1(3) seems to be optimal, though.) A proof of such strengthenings would however require considerable effort involving highly technical considerations.

2. Romik's recursive procedure for the computation of $d(n)$

In order to prove integrality of the coefficients $d(n)$ in (1.1), Romik sets up a recursive scheme to compute these numbers from which it is immediate that it produces integers. This scheme involves two further sequences, $\big(u(n)\big)_{n\ge0}$ and $\big(v(n)\big)_{n\ge0}$, and a lower triangular matrix $\big(r(n,k)\big)_{n,k\ge0}$, which we are going to define next.

Let $(u(n))_{n\ge0}$ be the sequence defined by an exponential generating function $U(t)$ via (cf. [10, Eq. (9) and Lemma 5][6])

$$U(t):=\sum_{n\ge0}\frac{u(n)}{(2n+1)!}t^{2n+1}=t\frac{{}_2F_1\left[\begin{matrix}\frac34,\frac34\\ \frac32\end{matrix};4t^2\right]}{{}_2F_1\left[\begin{matrix}\frac14,\frac14\\ \frac12\end{matrix};4t^2\right]}. \tag{2.1}$$

Here, ${}_2F_1[\dots]$ is the usual Gauß hypergeometric series. The reader is referred to any standard book on special functions for the definition, such as e.g. [2, Eq. (2.1.2)]. It

[6]The reader should be warned that our definitions of the series $U(t)$ and the later defined series $V(t)$ slightly deviate from Romik's definitions; one gets Romik's series from ours by dividing our $U(t)$ by t, and by then replacing t by $t^{1/2}$. Our convention is crucial for the application of Lagrange inversion in Proposition 2.

is not difficult to see (cf. [10, Eq. (17)]) that an equivalent definition of $u(n)$ is by the recurrence

$$u(n)=\prod_{j=1}^{n}(4j-1)^2-\sum_{m=0}^{n-1}\binom{2n+1}{2m+1}\left(\prod_{j=1}^{n-m}(4j-3)^2\right)u(m),\quad \text{with } u(0)=1. \tag{2.2}$$

The first few values turn out to be

$$1,6,256,28560,6071040,2098483200,1071889920000,758870167910400,\\ 711206089850880000,852336059876720640000,1271438437097485762560000,\dots$$

For convenience, we shall later frequently use the short notations

$$\Pi_1(N):=\prod_{j=1}^{N}(4j-1)^2 \quad \text{and} \quad \Pi_3(N):=\prod_{j=1}^{N}(4j-3)^2. \tag{2.3}$$

Then, using these, the above recurrence can be rewritten as

$$u(n)=\Pi_1(n)-\sum_{m=0}^{n-1}\binom{2n+1}{2m+1}\Pi_3(n-m)u(m),\quad \text{with } u(0)=1. \tag{2.4}$$

The sequence $(v(n))_{n\ge0}$ is also defined via an exponential generating function, namely by (cf. [10, Eq. (10) and Lemma 6])

$$\sum_{n\ge0}\frac{v(n)}{2^n(2n)!}t^{2n}={}_2F_1\left[\begin{matrix}\frac14,\frac14\\ \frac12\end{matrix};4t^2\right]^{1/2}=\left(\sum_{j\ge0}\frac{\prod_{\ell=1}^{j}(4\ell-3)^2}{(2j)!}t^{2j}\right)^{1/2}. \tag{2.5}$$

Again, it is not difficult to see (cf. [10, Eq. (20)]) that an equivalent definition of $v(n)$ is by the recurrence

$$v(n)=2^{n-1}\Pi_3(n)-\frac12\sum_{m=1}^{n-1}\binom{2n}{2m}v(m)v(n-m),\quad \text{with } v(0)=1. \tag{2.6}$$

The first few values turn out to be

$$1,1,47,7395,2453425,1399055625,1221037941375,1513229875486875,\\ 2526879997358510625,5469272714829657020625,14892997153152592003359375,\dots$$

The lower triangular matrix $\big(r(n,k)\big)_{n,k\ge0}$ is defined via the generating function $U(t)$ for the $u(n)$'s in (2.1), namely by

$$r(n,k):=2^{n-k}\frac{(2n)!}{(2k)!}\left\langle t^{2n}\right\rangle U^{2k}(t). \tag{2.7}$$

The matrix is indeed lower triangular since $r(n,k)=0$ for $n<k$, due to the fact that $U(t)$ has zero constant term. For the convenience of the reader, we display the table of

numbers $r(n,k)$ with $0 \le n,k \le 6$:

1	0	0	0	0	0	0
0	1	0	0	0	0	0
0	48	1	0	0	0	0
0	7584	240	1	0	0	0
0	2515968	97664	672	1	0	0
0	1432498176	63221760	560448	1440	1	0
0	1247557386240	60299053056	628024320	2141568	2640	1

Romik showed that the Taylor coefficients $d(n)$ in (1.1) are related to the numbers $v(n)$ via the triangular system of equations

$$v(n) = \sum_{k=0}^{n} r(n,k)d(k), \quad \text{for all } n \ge 0. \tag{2.8}$$

This may be "turned around" to obtain a recursion for the $d(n)$'s (cf. [10, Theorem 7]),

$$d(n) = v(n) - \sum_{k=0}^{n-1} r(n,k)d(k), \quad \text{and } d(0) = 1. \tag{2.9}$$

Without any doubt, Equation (2.9) does provide a recursive way to compute the coefficients $d(n)$. Indeed, Scherer [11] and Wakhare [13] used it for the proof of their results. However, in our opinion the suitability of (2.9) for the proof of congruence relations satisfied by the $d(n)$'s using inductive arguments is limited. It is more conceptual to invert the relation (2.8) and express the $d(n)$'s entirely in terms of the $v(n)$'s and the *inverse* of the matrix $\big(r(n,k)\big)_{n,k\ge 0}$.

In order to carry out this programme, we need an explicit formula for the entries of this inverse matrix. It turns out that this can best be achieved if one defines the (larger) infinite matrix $\mathbf{R} = (R(n,k))_{n,k\ge 0}$ by

$$R(n,k) = 2^{(n-k)/2}\frac{n!}{k!}\left\langle t^n\right\rangle U^k(t). \tag{2.10}$$

Since $U(t)$ is a power series in which even powers of t do not occur, the matrix $\mathbf{R}$ has a "checkerboard pattern"; more precisely, $R(n,k) \ne 0$ if, and only if, n and k have the same parity. The entries $R(n,k)$ are in fact all integers. This follows from this checkerboard pattern of $\mathbf{R}$ (implying that $2^{(n-k)/2}$ on the right-hand side of (2.10) is always an integer) and from the exponential formula of combinatorics as Romik explains in [10, Proof of Theorem 7] in a special case (namely in the case where both n and k are even; the general case can be treated in the same manner). The matrix $\big(r(n,k)\big)_{n,k\ge 0}$ is a submatrix of $\mathbf{R}$ since $R(2n,2k) = r(n,k)$ for all n and k (compare with (2.7)).

Proposition 2. *The inverse $\mathbf{R}^{-1}$ of $\mathbf{R}$ is given by $(R^{-1}(n,k))_{n,k\ge 0}$ with*

$$R^{-1}(n,k) = 2^{(n-k)/2}\frac{(n-1)!}{(k-1)!}\left\langle t^{-k}\right\rangle U^{-n}(t). \tag{2.11}$$

Here, the case $k=0$ has to be interpreted as $R^{-1}(0,0)=1$ and $R^{-1}(n,0)=0$ for $n \ge 1$. Moreover, $\mathbf{R}^{-1}$ has integer entries and $R^{-1}(n,k) \ne 0$ only if n and k have the same parity.

Proof. That $\mathbf{R}^{-1}$ has integer entries is obvious since it is the inverse of a triangular matrix with integer entries (cf. [10, Theorem 7]) and 1's on the main diagonal.

The first assertion is a consequence of Lagrange inversion (cf. [12, Theorem 5.4.2]): if $F(t)$ is a formal power series with $F(0) = 0$ and $F'(0) \neq 0$, and $F^{(-1)}(t)$ is its compositional inverse, then

$$\langle t^n \rangle \left(F^{(-1)}(t)\right)^k = \frac{k}{n} \left\langle t^{-k} \right\rangle F^{-n}(t).$$

In order to apply this theorem to our situation, it must be observed that under the above conditions the matrix $\left(\langle t^n \rangle F^k(t)\right)_{n,k\geq 0}$ is inverse to $\left(\langle t^n \rangle \left(F^{(-1)}(t)\right)^k\right)_{n,k\geq 0}$. If one applies this observation with $F(t) = U(t)$, then the assertion of the proposition follows upon little manipulation.

With the formula (2.11) established, the parity condition follows again from the fact that $U(t)$ is a power series in which only odd powers of t occur. □

Using the entries of the matrix $\mathbf{R}$, the system of equations (2.8) can be rewritten as

$$v(n) = \sum_{k=0}^{n} R(2n, 2k) d(k), \quad \text{for all } n \geq 0.$$

If we invert this relation using the inverse matrix $\mathbf{R}^{-1}$, then we obtain

$$d(n) = \sum_{k=0}^{n} R^{-1}(2n, 2k) v(k). \tag{2.12}$$

We are going to use this formula in the proofs in Sections 10 and 12.

3. Classical criteria for divisibility of factorials and binomial coefficients by prime powers

Here and in the sequel, for a prime number p, let $v_p(\alpha)$ denote the p-adic valuation of the integer (or rational number) α, defined as the maximal exponent e such that α/p^e is an integer (respectively a rational number with numerator and denominator coprime to p).

There are essentially two formulae for the p-adic valuation of a factorial. The one that we need in this article is Legendre's formula.

Lemma 3 (Legendre's formula [7, p. 12])**.** *Let N be a positive integer and p a prime number. Then*

$$v_p(N!) = \frac{N - s_p(N)}{p-1},$$

where $s_p(N)$ denotes the sum of digits in the p-adic representation of N.

Similarly, there are essentially two formulae for the p-adic valuation of a binomial coefficient, one in terms of the number of carries when adding the involved numbers, the other in terms of digit sums; we shall need the former one.

Lemma 4 (Kummer's theorem [5, pp. 115–116])**.** *Let N and K be positive integers and p a prime number. Then $v_p\left(\binom{N}{K}\right)$ equals the number of carries when K and $N-K$ are added in terms of their p-adic representations.*

The following relation forms the link between the previous two lemmas, and it provides, at the same time, the previously mentioned alternative in computing the p-adic valuation of a binomial coefficient.

Lemma 5. *Let A and B be positive integers and p a prime number. Then*

$$\frac{1}{p-1}\Big(s_p(A)+s_p(B)-s_p(A+B)\Big)$$
$$= \#(\text{carries when adding } A \text{ and } B \text{ in their } p\text{-adic representations}).$$

4. The sequence $(u(n))_{n\geq 0}$ modulo odd prime powers

In this section, we analyse the numbers $u(n)$ modulo odd prime powers p^e. The first result is Theorem 9 which states that, for primes p congruent to 3 modulo 4 and all integers $e \geq 2$, the number $u(n)$ vanishes modulo p^e for $n \geq \lfloor (e-1)p^2/2 \rfloor$. The proof of the theorem is inductive, the start of the induction being given in Proposition 8, which is itself based on auxiliary results in Lemma 7. In case the prime p should be congruent to 1 modulo 4, however, a much stronger result holds; see Theorem 11. The proof of that theorem requires two auxiliary results which we state and prove separately; cf. Lemmas 13 and 14.

We begin by providing lower bounds on the p-adic valuations of the products $\Pi_1(N)$ and $\Pi_3(N)$ defined in (2.3) that will be ubiquitously used in this and the next section.

Lemma 6. *For all odd primes p and non-negative integers N, we have*

$$v_p\big(\Pi_1(N)\big) \geq 2\left\lfloor \tfrac{N}{p} \right\rfloor \quad \textit{and} \quad v_p\big(\Pi_3(N)\big) \geq 2\left\lfloor \tfrac{N}{p} \right\rfloor. \tag{4.1}$$

If $p \equiv 1 \pmod 4$, then we even have

$$v_p\big(\Pi_3(N)\big) \geq 2\left\lfloor \tfrac{N+\frac{3}{4}(p-1)}{p} \right\rfloor. \tag{4.2}$$

Next we state and prove the announced auxiliary results, which afterwards lead to Proposition 8.

Lemma 7. *Let p be an odd prime number, and let $(u(n))_{n\geq 0}$ be defined by the recurrence (2.2). Then we have*

$$u(ap+b) \equiv 0 \pmod p, \quad \textit{for } 1 \leq a \leq \tfrac{p-1}{2} \textit{ and } 0 \leq b \leq a-1, \tag{4.3}$$

and

$$u\left(ap+\tfrac{p-1}{2}+b\right) \equiv 0 \pmod p, \quad \textit{for } 1 \leq a \leq \tfrac{p-1}{2} \textit{ and } 0 \leq b \leq a. \tag{4.4}$$

Moreover, if $p \equiv 3 \pmod 4$, the second congruence also holds for $a=0$, that is, $u\left(\frac{p-1}{2}\right) \equiv 0 \pmod p$ for primes p with $p \equiv 3 \pmod 4$.

Proof. We prove the assertions by induction on the size of $ap+b$ and of $ap+\frac{p-1}{2}+b$, simultaneously. The induction is based on the recurrence (2.2).

Now let first $n = ap+b$ with a and b satisfying the conditions in (4.3). We want to prove that $u(n) \equiv 0 \pmod p$.

It is clear that the first term on the right-hand side of (2.2), the product $\Pi_1(n) = \Pi_1(ap+b)$, is divisible by p because of (4.1).

From Lemma 4 we infer that the binomial coefficient $\binom{2n+1}{2m+1} = \binom{2ap+2b+1}{2m+1}$ is divisible by p, except when $2m = cp + d$ with both $0 \le c \le 2a$ and $0 \le d \le 2b$. It is important to note that at this point the upper bounds of $\frac{p-1}{2}$ for a and b enter crucially.

If $c = 0$ (and hence d even since $2m = cp+d = d$), then $\Pi_3(n-m) = \Pi_3\left(ap + b - \frac{d}{2}\right)$ is divisible by p according to (4.1). From now on we may assume that $c \ge 1$.

We distinguish whether c and d are both even or both odd. (There are no other cases since $2m = cp + d$ is even.)

If both c and d are even, then, provided $c > d$, we may use the induction hypothesis (4.3) to infer that $u(m) = u\left(\frac{c}{2}p + \frac{d}{2}\right)$ is divisible by p. On the other hand, if $c \le d$, then we have

$$n - m = \left(a - \tfrac{c}{2}\right)p + b - \tfrac{d}{2}.$$

Since, by assumption, we have $a > b$, we have

$$a - \tfrac{c}{2} > b - \tfrac{d}{2} \ge 0.$$

Consequently, again using (4.1), we obtain that $\Pi_3(n-m)$ is divisible by p.

Now let both c and d be odd. Here we may rewrite $m = \frac{c}{2}p + \frac{d}{2}$ as

$$m = \tfrac{c-1}{2}p + \tfrac{p-1}{2} + \tfrac{d+1}{2}.$$

Furthermore, we may write

$$n - m = \left(a - \tfrac{c+1}{2}\right)p + \tfrac{p-1}{2} + b - \tfrac{d-1}{2}.$$

It should be noted that, if $c \le d$, we have $a - \frac{c+1}{2} > b - \frac{d+1}{2} \ge 0$. As a consequence, by (4.1), we have $\Pi_3(n-m) \equiv 0 \pmod p$. If, on the other hand, we have $c > d$, then $u(m) \equiv 0 \pmod p$, again by the induction hypothesis (4.4).

Next we discuss the case where $n = ap + \frac{p-1}{2} + b$ with a and b satisfying the conditions in (4.4). We want to prove that $u(n) \equiv 0 \pmod p$.

Again it is clear that the first term on the right-hand side of (2.2), the product $\Pi_1(n) = \Pi_1(ap + \frac{p-1}{2} + b)$, is divisible by p because of (4.1).

In the current case, the binomial coefficient on the right-hand side of (2.2) becomes $\binom{2n+1}{2m+1} = \binom{(2a+1)p+2b}{2m+1}$. Here it must be observed that, because of the upper bounds on a and b in (4.4), we have $2a + 1 \le p$ and $2b \le p - 1$. If $a = \frac{p-1}{2}$, so that $2a + 1 = p$, then by Lemma 4 $\binom{2n+1}{2m+1} = \binom{p^2+2b}{2m+1}$ is divisible by p, except when $1 \le 2m + 1 \le 2b$. In this exceptional case, we have $\Pi_3(n-m) \equiv 0 \pmod p$ by (4.1).

We assume from now on that $a < \frac{p-1}{2}$. From Lemma 4 we infer that the binomial coefficient $\binom{2n+1}{2m+1} = \binom{(2a+1)p+2b}{2m+1}$ is divisible by p, except when $2m = cp + d$ with both $0 \le c \le 2a + 1$ and $0 \le d \le 2b - 1$.

We distinguish whether c and d are both even or both odd. (There are no other cases since $2m = cp + d$ is even.)

If both c and d are even, then, provided $c > d$, we may use the induction hypothesis (4.3) to infer that $u(m) = u\left(\frac{c}{2}p + \frac{d}{2}\right)$ is divisible by p. On the other hand, if $c \le d$, then we have

$$n - m = \left(a - \tfrac{c}{2}\right)p + \tfrac{p-1}{2} + b - \tfrac{d}{2}.$$

Since, by assumption, we have $a \ge b$, we have

$$a - \tfrac{c}{2} \ge b - \tfrac{d}{2} \ge 1.$$

Consequently, again using (4.1), we obtain that $\Pi_3(n-m)$ is divisible by p.

Now let both c and d be odd. We may again rewrite $m = \frac{c}{2}p + \frac{d}{2}$ as

$$m = \tfrac{c-1}{2}p + \tfrac{p-1}{2} + \tfrac{d+1}{2}.$$

Furthermore, we may write

$$n - m = \left(a - \tfrac{c-1}{2}\right)p + b - \tfrac{d+1}{2}.$$

Hence, according to the induction hypothesis (4.4), we have $u(m) \equiv 0 \pmod p$ if $c > d$. Otherwise we have

$$a - \tfrac{c-1}{2} > b - \tfrac{d+1}{2} \geq 0.$$

Hence, $\Pi_3(n-m) \equiv 0 \pmod p$ due to (4.1).

Finally, the congruence for $u\left(\frac{p-1}{2}\right)$ in the case where $p \equiv 3 \pmod 4$ holds because, as is seen by inspection, the first term on the right-hand side of (2.2), the product $\Pi_1(n) = \Pi_1(\frac{p-1}{2})$, is divisible by p^2 (here, the condition $p \equiv 3 \pmod 4$ enters crucially). □

Proposition 8. *Let $(u(n))_{n\geq 0}$ be defined by the recurrence* (2.2)*. Then, given a prime $p \equiv 3 \pmod 4$ and a positive integer e, the number $u(n)$ is divisible by p^2 for $n \geq \left\lfloor \frac{p^2}{2} \right\rfloor$.*

Proof. Let $n \geq \left\lfloor \frac{p^2}{2} \right\rfloor = \frac{p^2-1}{2}$. As in the proof of Lemma 7, we use again induction on n. Also here, the induction will be based on (2.2), and it proceeds by showing that each summand on the right-hand side is divisible by p^2.

For the start of the induction, we consider $n = \frac{p^2-1}{2}$, so that $2n+1 = p^2$. In that case, there are two carries when adding $2m+1$ and $2(n-m)$ for $0 \leq m \leq n-1$, except when both of $2m+1$ or $2(n-m)$ are divisible by p. In the former case, Lemma 4 implies that the binomial coefficient $\binom{2n+1}{2m+1}$ is divisible by p^2. In the latter case, there is only one carry and so the binomial coefficient $\binom{2n+1}{2m+1}$ is only divisible by p. In its turn, we see that $u(m)$ is divisible by p due to (4.4) with $b = 0$ and the last assertion in Lemma 7. In either case, each summand on the right-hand side of (2.2) is divisible by p^2. Furthermore, it is again clear that the first term on the right-hand side, the product $\Pi_1(n)$, is divisible by p for all $n \geq \left\lfloor \frac{p^2}{2} \right\rfloor$ because of (4.1).

We will assume $n \geq \frac{p^2+1}{2}$ from now on.

We may restrict our attention to $n \leq p^2$ because otherwise either $m \geq \frac{p^2+1}{2}$ or $n - m \geq \frac{p^2+1}{2}$; whence, either $u(m) \equiv 0 \pmod{p^2}$ or $\Pi_3(n-m) \equiv 0 \pmod{p^2}$. Consequently, in this case each term on the right-hand side of (2.2) would be divisible by p^2.

To summarise the discussion so far: we may write $2n$ as $2n = p^2 + ap + b$ for some a and b not of the same parity and with $0 \leq a, b \leq p-1$.

If there are two carries when adding $2m+1$ and $2(n-m)$, then by Lemma 4 the binomial coefficient $\binom{2n+1}{2m+1}$ is divisible by p^2. Hence the corresponding summand on the right-hand side of (2.2) is divisible by p^2.

Now let us assume that there is only one carry when adding $2m+1$ and $2(n-m)$. As earlier, if either m or $n-m$ are larger than $\frac{p^2}{2}$, then $u(m)$ or $\Pi_3(n-m)$ are divisible by p^2, and thus as well the corresponding summand on the right-hand side of (2.2). We may therefore assume without loss of generality that $2m = cp + d$ with $c \leq \frac{p-1}{2}$. We may furthermore assume that $d \le b$ since, otherwise, there would be two carries when adding $2m+1$ and $2(n-m)$.

We distinguish again whether c and d are both even or both odd.

Let first c and d be even. We write $m = \frac{c}{2}p + \frac{d}{2}$. If $c > d$, then by (4.3), we infer $u(m) \equiv 0 \pmod p$. If $c \le d$, then we may write

$$n - m = \left(\tfrac{p+a-c}{2}\right)p + \tfrac{b-d}{2} = \left(\tfrac{p+a-c-1}{2}\right)p + \tfrac{p-1}{2} + \tfrac{b-d+1}{2}$$

and, depending on the parities of a and b, use the alternative which has an integer coefficient in front of p. By our assumptions, we have

$$\tfrac{p+a-c}{2} > \tfrac{b+a-c}{2} \ge \tfrac{b-c}{2} \ge \tfrac{b-d}{2} \ge 0.$$

If $a = 0$ then b must be odd, implying that the last inequality is strict so that $\frac{p+a-c-1}{2} = \frac{p-c-1}{2}$ is also positive. By (4.1), regardless whether $a = 0$ or not, this implies that $\Pi_3(n-m) \equiv 0 \pmod p$. In total, in both cases this shows that the corresponding summand in (2.2) is divisible by p^2.

Now let c and d be odd. Here we write $m = \frac{c-1}{2}p + \frac{p-1}{2} + \frac{d+1}{2}$. If $c > d$, then by (4.4), we infer $u(m) \equiv 0 \pmod p$. If $c \le d$, then we may again write

$$n - m = \left(\tfrac{p+a-c}{2}\right)p + \tfrac{b-d}{2} = \left(\tfrac{p+a-c-1}{2}\right)p + \tfrac{b-d+1}{2}.$$

Arguing as before, we conclude that $\Pi_3(n-m) \equiv 0 \pmod p$. This shows again that the corresponding summand in (2.2) is divisible by p^2.

If there is no carry when adding $2m+1$ and $2(n-m)$, then necessarily one of $2m+1$ or $2(n-m)$ is at least p^2+1. So, again, one of $u(m)$ or $\Pi_3(n-m)$ is divisible by p^2 due to the induction hypothesis, respectively due to (4.1).

This completes the proof of the proposition. □

The following theorem proves Conjecture 18(1) in [13] for $u(n)$.

Theorem 9. *Let $(u(n))_{n\ge 0}$ be defined by the recurrence* (2.2). *Then, given a prime $p \equiv 3 \pmod 4$ and an integer $e \ge 2$, the number $u(n)$ is divisible by p^e for $n \ge \left\lfloor \frac{(e-1)p^2}{2} \right\rfloor$.*

Proof. We proceed by a double induction on e and n, the outer induction being on e. For the start of the induction, we use Proposition 8 which proves the assertion of the theorem for $e = 2$. From now on let $e \ge 3$.

We assume that $\left\lfloor \frac{(e-1)p^2}{2} \right\rfloor \le n < \left\lfloor \frac{ep^2}{2} \right\rfloor$. We claim that the first term on the right-hand side of (2.2), namely $\Pi_1(n)$, is always divisible by p^e under this assumption. Indeed, by (4.1) we have

$$v_p\left(\Pi_1(n)\right) \ge 2\left\lfloor \tfrac{n}{p} \right\rfloor \ge 2\left\lfloor \tfrac{1}{p}\left\lfloor \tfrac{(e-1)p^2}{2} \right\rfloor \right\rfloor \ge 2\left\lfloor \tfrac{(e-1)p}{2} - \tfrac{1}{2p} \right\rfloor \ge 2\left(\tfrac{3(e-1)}{2} - 1\right) \ge e \tag{4.5}$$

for $e \ge 3$. The conclusion $v_p\left(\Pi_1(n)\right) \ge e$ holds however as well for $e = 2$ as shown by a modification of the final part of the estimation:

$$v_p\left(\Pi_1(n)\right) \ge 2\left\lfloor \tfrac{n}{p} \right\rfloor \ge \cdots \ge 2\left\lfloor \tfrac{p}{2} - \tfrac{1}{2p} \right\rfloor = 2\left(\tfrac{p}{2} - \tfrac{1}{2}\right) \ge 2. \tag{4.6}$$

Next we consider the summand on the right-hand side of (2.2) for $\left\lfloor \frac{(f-1)p^2}{2} \right\rfloor \le m < \left\lfloor \frac{fp^2}{2} \right\rfloor$ with $2 \le f \le e-2$. By the induction hypothesis applied to $u(m)$, we have

$v_p(u(m)) \geq f$. Furthermore we have

$$n - m > \left\lfloor \tfrac{(e-1)p^2}{2} \right\rfloor - \left\lfloor \tfrac{fp^2}{2} \right\rfloor \geq \left\lfloor \tfrac{(e-f-1)p^2}{2} \right\rfloor.$$

Therefore, by replacing n by $n-m$ and e by $e-f$ in (4.5) and (4.6), we get

$$v_p\left(\Pi_3(n-m)\right) \geq e - f \tag{4.7}$$

since $e - f \geq 2$. We infer that $v_p\big(u(m)\Pi_3(n-m)\big) \geq f + (e-f) = e$, and hence the corresponding summand in (2.2) is divisible by p^e.

Let now $0 \leq m < \left\lfloor \frac{p^2}{2} \right\rfloor$. In that case, the previous argument yields that $n - m > \left\lfloor \frac{(e-2)p^2}{2} \right\rfloor$, with the consequence that we only have $v_p(\Pi_3(n-m)) \geq e-1$. It may be that actually $n - m \geq \left\lfloor \frac{(e-1)p^2}{2} \right\rfloor$. Then the estimation (4.7) implies that $v_p(\Pi_3(n-m)) \geq e$, so that the corresponding summand in (2.2) is divisible by p^e. On the other hand, if $\left\lfloor \frac{(e-2)p^2}{2} \right\rfloor \leq n - m < \left\lfloor \frac{(e-1)p^2}{2} \right\rfloor$, then we may write $2n = (e-1)p^2 + ap + b$ and $2(n-m) = (e-2)p^2 + cp + d$ for some a, b, c, d with $0 \leq a, b, c, d \leq p-1$. Since $2m+1 < p^2$, there is (at least) one carry when adding $2(n-m)$ and $2m+1$. Therefore, by Lemma 4, the binomial coefficient $\binom{2n+1}{2m+1}$ is divisible by p. Together with the previously observed fact that $v_p(\Pi_3(n-m)) \geq e-1$ this shows that the corresponding summand in (2.2) is divisible by p^e.

Finally, let $\left\lfloor \frac{(e-2)p^2}{2} \right\rfloor \leq m < \left\lfloor \frac{(e-1)p^2}{2} \right\rfloor$. The induction hypothesis (in n) implies that in this case we have $v_p(u(m)) \geq e-1$. We write $2n+1 = (e-1)p^2 + ap + b$ and $2m+1 = (e-2)p^2 + cp + d$ for some a, b, c, d with $0 \leq a, b, c, d \leq p-1$. If $n - m \geq \left\lfloor \frac{p^2}{2} \right\rfloor$, then by (4.6) we obtain $v_p(\Pi_3(n-m)) \geq 1$. If, on the other hand, we have $n - m < \left\lfloor \frac{p^2}{2} \right\rfloor$, then there is (at least) one carry when adding $2m+1$ and $2(n-m)$ in their p-adic representations. Therefore, by Lemma 4, the binomial coefficient $\binom{2n+1}{2m+1}$ is divisible by p. In either case, together with the previously observed fact that $v_p(u(m)) \geq e-1$ this shows that the corresponding summand in (2.2) is divisible by p^e.

This concludes the induction step, and, thus, the proof of the theorem. ☐

Remark 10. An examination of the above arguments reveals that the products $\Pi_1(n)$ and $\Pi_3(n)$ in the definition (2.4) could have been replaced with any functions $f(n)$ and $g(n)$ that satisfy the p-divisibility properties in (4.1).

Theorem 11. *Let* $(u(n))_{n\geq 0}$ *be defined by the recurrence* (2.2). *Then, given a prime* $p \equiv 1 \pmod 4$ *and a positive integer* e, *the number* $u(n)$ *is divisible by* p^e *for* $n \geq \left\lceil \frac{ep}{2} \right\rceil$. *Moreover, the number* $u\big(\frac{p-1}{2}\big)$ *is a quadratic residue modulo* p *and relatively prime to* p.

Proof. We begin with the second assertion. Setting $n = \frac{p-1}{2}$ in (2.2)/(2.4), we obtain

$$u\left(\tfrac{p-1}{2}\right) = \Pi_1\left(\tfrac{p-1}{2}\right) - \sum_{m=0}^{(p-3)/2} \binom{p}{2m+1} \Pi_3\left(\tfrac{p-1}{2}\right) u(m).$$

Due to the range of the sum on the right-hand side, the binomial coefficient is always divisible by p. Therefore, we have

$$u\left(\tfrac{p-1}{2}\right) \equiv \Pi_1\left(\tfrac{p-1}{2}\right) \pmod p. \tag{4.8}$$

The assertion now follows by observing that $\Pi_1\left(\frac{p-1}{2}\right)$ is a square not divisible by p.

For the proof of the first assertion, we proceed again by a double induction on e and n, the outer induction being on e. The theorem is trivial for $e=0$, which serves as the start of the induction.

We divide the proof into subtasks. At many places, the argument depends on the parity of e and/or on the distance of n from its lower bound $\lceil \frac{ep}{2} \rceil$.

TASK 1: THE FIRST TERM ON THE LEFT-HAND SIDE OF (2.4) VANISHES MODULO p^e FOR EVEN e. By (4.1), we have

$$v_p\big(\Pi_1(n)\big) \ge 2\left\lfloor \frac{n}{p} \right\rfloor \ge 2\left\lfloor \frac{\lceil \frac{ep}{2} \rceil}{p} \right\rfloor \ge 2\left\lfloor \frac{e}{2} \right\rfloor = e,$$

as desired, since e is even.

TASK 2: THE ASSERTION HOLDS FOR $n \ge \left\lceil \frac{(e+1)p}{2} \right\rceil$. Under this assumption we have

$$v_p\big(\Pi_1(n)\big) \ge 2\left\lfloor \frac{n}{p} \right\rfloor \ge 2\left\lfloor \frac{\lceil \frac{(e+1)p}{2} \rceil}{p} \right\rfloor \ge 2\left\lfloor \frac{e+1}{2} \right\rfloor \ge e,$$

which shows that the first term on the right-hand side of (2.4) vanishes modulo p^e.

Next we consider the summand on the right-hand side of (2.4). For $m \ge \lceil \frac{ep}{2} \rceil$, the term $u(m)$ is divisible by p^e by the inductive hypothesis (with respect to n), hence the corresponding summand vanishes modulo p^e. Now let $\left\lceil \frac{(f-1)p}{2} \right\rceil \le m < \lceil \frac{fp}{2} \rceil$ with $1 \le f \le e$. Our conditions imply that

$$n - m \ge \left\lceil \frac{(e+1)p}{2} \right\rceil - \left\lceil \frac{fp}{2} \right\rceil + 1 \ge \left\lceil \frac{(e+1-f)p}{2} \right\rceil .$$

Therefore, by using (4.2) we obtain

$$v_p\left(\big(\Pi_3(n-m)\big)u(m)\right) \ge 2\left\lfloor \frac{\lceil \frac{(e+1-f)p}{2} \rceil + \frac{3}{4}(p-1)}{p} \right\rfloor + f - 1 \ge (e-f+1) + f - 1 = e,$$

which shows that also in this case the corresponding summand vanishes modulo p^e.

From now on we assume that $n < \left\lceil \frac{(e+1)p}{2} \right\rceil$ or, more precisely, integrating the overall assumption, that $\lceil \frac{ep}{2} \rceil \le n < \left\lceil \frac{(e+1)p}{2} \right\rceil$.

TASK 3: p-ADIC ANALYSIS OF THE SUMMAND IN (2.4) FOR $\lceil \frac{ep}{2} \rceil \le n < \left\lceil \frac{(e+1)p}{2} \right\rceil$. As before, by the induction hypothesis of the induction on n, the term $u(m)$ in the sum in (2.4) is divisible by p^e for $m \ge \lceil \frac{ep}{2} \rceil$, and thus is the corresponding summand.

Next we consider the summand on the right-hand side of (2.4) for $\left\lceil \frac{(f-1)p}{2} \right\rceil \le m < \lceil \frac{fp}{2} \rceil$ with $1 \le f \le e$. Our conditions imply $n - m \ge \lceil \frac{ep}{2} \rceil - \lceil \frac{fp}{2} \rceil + 1 \ge \left\lceil \frac{(e-f)p}{2} \right\rceil$. Therefore, by using (4.2) we obtain

$$v_p\left(\big(\Pi_3(n-m)\big)u(m)\right) \ge 2\left\lfloor \frac{\lceil \frac{(e-f)p}{2} \rceil + \frac{3}{4}(p-1)}{p} \right\rfloor + f - 1 \ge (e-f) + f - 1 = e - 1.$$

Our goal is to show that the summand is divisible by p^e. We claim that this is indeed the case as long as e is even, or e is odd and $m \neq \frac{fp-1}{2}$ for odd f. We must therefore prove that the binomial coefficient in (2.4) is divisible by p in these cases.

To see this, we consider the p-adic representations of $2m+1$ and $2n-2m$. Since $m \neq \frac{fp-1}{2}$, (this condition is essential for the first line below), these are

$$\begin{aligned}(2m+1)_p &= (f-1)_p * \\ \big(2n-2m\big)_p &= (e-f)_p * \end{aligned} \tag{4.9}$$

Here, $(\alpha)_p$ denotes the p-adic representation of the integer α, and the stars on the right-hand sides indicate the right-most digits of $(2m+1)_p$ and $(2n-2m)_p$ whose precise values are irrelevant. The sum of $2m+1$ and $2n-2m$ is $2n+1$ whose p-adic representation has the form $(e)_p *$. Hence, when adding the two numbers on the right-hand sides of (4.9), at least one carry must occur — namely one from the p^0-digit to the p^1-digit. By Kummer's theorem in Lemma 4, the consequence is that the binomial coefficient $\binom{2n+1}{2m+1}$ is divisible by p. Therefore the corresponding summand is divisible by p^e.

In order to summarise our findings so far:

(1) By Task 2 the assertion of the theorem holds for $n \geq \left\lceil \frac{(e+1)p}{2} \right\rceil$.
(2) For even e and $\left\lceil \frac{ep}{2} \right\rceil \leq n < \left\lceil \frac{(e+1)p}{2} \right\rceil$ we have shown that all summands of the sum on the right-hand side of (2.4) are divisible by p^e. Since in Task 1 we have proved that also the first term on the right-hand side of (2.4) is divisible by p^e, this establishes the assertion of the theorem for even e.
(3) For odd e and $\left\lceil \frac{ep}{2} \right\rceil \leq n < \left\lceil \frac{(e+1)p}{2} \right\rceil$ we have shown that all summands of the sum on the right-hand side of (2.4) vanish modulo p^e except for those where m is of the form $\frac{p-1}{2} + ip$ for some non-negative integer i.

Hence, it remains to discuss the case where e is odd and $\left\lceil \frac{ep}{2} \right\rceil \leq n < \left\lceil \frac{(e+1)p}{2} \right\rceil$.

TASK 4: e IS ODD AND $\left\lceil \frac{ep}{2} \right\rceil \leq n < \left\lceil \frac{(e+1)p}{2} \right\rceil$. By Item (3) above, the relation (2.4) reduces modulo p^e to

$$u(n) \equiv \Pi_1(n) - \sum_{i=0}^{(e-1)/2} \binom{2n+1}{(2i+1)p} \Pi_3\big(n - \tfrac{p-1}{2} - ip\big) u\big(\tfrac{p-1}{2} + ip\big) \pmod{p^e}. \tag{4.10}$$

By the induction hypothesis, we know that

$$v_p\left(u\left(\tfrac{p-1}{2} + ip\right)\right) \geq 2i. \tag{4.11}$$

Furthermore, by (4.1) we have

$$v_p\left(\Pi_3\big(n - \tfrac{p-1}{2} - ip\big)\right) \geq 2\left\lfloor \tfrac{1}{p}\left(n - \tfrac{p-1}{2} - ip\right)\right\rfloor \geq 2\left\lfloor \tfrac{1}{p}\left(\tfrac{(e-2i-1)p}{2}\right)\right\rfloor \geq e - 2i - 1, \tag{4.12}$$

since e is odd. In particular, the inequalities (4.11) and (4.12) together imply that

$$v_p\left(\Pi_3\big(n - \tfrac{p-1}{2} - ip\big) u\big(\tfrac{p-1}{2} + ip\big)\right) \geq e - 1.$$

Consequently, we may consider the binomial coefficient in (4.10) modulo p. Now we use the elementary congruence

$$\binom{ap+r}{bp} \equiv \binom{ap}{bp} \pmod p$$

for positive integers a, b, r with $1 \le r < p$. Since the assumptions of the case in which we are imply that $ep + 2 \le 2n + 1 \le (e+1)p - 1$, we infer that

$$\binom{2n+1}{(2i+1)p} \equiv \binom{ep}{(2i+1)p} \pmod p.$$

Thus, we see that the congruence (4.10) is equivalent with

$$u(n) \equiv \Pi_1(n) - \sum_{i=0}^{(e-1)/2} \binom{ep}{(2i+1)p} \Pi_3\big(n - \tfrac{p-1}{2} - ip\big) u\big(\tfrac{p-1}{2} + ip\big) \pmod{p^e}. \tag{4.13}$$

On the other hand, the inequality (4.12) also implies that we may consider the term $u\big(\frac{p-1}{2} + ip\big)$ in (4.13) modulo p^{2i+1}. This allows us to use Lemma 14 with e replaced by $2i + 1$. The corresponding substitution in (4.13) gives

$$\begin{aligned} u(n) \equiv \Pi_1(n) - \sum_{i=0}^{(e-1)/2} \binom{ep}{(2i+1)p} &\Pi_3\big(n - \tfrac{p-1}{2} - ip\big) \\ \cdot \sum_{k\ge 0} \sum_{i=\alpha_0>\alpha_1>\cdots>\alpha_k\ge 0} &(-1)^k \Pi_1\left(\tfrac{p-1}{2} + \alpha_k p\right) \\ &\cdot \prod_{j=0}^{k-1} \binom{(2\alpha_j+1)p}{(2\alpha_{j+1}+1)p} \Pi_3\big((\alpha_j - \alpha_{j+1})p\big) \pmod{p^e}. \end{aligned} \tag{4.14}$$

We have

$$\Pi_3\big(n - \tfrac{p-1}{2} - ip\big) = \Pi_3\big(\tfrac{ep-2i-1}{2}\big) \prod_{j=\frac{(e-2i-1)p}{2}+1}^{n-\frac{p-1}{2}-ip} (4j-3)^2. \tag{4.15}$$

Moreover, by (4.1), and remembering that $i = \alpha_0$, we get

$$\begin{aligned} v_p\left(\Pi_3\big(\tfrac{(e-2i-1)p}{2}\big)\Pi_1\left(\tfrac{p-1}{2} + \alpha_k p\right) \prod_{j=0}^{k-1} \Pi_3\big((\alpha_j - \alpha_{j+1})p\big)\right) \\ \ge (e - 2i - 1) + 2\alpha_k + \sum_{j=0}^{k-1} 2(\alpha_j - \alpha_{j+1}) = e - 1. \end{aligned}$$

This allows us to consider the product on the right-hand side of (4.15) modulo p, once that equation is substituted in (4.14). The result then is

$$u(n) \equiv \Pi_1(n) - \left(\prod_{j=1}^{n-\frac{ep-1}{2}} (4j-3)^2 \right) \sum_{i=0}^{(e-1)/2} \binom{ep}{(2i+1)p} \Pi_3\big(\tfrac{(e-2i-1)p}{2}\big) \cdot \sum_{k\ge 0} \sum_{i=\alpha_0>\alpha_1>\cdots>\alpha_k\ge 0} (-1)^k \Pi_1\left(\tfrac{p-1}{2}+\alpha_k p\right) \cdot \prod_{j=0}^{k-1} \binom{(2\alpha_j+1)p}{(2\alpha_{j+1}+1)p} \Pi_3\big((\alpha_j-\alpha_{j+1})p\big) \pmod{p^e}. \tag{4.16}$$

Here we see that, in the sum, for $k \ge 1$ the term for

$$i = \tfrac{e-1}{2} = \alpha_0 > \alpha_1 > \cdots > \alpha_k \ge 0$$

cancels with the term for

$$\tfrac{e-1}{2} > \alpha'_0 > \alpha'_1 > \cdots > \alpha'_{k-1} \ge 0,$$

where $\alpha'_j = \alpha_{j+1}$ for $j = 0, 1, \dots, k-1$. After this cancellation, the only remaining term in the sum is the one for $k = 0$ and $\alpha_0 = \frac{e-1}{2}$. In this regard, we have

$$\left(\prod_{j=1}^{n-\frac{ep-1}{2}} (4j-3)^2 \right) \Pi_1\left(\tfrac{p-1}{2}+\alpha_0 p\right) \equiv \left(\prod_{j=1}^{n-\frac{ep-1}{2}} (4j+2p+4\alpha_0 p-3)^2 \right) \Pi_1\left(\tfrac{p-1}{2}+\alpha_0 p\right) \equiv \Pi_1(n) \pmod{p^e}$$

since, again using (4.1),

$$v_p\left(\Pi_1\left(\tfrac{p-1}{2}+\alpha_0 p\right)\right) = v_p\left(\Pi_1\left(\tfrac{p-1}{2}+\tfrac{e-1}{2}p\right)\right) \ge e-1.$$

Consequently, this term cancels with the first term on the right-hand side of (4.16).

This concludes the induction step, and hence the proof of the theorem is now complete. ☐

Remark 12. An examination of the above arguments (including the proofs of Lemmas 13 and 14 which are used in the above proof) reveals that the products $\Pi_1(n)$ and $\Pi_3(n)$ in the definition (2.4) could have been replaced with any functions $f(n)$ and $g(n)$ that satisfy the p-divisibility properties in (4.1) and (4.2), and where $f(n)$ is a quadratic residue modulo p not divisible by p.

Lemma 13. *We assume that, given a prime $p \equiv 1 \pmod 4$ and an odd positive integer e, the number $u(n)$ is divisible by p^h for $n \ge \lceil \frac{hp}{2} \rceil$ and $h < e$. Then*

$$u\left(\tfrac{ep-1}{2}\right) \equiv \Pi_1\left(\tfrac{ep-1}{2}\right) - \sum_{i=1}^{(e-1)/2} \binom{ep}{2ip} \Pi_3(ip)\, u\big(\tfrac{ep-1}{2}-ip\big) \pmod{p^e}. \tag{4.17}$$

Proof. We put $n = \frac{ep-1}{2}$ in (2.4) and consider the summand indexed by m on the right-hand side for $\left\lceil \frac{(f-1)p}{2} \right\rceil \le m < \left\lceil \frac{fp}{2} \right\rceil$ with $1 \le f \le e$. By our assumption on the divisibility of $u(m)$ by powers of p and by (4.2), we have

$$v_p\left(\big(\Pi_3\big(\tfrac{ep-1}{2}-m\big)\big)u(m)\right) \ge 2\left\lfloor \frac{\frac{ep-1}{2}-m+\frac{3}{4}(p-1)}{p} \right\rfloor + f - 1.$$

Our conditions imply $\frac{ep-1}{2} - m \ge \frac{ep-1}{2} - \lceil \frac{fp}{2} \rceil + 1 \ge \left\lceil \frac{(e-f)p}{2} \right\rceil$. Therefore, we obtain

$$v_p\left(\left(\Pi_3\left(\tfrac{ep-1}{2}-m\right)\right)u(m)\right) \ge 2\left\lfloor \frac{\left\lceil \frac{(e-f)p}{2}\right\rceil + \frac{3}{4}(p-1)}{p} \right\rfloor + f - 1 \ge (e-f)+f-1 = e-1.$$

In order to show that the summand is indeed divisible by p^e for m not of the form $\frac{ep-1}{2} - ip = \frac{p-1}{2} + \frac{e-2i-1}{2}p$ for some i, we must therefore prove that the binomial coefficient in (2.4) is divisible by p in this case. To see this, we consider the p-adic representations of $2m+1$ and $ep-1-2m$. Since m is not of the form $\frac{p-1}{2} + sp$ (this condition is essential for the first line below), these are

$$\begin{aligned} (2m+1)_p &= (f-1)_p \, * \\ \big(ep-1-2m\big)_p &= (e-f)_p \, * \end{aligned} \tag{4.18}$$

As before, $(\alpha)_p$ denotes the p-adic representation of the integer α, and the stars on the right-hand sides indicate the right-most digits of $(2m+1)_p$ and $(ep-1-2m)_p$ whose precise values are irrelevant. The sum of $2m+1$ and $ep-1-2m$ is ep whose p-adic representation has the form $(e)_p \, *$. Hence, when adding the two numbers on the right-hand sides of (4.18), at least one carry must occur — namely one from the p^0-digit to the p^1-digit. By Kummer's theorem in Lemma 4, the consequence is that the binomial coefficient $\binom{ep}{2m+1}$ is divisible by p. Therefore the corresponding summand is divisible by p^e.

This proves that, under our assumptions, the only summands which "survive" on the right-hand side of (2.4) modulo p^e are those for which m is of the form $\frac{p-1}{2} + sp$ for some s. This leads directly to (4.17). □

By iteration of the recurrence in (4.17), we obtain the following non-recursive congruence.

Lemma 14. *Under the assumptions of Lemma* 13, *we have*

$$u\left(\tfrac{ep-1}{2}\right) \equiv \sum_{k\ge 0} \sum_{\frac{e-1}{2}=\alpha_0>\alpha_1>\dots>\alpha_k\ge 0} (-1)^k \Pi_1\left(\tfrac{p-1}{2}+\alpha_k p\right) \cdot \prod_{j=0}^{k-1} \binom{(2\alpha_j+1)p}{(2\alpha_{j+1}+1)p} \Pi_3\big((\alpha_j-\alpha_{j+1})p\big) \pmod{p^e}. \tag{4.19}$$

Proof. We show the claim by an induction on e. For the start of the induction, we observe that for $e=1$ the sum on the right-hand side of (4.19) reduces to a single term for $k=0$ and $\alpha_0=0$, which turns out to equal $u(\frac{p-1}{2})$, in agreement with the claim.

For the induction step, we observe that, by (4.1), we have $v_p\big(\Pi_3(ip)\big) \ge 2i$. Hence we may consider the term $u\left(\frac{ep-1}{2} - ip\right)$ in (4.17) modulo p^{e-2i}. This allows us to substitute the right-hand side of (4.19) for e replaced by $e-2i$ in (4.17). If, at the same time, we replace α_j by α_{j+1} for all j, then this leads us to

$$u\left(\tfrac{ep-1}{2}\right) \equiv \Pi_1\left(\tfrac{ep-1}{2}\right) - \sum_{i=1}^{(e-1)/2} \binom{ep}{(e-2i)p} \Pi_3(ip) \sum_{k\ge0} \sum_{\frac{e-1}{2}-i=\alpha_1>\alpha_2>\cdots>\alpha_{k+1}\ge0} (-1)^k \Pi_1\left(\tfrac{p-1}{2}+\alpha_{k+1}p\right) \cdot \prod_{j=1}^{k} \binom{(2\alpha_j+1)p}{(2\alpha_{j+1}+1)p} \Pi_3\big((\alpha_j-\alpha_{j+1})p\big) \pmod{p^e}.$$

Setting $\alpha_0 = \frac{e-1}{2}$, we realise that the right-hand side can be put together in the form of the expression on the right-hand side of (4.19) with k replaced by $k+1$. This concludes the induction step and, hence, the induction argument. □

5. The sequence $(v(n))_{n\ge0}$ modulo odd prime powers

Here, we analyse the numbers $v(n)$ modulo odd prime powers p^e. The first result is Theorem 17 which says that $v(n)$ vanishes modulo p^e for $n \ge \lceil (e-1)p^2/2 \rceil$, for all odd primes and all integers $e \ge 2$. Also here, the proof of the theorem is inductive, the start of the induction being given in Proposition 16, which is itself based on auxiliary results in Lemma 15. Again, should the prime p be congruent to 1 modulo 4, Theorem 17 can be significantly improved; see Theorem 19.

We begin with the announced auxiliary results, which afterwards lead to Proposition 16.

Lemma 15. *Let p be an odd prime number, and let $(v(n))_{n\ge0}$ be defined by the recurrence* (2.6)*. Then we have*

$$v(ap+b) \equiv 0 \pmod p, \quad \text{for } 1 \le a \le \tfrac{p-1}{2} \text{ and } 0 \le b \le a-1, \tag{5.1}$$

and

$$v\left(ap+\tfrac{p+1}{2}+b\right) \equiv 0 \pmod p, \quad \text{for } 1 \le a \le \tfrac{p-1}{2} \text{ and } 0 \le b \le a-1. \tag{5.2}$$

Proof. We prove the assertions by induction on the size of $ap+b$ and of $ap+\frac{p+1}{2}+b$, simultaneously. The induction is based on the recurrence (2.6). It is clear that the first term on the right-hand side, the product $2^{n-1}\Pi_3(n) = 2^{n-1}\Pi_3(ap+b)$, is divisible by p because of (4.1).

Now let first $n = ap+b$ with a and b satisfying the conditions in (5.1). We want to prove that $v(n) \equiv 0 \pmod p$.

From Lemma 4 we infer that the binomial coefficient $\binom{2n}{2m} = \binom{2ap+2b}{2m}$ is divisible by p, except when $2m = cp+d$ with both $0 \le c \le 2a$ and $0 \le d \le 2b$. It is important to note that at this point the upper bounds of $\frac{p-1}{2}$ for a and b enter crucially.

If $c = 0$ (and hence d even since $2m = cp+d = d$), then $v(n-m) = v\left(ap+b-\frac{d}{2}\right)$ is divisible by p according to the induction hypothesis. From now on we may assume that $c \ge 1$.

We distinguish whether c and d are both even or both odd. (There are no other cases since $2m = cp+d$ is even.)

If both c and d are even, then, provided $c > d$, we may use the induction hypothesis (5.1) to infer that $v(m) = v\left(\frac{c}{2}p + \frac{d}{2}\right)$ is divisible by p. On the other hand, if $c \le d$, then we have

$$n - m = \left(a - \tfrac{c}{2}\right)p + b - \tfrac{d}{2}.$$

Since, by assumption, we have $a > b$, we have

$$a - \tfrac{c}{2} > b - \tfrac{d}{2} \ge 0.$$

Consequently, again using the induction hypothesis (5.1), we obtain that $v(n-m)$ is divisible by p.

Now let both c and d be odd. Here we may rewrite $m = \frac{c}{2}p + \frac{d}{2}$ as

$$m = \tfrac{c-1}{2}p + \tfrac{p+1}{2} + \tfrac{d-1}{2}.$$

Furthermore, we may write

$$n - m = \left(a - \tfrac{c+1}{2}\right)p + \tfrac{p+1}{2} + b - \tfrac{d+1}{2}.$$

It should be noted that, if $c \le d$, we have $a - \frac{c+1}{2} > b - \frac{d+1}{2} \ge 0$. As a consequence, by the induction hypothesis (5.2), we have $v(n-m) \equiv 0 \pmod p$. If, on the other hand, we have $c \ge d$, then $v(m) \equiv 0 \pmod p$, again by the induction hypothesis (5.2).

Next we discuss the case where $n = ap + \frac{p+1}{2} + b$ with a and b satisfying the conditions in (5.2). We want to prove that $v(n) \equiv 0 \pmod p$.

In the current case, the binomial coefficient on the right-hand side of (2.6) becomes $\binom{2n}{2m} = \binom{(2a+1)p+2b+1}{2m}$. Here it must be observed that, because of the upper bounds on a and b in (5.2), we have $2a+1 \le p$ and $2b+1 \le p-1$. If $a = \frac{p-1}{2}$, so that $2a+1 = p$, then, by Lemma 4, $\binom{2n}{2m} = \binom{p^2+2b+1}{2m}$ is divisible by p, except when $2 \le 2m \le 2b$. In this exceptional case, we have $v(n-m) \equiv 0 \pmod p$ by induction hypothesis.

We assume from now on that $a < \frac{p-1}{2}$. From Lemma 4 we infer that the binomial coefficient $\binom{2n}{2m} = \binom{(2a+1)p+2b+1}{2m}$ is divisible by p, except when $2m = cp + d$ with both $0 \le c \le 2a+1$ and $0 \le d \le 2b+1$.

We distinguish whether c and d are both even or both odd. (There are no other cases since $2m = cp + d$ is even.)

If both c and d are even, then, provided $c > d$, we may use the induction hypothesis (5.1) to infer that $v(m) = v\left(\frac{c}{2}p + \frac{d}{2}\right)$ is divisible by p. On the other hand, if $c \le d$, then we have

$$n - m = \left(a - \tfrac{c}{2}\right)p + \tfrac{p+1}{2} + b - \tfrac{d}{2}.$$

Since, by assumption, we have $a > b$, we have

$$a - \tfrac{c}{2} > b - \tfrac{d}{2} \ge 0.$$

Consequently, using the induction hypothesis (5.2), we obtain that $v(n-m)$ is divisible by p.

Now let both c and d be odd. We may again rewrite $m = \frac{c}{2}p + \frac{d}{2}$ as

$$m = \tfrac{c-1}{2}p + \tfrac{p+1}{2} + \tfrac{d-1}{2}.$$

Furthermore, we may write

$$n - m = \left(a - \tfrac{c-1}{2}\right)p + b - \tfrac{d-1}{2}.$$

Hence, according to the induction hypothesis (5.2), we have $v(m) \equiv 0 \pmod p$ if $c > d$, and otherwise we have $v(n-m) \equiv 0 \pmod p$ according to the induction hypothesis (5.1). ☐

Proposition 16. *Let $(v(n))_{n\ge 0}$ be defined by the recurrence* (2.6)*. Then, given an odd prime p, the number $v(n)$ is divisible by p^2 for $n \ge \left\lceil \frac{p^2}{2} \right\rceil$.*

Proof. Let $n \ge \left\lceil \frac{p^2}{2} \right\rceil = \frac{p^2+1}{2}$. Again we use induction on n. The induction will be based on (2.6), and it proceeds by showing that each summand on the right-hand side is divisible by p^2.

It is again clear that the first term on the right-hand side, the product $\Pi_3(n) = \Pi_3(ap+b)$, is divisible by p^2 because of (4.1).

In the sequel, we may restrict our attention to $n < p^2$ because otherwise either $m \ge \frac{p^2+1}{2}$ or $n - m \ge \frac{p^2+1}{2}$. The induction hypothesis then implies that either $v(m) \equiv 0 \pmod{p^2}$ or $v(n-m) \equiv 0 \pmod{p^2}$, and therefore each term on the right-hand side of (2.6) would be divisible by p^2.

To summarise the discussion so far: we may write $2n$ as $2n = p^2 + ap + b$ for some a and b not of the same parity and with $0 \le a, b \le p-1$.

If there are two carries when adding $2m$ and $2(n-m)$ in their p-adic representations, then, by Lemma 4, the binomial coefficient $\binom{2n}{2m}$ is divisible by p^2. Hence the corresponding summand on the right-hand side of (2.6) is divisible by p^2.

Now let us assume that there is only one carry when adding $2m$ and $2(n-m)$ in their p-adic representations. As earlier, if either m or $n-m$ is larger than $\frac{p^2}{2}$, then $v(m)$ or $v(n-m)$ is divisible by p^2, and thus as well the corresponding summand on the right-hand side of (2.6). We may therefore assume without loss of generality that $2m = cp + d$ with $c \le \frac{p-1}{2}$. Furthermore, we have $d \le b$ since, otherwise, there would be two carries when adding $2m$ and $2n - 2m$ in their p-adic representations.

We distinguish again whether c and d are both even or both odd.

Let first c and d be even. We write $m = \frac{c}{2}p + \frac{d}{2}$. If $c > d$, then, by (5.1), we infer $v(m) \equiv 0 \pmod p$. If $c \le d$, then we may write

$$n - m = \left(\tfrac{p+a-c}{2}\right)p + \tfrac{b-d}{2} = \left(\tfrac{p+a-c-1}{2}\right)p + \tfrac{p+1}{2} + \tfrac{b-d-1}{2}.$$

We use one of the two expressions, depending on the parities of a and b (the reader should recall that a and b have different parities), so that the fractions produce integers. By our assumptions, we have

$$\tfrac{p+a-c}{2} > \tfrac{b+a-c}{2} \ge \tfrac{b-c}{2} \ge \tfrac{b-d}{2} \ge 0.$$

By Lemma 15, this implies that $v(n-m) \equiv 0 \pmod p$. In total, in both cases this shows that the corresponding summand in (2.6) is divisible by p^2.

Now let c and d be odd. Here we write $m = \frac{c-1}{2}p + \frac{p+1}{2} + \frac{d-1}{2}$. If $c > d$, then by (5.2), we infer $v(m) \equiv 0 \pmod p$. If $c \le d$, then we may again write

$$n - m = \left(\tfrac{p+a-c}{2}\right)p + \tfrac{b-d}{2} = \left(\tfrac{p+a-c-1}{2}\right)p + \tfrac{p+1}{2} + \tfrac{b-d-1}{2}.$$

Arguing as before, we conclude that $v(n-m) \equiv 0 \pmod p$. This shows again that the corresponding summand in (2.6) is divisible by p^2.

If there is no carry when adding $2m$ and $2(n-m)$ in their p-adic representations, then necessarily one of $2m$ or $2(n-m)$ is at least p^2+1. So, again, one of $v(m)$ or $v(n-m)$ is divisible by p^2 due to the induction hypothesis.

This completes the proof of the proposition. $\square$

The following theorem proves Conjecture 18(1) in [13] for $v(n)$.

Theorem 17. *Let $(v(n))_{n\ge 0}$ be defined by the recurrence* (2.6). *Then, given an odd prime p and a positive integer $e\ge 2$, the number $v(n)$ is divisible by p^e for $n\ge \left\lceil \frac{(e-1)p^2}{2}\right\rceil$.*

Proof. In analogy with the proof of Theorem 9, we proceed by a double induction on e and n, the outer induction being on e. For the start of the induction, we use Proposition 16 which proves the assertion of the theorem for $e=2$. From now on let $e\ge 3$.

We assume that $\left\lceil \frac{(e-1)p^2}{2}\right\rceil \le n < \left\lceil \frac{ep^2}{2}\right\rceil$. We claim that the first term on the right-hand side of (2.6), namely $2^{n-1}\Pi_3(n)$, is always divisible by p^e under this assumption. Indeed, by (4.1) we have

$$v_p\left(2^{n-1}\Pi_3(n)\right)\ge 2\left\lfloor \tfrac{n}{p}\right\rfloor \ge 2\left\lfloor \tfrac{1}{p}\left\lceil \tfrac{(e-1)p^2}{2}\right\rceil\right\rfloor \ge 2\left\lfloor \tfrac{(e-1)p}{2}\right\rfloor \ge 2(e-1)\ge e$$

for $e\ge 3$.

Next we consider the summand on the right-hand side of (2.6) for $\left\lceil \frac{(f-1)p^2}{2}\right\rceil \le m < \left\lceil \frac{fp^2}{2}\right\rceil$ with $2\le f\le e-2$. By the induction hypothesis applied to $v(m)$, we have $v_p(v(m))\ge f$. Furthermore we have

$$n-m > \left\lceil \tfrac{(e-1)p^2}{2}\right\rceil - \left\lceil \tfrac{fp^2}{2}\right\rceil = \left\lceil \tfrac{(e-f-1)p^2}{2}\right\rceil - \chi(e,f\text{ odd}),$$

where $\chi(\mathcal{A})=1$ if $\mathcal{A}$ is true and $\chi(\mathcal{A})=0$ otherwise. The above inequality implies

$$n-m\ge \left\lceil \tfrac{(e-f-1)p^2}{2}\right\rceil .$$

Therefore, if we apply the induction hypothesis to $v(n-m)$, then we obtain $v_p(v(n-m))\ge e-f$. We infer that $v_p\big(v(m)v(n-m)\big)\ge f+(e-f)=e$, and hence the corresponding summand in (2.6) is divisible by p^e.

Let now $0\le m<\left\lceil \frac{p^2}{2}\right\rceil$. In that case, the previous argument only shows that $n-m\ge \left\lceil \frac{(e-2)p^2}{2}\right\rceil$, with the consequence that we only have $v_p(v(n-m))\ge e-1$. It might be that actually $n-m\ge \left\lceil \frac{(e-1)p^2}{2}\right\rceil$. Then the induction hypothesis (in n) implies that $v_p(v(n-m))\ge e$, so that the corresponding summand in (2.6) is divisible by p^e. On the other hand, if $\left\lceil \frac{(e-2)p^2}{2}\right\rceil \le n-m < \left\lceil \frac{(e-1)p^2}{2}\right\rceil$, then we may write $2n=(e-1)p^2+ap+b$ and $2(n-m)=(e-2)p^2+cp+d$ for some a,b,c,d with $0\le a,b,c,d\le p-1$. Then there is (at least) one carry when adding $2(n-m)$ and $2m$ in their p-adic representations. Therefore, by Lemma 4, the binomial coefficient $\binom{2n}{2m}$ is divisible by p, and together with the previously observed fact that $v_p(v(n-m))\ge e-1$ this shows that the corresponding summand in (2.6) is divisible by p^e.

Finally, let $\left\lceil\frac{(e-2)p^2}{2}\right\rceil \le m < \left\lceil\frac{(e-1)p^2}{2}\right\rceil$. The induction hypothesis (in n) implies that in this case we have $v_p(v(m)) \ge e-1$. If $n-m \ge \left\lceil\frac{p^2}{2}\right\rceil$, then the induction hypothesis (in n) implies that $v(n-m)$ is divisible by p^2, so that the corresponding summand in (2.6) is divisible by p^e. On the other hand, if $0 \le n-m < \left\lceil\frac{p^2}{2}\right\rceil$, then we may write $2n = (e-1)p^2 + ap + b$ and $2m = (e-2)p^2 + cp + d$ for some a, b, c, d with $0 \le a, b, c, d \le p-1$. Then there is (at least) one carry when adding $2(n-m)$ and $2m$ in their p-adic representations. Therefore, by Lemma 4, the binomial coefficient $\binom{2n}{2m}$ is divisible by p, and together with the previously observed fact that $v_p(v(m)) \ge e-1$ this shows that the corresponding summand in (2.6) is divisible by p^e.

This concludes the induction step, and, thus, the proof of the theorem. □

Remark 18. An examination of the above arguments reveals that the product $\Pi_3(n)$ in the definition (2.6) could have been replaced with any function $f(n)$ that satisfies the p-divisibility property in (4.1).

Theorem 19. *Let $(v(n))_{n\ge0}$ be defined by the recurrence* (2.6)*. Then, given a prime $p \equiv 1 \pmod 4$ and a positive integer e, the number $v(n)$ is divisible by p^e for $n \ge \left\lceil\frac{ep}{2}\right\rceil$.*

Proof. In analogy with the proof of Theorem 9, we proceed by a double induction on e and n, the outer induction being on e. Clearly, the theorem is trivial for $e = 0$, which serves as the start of the induction.

Now let $n \ge \left\lceil\frac{ep}{2}\right\rceil$. Hence, by (4.2) for $n \ge \lceil ep/2\rceil$ we have

$$v_p\big(\Pi_3(n)\big) \ge 2\left\lfloor\frac{\left\lceil\frac{ep}{2}\right\rceil + \frac{3}{4}(p-1)}{p}\right\rfloor \ge 2\left\lfloor\frac{e}{2} + \frac{3}{4} - \frac{3}{4p}\right\rfloor \ge e.$$

Thus, the first term on the right-hand side of (2.6) is divisible by p^e.

We consider the summand on the right-hand side of (2.6) for $\left\lceil\frac{fp}{2}\right\rceil \le m < \left\lceil\frac{(f+1)p}{2}\right\rceil$ with $0 \le f < e$. By the induction hypothesis applied to $v(m)$, we have $v_p(v(m)) = f$. On the other hand, if we apply the induction hypothesis to $v(n-m)$, then we obtain $v_p(v(n-m)) = e-f-1$ or $v_p(v(n-m)) = e-f$, depending on whether or not $n-m < \left\lceil\frac{(e-f)p}{2}\right\rceil$. In the latter case, we infer that $v_p\big(v(m)v(n-m)\big) = f + (e-f) = e$, and hence the corresponding summand in (2.6) is divisible by p^e.

On the other hand, in the former case, the conclusion is that $v_p\big(v(m)v(n-m)\big) = e-1$. In order to show that the corresponding summand is divisible by p^e, we must therefore prove that the binomial coefficient in (2.6) is divisible by p in this case. To see this, we consider the p-adic representations of $2m$ and $2(n-m)$. These are

$$\begin{aligned}(2m)_p &= \qquad (f)_p * \\ \big(2(n-m)\big)_p &= (e-f-1)_p * \end{aligned} \tag{5.3}$$

Here as before, $(\alpha)_p$ denotes the p-adic representation of the integer α, and the stars on the right-hand sides indicate the right-most digits of $(2m)_p$ and $(2(n-m))_p$ whose precise values are irrelevant. The sum of $2m$ and $2(n-m)$ is $2n$ whose p-adic representation has the form $(e)_p *$. Hence, when adding the two numbers on the right-hand sides of (5.3), at least one carry must occur — namely one from the p^0-digit to the p^1-digit. By

Kummer's theorem in Lemma 4, the consequence is that the binomial coefficient $\binom{2n}{2m}$ is divisible by p. Therefore, again, the corresponding summand is divisible by p^e.

Finally, if $\left\lceil \frac{ep^2}{2} \right\rceil \le m < n$, by the induction hypothesis (for n), the number $v(m)$ is divisible by p^e, which of course implies divisibility of the corresponding summand by p^e.

This concludes the induction step, and, thus, the proof of the theorem. □

Remark 20. An examination of the above arguments reveals that the product $\Pi_3(n)$ in the definition (2.6) could have been replaced with any function $f(n)$ that satisfies the p-divisibility property in (4.2).

6. The inverse of the matrix $\mathbf{R}$ modulo prime powers p^e with $p \equiv 3 \pmod 4$

The goal of this section is to derive a divisibility result for the matrix entries $R^{-1}(n,k)$ by prime powers p^e with $p \equiv 3$ (mod 4) that would allow us to carry through an inductive proof of Theorem 1(1) via the use of the relation (2.12). This result is presented in Theorem 22. It is based on Proposition 21 which is stated and proved before.

We start by deriving an explicit expression for $R^{-1}(2n,2k)$, the other entries of the matrix $\mathbf{R}^{-1} = (R^{-1}(n,k))_{n,k\ge 0}$ being zero due to the checkerboard pattern of the matrix; cf. Proposition 2. By the definition (2.11), we have

$$
\begin{aligned}
R^{-1}(2n,2k) &= 2^{n-k}\frac{(2n-1)!}{(2k-1)!}\left\langle t^{2n-2k}\right\rangle \big(U(t)/t\big)^{-2n}\\
&= 2^{n-k}\frac{(2n-1)!}{(2k-1)!}\left\langle t^{2n-2k}\right\rangle \sum_{m\ge 0}\binom{-2n}{m}\big(U(t)/t-1\big)^{m}\\
&= 2^{n-k}\frac{(2n-1)!}{(2k-1)!}\left\langle t^{2n-2k}\right\rangle \sum_{m\ge 0}(-1)^m\binom{2n+m-1}{m}\left(\sum_{j\ge 1}\frac{u(j)}{(2j+1)!}t^{2j}\right)^{m}\\
&= 2^{n-k}\frac{(2n-1)!}{(2k-1)!}\sum_{m\ge 0}(-1)^m\binom{2n+m-1}{m}\\
&\qquad\cdot \sum_{\substack{(c_i)\in\mathcal{P}^o_{2n-2k+m,m}\\ c_1=0}}\frac{m!}{3!^{c_3}c_3!\,5!^{c_5}c_5!\cdots(2n-2k+1)!^{c_{2n-2k+1}}c_{2n-2k+1}!}\prod_{i=1}^{2n-2k+1}u^{c_i}\left(\tfrac{i-1}{2}\right)\\
&= \sum_{m\ge 0}\sum_{\substack{(c_i)\in\mathcal{P}^o_{2n-2k+m,m}\\ c_1=0}}(-1)^m 2^{n-k}\frac{(2n+m-1)!}{(2k-1)!\,\prod_{i=1}^{2n-2k+1}i!^{c_i}c_i!}\prod_{i=1}^{2n-2k+1}u^{c_i}\left(\tfrac{i-1}{2}\right).
\end{aligned}
\tag{6.1}
$$

Here, the symbol $\mathcal{P}^o_{N,K}$ stands for the set of all tuples $(c_1,c_2,\dots,c_N)$ of non-negative integers c_i for which $c_{2j}=0$ for all j, and which satisfy

$$c_1+c_3+\dots+c_{2n-1}=K, \tag{6.2}$$

$$c_1+3c_3+\dots+(2n-1)c_{2n-1}=N, \tag{6.3}$$

with $n = \lceil N/2 \rceil$. It should be noted that, if N and K do not have the same parity, then the set $\mathcal{P}^o_{N,K}$ is empty.

The next proposition provides a lower bound on the p-divisibility of (the essential part of) the summand on the right-hand side of (6.1).

Proposition 21. *Let n, k, m, e, f be positive integers with $n \ge k$, and let p be a prime number with $p \equiv 3 \pmod 4$. If $2n \ge ep^2$, $(f-1)p^2 \le 2k-1 < fp^2$, and $(c_i) \in \mathcal{P}^o_{2n-2k+m,m}$ with $c_1 = 0$, then the expression*

$$F(n,k,m,(c_i)) := \frac{(2n+m-1)!}{(2k-1)!\prod_{i=1}^{2n-2k+1} i!^{c_i}\, c_i!} \prod_{i=1}^{2n-2k+1} u^{c_i}\big(\tfrac{i-1}{2}\big) \tag{6.4}$$

is divisible by p^{e-f+1}. Furthermore, if $f = 1$, then the above expression multiplied by $v(k)$ is divisible by p^{e+1}.

Proof. As a consequence of Kummer's theorem in Lemma 4 (the multinomial coefficient below can be written as a product of binomial coefficients), we have

$$v_p\left(\frac{(2n+m-1)!}{(2k-1)!\prod_{i=1}^{2n-2k+1} i!^{c_i}}\right) = \#\big(\text{carries when performing the addition } (2k-1) + \textstyle\sum_{i=1}^{2n-2k+1} c_i \cdot i\big). \tag{6.5}$$

Here, "performing the addition $(2k-1) + \sum_{i=1}^{2n-2k+1} c_i \cdot i$" means that we start with $(2k-1)_p$ (the p-adic representation of $2k-1$), then add $(1)_p$ to it c_1 many times, then add $(3)_p$ to it c_3 many times (the reader should recall that even-indexed c_i's are zero by definition of $\mathcal{P}^o_{2n-2k+m,m}$), etc. Carries are recorded at each single addition. Moreover, we have

$$v_p\big(u\big(\tfrac{i-1}{2}\big)\big) \ge \begin{cases} \left\lfloor \frac{i}{p^2} \right\rfloor + 1, & \text{for } i \ge p^2, \\ 1, & \text{for } i = ap+b \text{ with } 1 \le a \le p-1 \text{ and } 0 \le b < a, \end{cases}$$

the first alternative being due to Theorem 9, and the second alternative being due to Lemma 7.

Combining the last inequality with (6.5), we obtain

$$\begin{aligned} &v_p\big(F(n,k,m,(c_i))\big) \\ &\quad\ge \#\big(\text{carries when performing the addition } (2k-1) + \textstyle\sum_{i=1}^{2n-2k+1} c_i \cdot i\big) \\ &\qquad - \sum_{i=1}^{2n-2k+1} v_p(c_i!) + \sum_{i=p^2}^{2n-2k+1} c_i \cdot \left(\left\lfloor \frac{i}{p^2} \right\rfloor + 1\right) + {\sum}' c_i, \end{aligned} \tag{6.6}$$

where $\sum'$ is over all odd i with $1 \le i < p^2$ and $i = ap+b$ for some a and b with $1 \le a \le p-1$ and $0 \le b < a$.

We begin with the negative term in (6.6), namely $-\sum_{i=1}^{2n-2k+1} v_p(c_i!)$. By Legendre's formula in Lemma 3, we have $v_p(c_i!) \le \frac{c_i}{p-1}$, so that

$$-\sum_{i=1}^{2n-2k+1} v_p(c_i!) \ge -\sum_{i=1}^{2n-2k+1} \frac{c_i}{p-1} = -\frac{m}{p-1},$$

the last step being due to the fact that the tuple (c_i) is in $\mathcal{P}^o_{2n-2k+m,m}$. To compensate this term, we consider the p^0-digits of $i_1, i_2, \dots, i_m$, the carries that they cause in the addition $i_1 + i_2 + \cdots + i_m$, and contributions from $\sum' c_i$ on the right-hand side of (6.6). Let us assume that exactly t of the i_ℓ's are $\equiv 0, 1 \pmod p$. Then we get

$$\#\Big(\text{carries from the } p^0\text{-digit to the } p^1\text{-digit when doing the addition } \sum_{i=1}^{2n-2k+1} c_i \cdot i\Big) \\ + {\sum}' c_i - \sum_{i=1}^{2n-2k+1} v_p(c_i!) \ge \left\lfloor \tfrac{2(m-t)}{p} \right\rfloor + t - \tfrac{m}{p-1} \ge \left\lfloor \tfrac{2m}{p} \right\rfloor - \tfrac{m}{p-1} \ge 0 \quad (6.7)$$

as long as $m \ge p$. However, if $m < p$, then the sum $\sum_{i=1}^{2n-2k+1} v_p(c_i!)$ equals zero, so that the left-hand side in (6.7) is also non-negative in this case.

For the next step, in order to ease notation, let

$$(i_1, i_2, \dots, i_m) = (3^{c_3}, 5^{c_5}, \dots),$$

where i^{c_i} stands for the sequence $i, i, \dots, i$, with i repeated c_i times. We assume that $j_\ell p^2 \le i_\ell < (j_\ell + 1)p^2$ for all ℓ. Then, when concentrating on the p^2-digit in the p-adic representations of $2n + m - 1$, $2k - 1$, i_1, i_2, $\dots$, i_m while performing the addition described on the right-hand side of (6.5), namely

$$(2k - 1) + i_1 + i_2 + \cdots + i_m \quad (6.8)$$

(resulting in $2n + m - 1$), we may extract the inequality

$$(f - 1) + j_1 + j_2 + \cdots + j_m + C \ge e, \quad (6.9)$$

where C is the number of carries from the p^1- to the p^2-digit when performing the addition (6.8).

If we now use (6.7) and (6.9) in (6.6), then we obtain

$$v_p\big(F(n, k, m, (c_i))\big) \ge C + \sum_{i=p^2}^{2n-2k+1} c_i \cdot \Big(\left\lfloor \tfrac{i}{p^2} \right\rfloor + 1 \Big) \\ \ge \big(e - (f - 1) - j_1 - j_2 - \cdots - j_m\big) + j_1 + j_2 + \cdots + j_m = e - f + 1. \quad (6.10)$$

Finally we address the case where $f = 1$. The previous arguments show that

$$v_p\big(F(n, k, m, (c_i))\big) \ge e.$$

Hence, the task is to find — so-to-speak — an additional $+1$ somewhere, which may also come from $v_p(v(k))$.

Inspection of (6.10) shows that, using the earlier notation, we gain such an additional $+1$ whenever one of the i_ℓ's is at least p^2 since in the inequality (6.10) we dropped the $+1$ in $\Big(\left\lfloor \frac{i}{p^2} \right\rfloor + 1 \Big)$ on the right-hand side. Hence, from now on, we may assume that $i_\ell < p^2$ for all ℓ.

We may furthermore assume $m < p$ because for $m \ge p$ we have actually strict inequality in (6.7) thereby having again found an additional $+1$. In particular, as already remarked earlier, the restriction $m < p$ implies that the sum $\sum_{i=1}^{2n-2k+1} v_p(c_i!)$

equals zero so that the argument in (6.7) is not required, and consequently no carries from the p^0-digit to the p^1-digit need to be considered at this point.

Since in the current case $2k-1 < p^2$, from (6.9) we deduce that the number C of carries from before is at least e. If there is an i_ℓ of the form $i_\ell = ap+b$ with $1 \le a \le p-1$ and $0 \le b < a$, then we get an additional $+1$ from $\sum' c_i$ in (6.6). If $k = ap+b$ or $k = ap+\frac{p+1}{2}+b$ with $1 \le a \le \frac{p-1}{2}$ and $1 \le b < a$ so that $2k-1 = Ap+B$ with $2 \le A \le p-1$ and $0 \le B \le A-3$ then $v_p(v(k)) \ge 1$ by Lemma 15. Therefore the remaining case to discuss is when $i_\ell = a_\ell p + b_\ell$ with $a_\ell \le b_\ell$, $1 \le \ell \le m$, and $2k-1 = Ap+B$ with $A \le B+1$. Since the i_ℓ's are odd, we have actually $a_\ell < b_\ell$ for all ℓ. Since $m \ge 1$, the above conditions imply that

$$A + a_1 + a_2 + \cdots + a_m \le (B+1) + (b_1 - 1) + b_2 + \cdots + b_m. \tag{6.11}$$

We know that the number of carries C from the p^1-digit to the p^2-digit when adding $(2k-1)+i_1+i_2+\cdots+i_m$ is at least $e \ge 1$. Hence, either $B+b_1+b_2+\cdots+b_m \ge p$, thus creating a carry from the p^0-digit to the p^1-digit when adding $(2k-1)+i_1+i_2+\cdots+i_m$, or $A+a_1+a_2+\cdots+a_m \ge p$. But then (6.11) implies again $B+b_1+b_2+\cdots+b_m \ge p$ with the consequence of an additional carry. Consequently, we have found the additional $+1$ in all cases.

This completes the proof of the proposition. □

Theorem 22. *Let n, k, e, f be non-negative integers with $n \ge k$, and let p be a prime number with $p \equiv 3 \pmod 4$. If $n \ge \left\lceil \frac{ep^2}{2} \right\rceil$ and $k < \left\lceil \frac{fp^2}{2} \right\rceil$, then $R^{-1}(2n, 2k)$ is divisible by p^{e-f+1}. Moreover, if $f = 1$ then $R^{-1}(2n, 2k)v(k)$ is divisible by p^{e+1}.*

Proof. The result follows immediately when using Proposition 21 in (6.1). □

7. The sequence $(d(n))_{n\ge0}$ modulo prime powers p^e with $p \equiv 3 \pmod 4$

We are now in a position to prove our first main result. The following theorem proves Conjecture 18(3) in [13], in the stronger form given in Theorem 1(1).

Theorem 23. *Given a prime p with $p \equiv 3 \pmod 4$ and an integer $e \ge 2$, the number $d(n)$ is divisible by p^e for $n \ge \left\lceil \frac{(e-1)p^2}{2} \right\rceil$.*

Proof. We prove the assertion by induction on n. Let $n \ge \left\lceil \frac{(e-1)p^2}{2} \right\rceil$. We use the relation (2.12). We consider some k with $(f-1)p^2 \le k < fp^2$. If $f \ge 2$, then Theoremxx 22 and 17 imply

$$v_p\big(R^{-1}(2n, 2k)v(k)\big) \ge (e-f) + f = e. \tag{7.1}$$

On the other hand, if $f = 1$ then the supplement in Theorem 22 says that (7.1) also holds in this case. In other words, each term on the right-hand side of (2.12) is divisible by p^e, hence so is $d(n)$, as desired. □

8. The sequence $(v(n))_{n\ge0}$ modulo powers of 2

The purpose of this section is to show periodicity of the sequence $\big(v(n)\big)_{n\ge0}$ modulo powers of 2, together with a precise statement on the period length. The corresponding analysis is much more involved than the preceding ones modulo odd prime powers. Our starting point is an expansion that is very similar in spirit to the one in Section 6, namely (8.20). As a matter of fact, the main results of this section concern a polynomial refinement of $v(n)$ in which the product $\Pi_3(j) = \prod_{\ell=1}^{j}(4\ell-3)^2$ gets replaced by a variable $x(j)$, $j = 0, 1, \dots$, with the only restriction that $x(0) = 1$ and that both $x(1)$ and $x(2)$ are odd.

The main results in Theorems 31 and 32 need substantial preparations. These are the contents of Lemma 24, Corollaries 25 and 26, and Lemmas 27–29, which provide formulae and bounds for the 2-adic valuation of the ratios of factorials that appear in the expansion (8.20).

Lemma 24. *For all positive integers n and c_2 with $n \ge 2c_2$, we have*

$$v_2\left(\frac{(2n)!}{2!^{n-2c_2}(n-2c_2)!\,4!^{c_2}c_2!}\right) = \#(\text{carries when adding } (n-2c_2)_2 \text{ and } (2c_2)_2), \quad (8.1)$$

where, as before, $(\alpha)_2$ denotes the 2-adic representation of the integer α.

Proof. By Legendre's formula in Lemma 3, we obtain

$$\begin{aligned} &v_2\left(\frac{(2n)!}{2!^{n-2c_2}(n-2c_2)!\,4!^{c_2}c_2!}\right)\\ &\qquad = 2n - s_2(2n) - (n-2c_2) - \big(n-2c_2-s_2(n-2c_2)\big) - 3c_2 - (c_2 - s_2(c_2))\\ &\qquad = -s_2(n) + s_2(n-2c_2) + s_2(2c_2). \end{aligned}$$

By Lemma 5, this is indeed the number of carries when adding $n-2c_2$ and $2c_2$ in their 2-adic representations. $\square$

Corollary 25. *For all positive integers n, we have*

$$v_2\left(\frac{(2n)!}{2!^{n-2}(n-2)!\,4!}\right) = \begin{cases} v_2(n)-1, & \textit{if } n \textit{ is even},\\ v_2(n-1)-1, & \textit{if } n \textit{ is odd.}\end{cases}$$

Proof. We appeal to Lemma 24 with $c_2 = 1$. If n is even, say $n = 2^{v_2(n)}n_0$ for an odd integer n_0 and $v_2(n) \ge 1$, then the number of carries in (8.1) is $v_2(n)-1$. On the other hand, if n is odd, say $n = 2^{v_2(n-1)}n_0 + 1$ for an odd integer n_0, then this number of carries is $v_2(n-1)-1$. $\square$

Corollary 26. *For all positive integers n, we have*

$$v_2\left(\frac{(2n)!}{2!^{n-4}(n-4)!\,4!^2 2!}\right) = \begin{cases} v_2(n)-2, & \textit{if } n \equiv 0 \pmod 4,\\ v_2(n-1)-2, & \textit{if } n \equiv 1 \pmod 4,\\ v_2(n-2)-2, & \textit{if } n \equiv 2 \pmod 4,\\ v_2(n-3)-2, & \textit{if } n \equiv 3 \pmod 4.\end{cases}$$

Proof. Again, we appeal to Lemma 24, here with $c_2 = 2$. If $n \equiv 0 \pmod 4$, say $n = 2^{v_2(n)}n_0$ for an odd integer n_0 and $v_2(n) \ge 2$, then the number of carries in (8.1) is $v_2(n)-2$. The other cases are treated similarly. We leave the details to the reader. $\square$

Lemma 27. *For all positive integers n and c_2 with $n \ge 2c_2 \ge 6$, we have*

$$c_2 + v_2\left(\frac{(2n)!}{2!^{n-2c_2}(n-2c_2)!\,4!^{c_2}c_2!}\right) \ge 1 + \max_{n-2c_2 < i \le n} v_2(i). \quad (8.2)$$

Proof. Choose α and β such that $n = n_0 2^\alpha + n_1$, with n_0 odd and $n_1 < 2^{\beta+2}$, and $2^\beta \le c_2 < 2^{\beta+1}$. These conditions imply that the 2-adic representations can be schematically indicated as

$$\begin{array}{rl} & \quad\;\; \overset{\alpha}{\downarrow} \qquad \overset{\beta+2}{\downarrow} \\ (n)_2 = & \dots\, 10 \,\dots\, 0 * \dots \\ (2c_2)_2 = & \qquad\qquad\;\; 1 \,\dots \end{array} \tag{8.3}$$

with the meaning that the 1 shown in the 2-adic representation of n is the α-th digit counted from right (the counting starting with 0), and that the left-most (non-zero) digit of the 2-adic representation of $2c_2$ is the $(\beta+1)$-st digit, that is, $2c_2 < 2^{\beta+2}$.

First, we assume that $\beta \ge 2$. The case of $\beta = 1$, which implies that $2c_2 = 6$, will be disposed of at the end of this proof.

We distinguish two cases, depending on the relative sizes of n_1 and $2c_2$.

Case 1: $n_1 < 2c_2$. Here, by inspection of (8.3), we see that

$$\max_{n-2c_2<i\le n} v_2(i) = \alpha. \tag{8.4}$$

On the other hand, by Lemma 24, the term $v_2(\,.\,)$ on the left-hand side of (8.2) equals the number of carries when adding $n-2c_2$ and $2c_2$ in their 2-adic representations. Equivalently, this is the number of carries when performing the subtraction of $(2c_2)_2$ from $(n)_2$. Here, inspection of (8.3) yields that this is at least $\alpha-(\beta+2)+1$. Thus, together with (8.4) and the elementary inequality

$$2^\beta \ge \beta+2 \quad \text{for } \beta \ge 2, \tag{8.5}$$

we get

$$\begin{aligned} c_2 + v_2\left(\frac{(2n)!}{2!^{n-2c_2}(n-2c_2)!\,4!^{c_2}c_2!}\right) &\ge c_2+\alpha-\beta-1 \ge 2^\beta+\alpha-\beta-1 \\ &\ge \beta+2+\alpha-\beta-1 = \alpha+1 \ge 1+\max_{n-2c_2<i\le n} v_2(i). \end{aligned}$$

Case 2: $n_1 \ge 2c_2$. Now, by inspection of (8.3), we see that

$$\max_{n-2c_2<i\le n} v_2(i) \le \beta+1.$$

Hence, using again (8.5), we get

$$c_2 + v_2\left(\frac{(2n)!}{2!^{n-2c_2}(n-2c_2)!\,4!^{c_2}c_2!}\right) \ge c_2 \ge 2^\beta \ge \beta+2 \ge 1+\max_{n-2c_2<i\le n} v_2(i).$$

Finally we address the case where $\beta = 1$, and thus $2c_2 = 6$. In this case, the schematic representation (8.3) becomes

$$\begin{array}{rl} & \quad\;\; \overset{\alpha}{\downarrow} \qquad \overset{3}{\downarrow} \\ (n)_2 = & \dots\, 10 \,\dots\, 0 *** \\ (6)_2 = & \qquad\qquad\;\; 110 \end{array}$$

Here also, we must distinguish two cases depending on whether or not n_1 is greater than 6.

If $n_1 < 6$, then (8.4) holds. By Lemma 24, we then get

$$c_2 + v_2\left(\frac{(2n)!}{2!^{n-2c_2}(n-2c_2)!\,4!^{c_2}c_2!}\right) \ge 3 + (\alpha - 2) = \alpha + 1 \ge 1 + \max_{n-2c_2<i\le n} v_2(i).$$

On the other hand, if $n_1 \ge 6$ then

$$\max_{n-2c_2<i\le n} v_2(i) \le 2,$$

and we obtain

$$c_2 + v_2\left(\frac{(2n)!}{2!^{n-2c_2}(n-2c_2)!\,4!^{c_2}c_2!}\right) \ge 3 \ge 1 + \max_{n-2c_2<i\le n} v_2(i).$$

This completes the proof of the lemma. □

Lemma 28. *For all positive integers n and c_2 with $n \ge 2c_2 + 3$, we have*

$$c_2 + 2 + v_2\left(\frac{(2n)!}{2!^{n-2c_2-3}(n-2c_2-3)!\,4!^{c_2}c_2!\,6!}\right) \ge 1 + \max_{n-2c_2-3<i\le n} v_2(i). \tag{8.6}$$

Proof. By Legendre's formula in Lemma 3, we obtain

$$\begin{aligned} v_2&\left(\frac{(2n)!}{2!^{n-2c_2-3}(n-2c_2-3)!\,4!^{c_2}c_2!\,6!}\right)\\ &= 2n - s_2(2n) - (n-2c_2-3) - \big(n-2c_2-3-s_2(n-2c_2-3)\big)\\ &\qquad - 3c_2 - (c_2 - s_2(c_2)) - 4\\ &= -s_2(n) + s_2(n-2c_2-3) + s_2(2c_2) + s_2(3)\\ &\ge -s_2(n) + s_2(n-2c_2-3) + s_2(2c_2+3)\\ &= \#(\text{carries when adding } (n-2c_2-3)_2 \text{ and } (2c_2+3)_2). \end{aligned}$$

From here on we follow the setup and the arguments in the proof of Lemma 27, with $2c_2+3$ in place of $2c_2$; see, in particular, the schematic representation in (8.3) with that replacement. There is one notable difference, though: here the lower bound on c_2 is zero (as opposed to 3 in the proof of Lemma 27). This entails $2c_2+3 \ge 3$, and hence the lower bound on the parameter β is $\beta \ge 0$. Thus, instead of (8.5), we can only use $2^\beta \ge \beta + 1$ here, a bound that is by 1 weaker. This is balanced by the additional summand $+2$ on the left-hand side of (8.6) when compared to the left-hand side of (8.2). □

In order to have a convenient notation for the following considerations, inspired by [11], we write $\mathcal{P}_{N,K}$ for the set of all tuples $(c_1, c_2, \dots, c_N)$ of non-negative integers with

$$c_1 + c_2 + \cdots + c_N = K, \tag{8.7}$$

$$c_1 + 2c_2 + \cdots + Nc_N = N. \tag{8.8}$$

Lemma 29. *For all positive integers n and tuples $(c_1, c_2, \dots, c_n)$ in*

$$\mathcal{P}_{n,k}\backslash\{(n,0,\dots,0),(n-2,1,0,\dots,0),(n-4,2,0,\dots,0)\},$$

we have

$$n-k+v_2\left(\frac{(2n)!}{2!^{c_1}c_1!\,4!^{c_2}c_2!\cdots(2n)!^{c_n}c_n!}\right)\ge 1+\max_{c_1<i\le n} v_2(i). \tag{8.9}$$

Proof. By Legendre's formula in Lemma 3, the 2-adic valuation on the left-hand side of (8.9) equals

$$\begin{aligned}v_2\left(\frac{(2n)!}{2!^{c_1}c_1!\,4!^{c_2}c_2!\cdots(2n)!^{c_n}c_n!}\right)&=2n-s_2(2n)-\sum_{i=1}^n\big(c_i(2i-s_2(2i))+c_i-s_2(c_i)\big)\\&=\sum_{i=1}^n c_is_2(i)-\sum_{i=1}^n\big(c_i-s_2(c_i)\big)-s_2(n).\end{aligned}$$

Define the quantity $G(n,k)$ by

$$G(n,k):=n-k+\sum_{i=1}^n c_is_2(i)-\sum_{i=1}^n\big(c_i-s_2(c_i)\big)-s_2(n).$$

We must show that $G(n,k)$ is at least as large as the right-hand side of (8.9). We achieve this by demonstrating that, among all elements $(c_1,c_2,\dots,c_n)\in\mathcal{P}_{n,k}$ with fixed c_1, the ones with $c_i=0$ for $i\ge 4$ and $c_3=0$ or $c_3=1$, depending on the parity of $n-c_1$, attain the smallest values of $G(n,k)$, and then appealing to Lemmas 27 and 28.

First consider a tuple $(c_1,c_2,\dots,c_n)$ in which $c_{2j}>0$ for some $j\ge 2$. We claim that the value of $G(n,k)$ decreases if instead we consider the tuple $(c_1,c_2+jc_{2j},\dots,0,\dots,c_n)$, with 0 appearing in position $2j$. This new tuple is an element of $\mathcal{P}_{n,k+(j-1)c_{2j}}$. In order to prove the claim, we compare the contributions of the tuples to $G(n,k)$, ignoring the terms that are the same for both tuples. In particular, we may ignore appearances of n (such as in $s_2(n)$) since n is the same for both tuples (as opposed to k, which becomes $k+(j-1)c_{2j}$ for the modified tuple). The — in this sense — relevant contribution of $(c_1,c_2,\dots,c_n)$ to $G(n,k)$ is

$$\begin{aligned}&c_2s_2(2)+c_{2j}s_2(2j)-(c_2-s_2(c_2))-(c_{2j}-s_2(c_{2j}))\\&\qquad=c_{2j}\big(s_2(j)-1\big)+s_2(c_2)+s_2(c_{2j}).\end{aligned}\tag{8.10}$$

On the other hand, the (relevant) contribution of $(c_1,c_2+jc_{2j},\dots,0,\dots,c_n)$ to $G(n,k+(j-1)c_{2j})$ is

$$-(j-1)c_{2j}+(c_2+jc_{2j})s_2(2)-(c_2+jc_{2j}-s_2(c_2+jc_{2j}))=-(j-1)c_{2j}+s_2(c_2+jc_{2j}). \tag{8.11}$$

The difference of (8.10) and (8.11) is

$$\begin{aligned}&c_{2j}\big(s_2(j)+j-2\big)+s_2(c_2)+s_2(c_{2j})-s_2(c_2+jc_{2j})\\&\qquad\ge c_{2j}s_2(j)+(j-2)c_{2j}+s_2(c_{2j})-s_2(c_{2j}j)\\&\qquad\ge(j-2)c_{2j}+s_2(c_{2j})\ge s_2(c_{2j}),\end{aligned}$$

which is positive, thus proving our claim.

Now consider a tuple $(c_1,c_2,\dots,c_n)$ in which $c_{2j+1}>0$ for some $j\ge 2$. Again, we claim that the value of $G(n,k)$ (weakly) decreases if instead we consider the tuple $(c_1,c_2+(j-1)c_{2j+1},c_3+c_{2j+1},\dots,0,\dots,c_n)$, with 0 appearing in position $2j+1$. This new tuple is an element of $\mathcal{P}_{n,k+(j-1)c_{2j+1}}$. In order to prove the claim, we compare the contributions of the tuples to $G(n,k)$, ignoring the terms that are the same for both tuples. The (relevant) contribution of $(c_1,c_2,\dots,c_n)$ to $G(n,k)$ is

$$c_2s_2(2)+c_3s_2(3)+c_{2j+1}s_2(2j+1)-(c_2-s_2(c_2))-(c_3-s_2(c_3))-(c_{2j+1}-s_2(c_{2j+1}))\\ =c_3+c_{2j+1}s_2(j)+s_2(c_2)+s_2(c_3)+s_2(c_{2j+1}). \tag{8.12}$$

On the other hand, the (relevant) contribution of $(c_1,c_2+(j-1)c_{2j+1},c_3+c_{2j+1},\dots,0,\dots,c_n)$ to $G(n,k+(j-1)c_{2j+1})$ is

$$-(j-1)c_{2j+1}+(c_2+(j-1)c_{2j+1})s_2(2)+(c_3+c_{2j+1})s_2(3)\\ -(c_2+(j-1)c_{2j+1}-s_2(c_2+(j-1)c_{2j+1}))-(c_3+c_{2j+1}-s_2(c_3+c_{2j+1}))\\ =c_3-(j-2)c_{2j+1}+s_2(c_2+(j-1)c_{2j+1})+s_2(c_3+c_{2j+1}). \tag{8.13}$$

The difference of (8.12) and (8.13) is

$$c_{2j+1}\big(s_2(j)+j-2\big)+s_2(c_2)+s_2(c_3)+s_2(c_{2j+1})\\ -s_2(c_2+(j-1)c_{2j+1})-s_2(c_3+c_{2j+1})\\ \ge c_{2j+1}\big(s_2(j)+j-2\big)+s_2(c_2)-s_2(c_2+(j-1)c_{2j+1})\\ \ge c_{2j+1}\big(s_2(j)-1\big)+(j-1)c_{2j+1}-s_2((j-1)c_{2j+1})\\ \ge c_{2j+1}\big(s_2(j)-1\big),$$

which is non-negative, as claimed.

So far, the above arguments show that we may restrict our attention to tuples $(c_1,c_2,\dots,c_n)$ in $\mathcal P_{n,k}$ with $c_i=0$ for $i\ge 4$. Finally, we argue that "3's can be traded for 2's", that is, we may decrease c_3 at the cost of increasing c_2. There are two cases to be considered. First let c_3 be even, $c_3=2c_3'$ say, with $c_3'\ge 1$. We claim that the value of $G(n,k)$ decreases if instead of $(c_1,c_2,c_3,\dots,c_n)$ we consider the tuple $(c_1,c_2+3c_3',0,\dots,c_n)$, This new tuple is an element of $\mathcal P_{n,k+c_3'}$. In order to prove the claim, we compare the contributions of the tuples to $G(n,k)$, ignoring the terms that are the same for both tuples. The (relevant) contribution of $(c_1,c_2,c_3,\dots,c_n)$ to $G(n,k)$ is

$$c_2s_2(2)+c_3s_2(3)-(c_2-s_2(c_2))-(c_3-s_2(c_3))=c_3+s_2(c_2)+s_2(c_3'). \tag{8.14}$$

On the other hand, the (relevant) contribution of $(c_1,c_2+3c_3',0,\dots,c_n)$ to $G(n,k+c_3')$ is

$$-c_3'+(c_2+3c_3')s_2(2)-(c_2+3c_3'-s_2(c_2+3c_3'))=-c_3'+s_2(c_2+3c_3'). \tag{8.15}$$

The difference of (8.14) and (8.15) is

$$3c_3'+s_2(c_2)+s_2(c_3')-s_2(c_2+3c_3')\ge 3c_3'+s_2(c_2+c_3')-s_2(c_2+3c_3')\\ \ge 3c_3'-s_2(2c_3')\ge c_3', \tag{8.16}$$

which is positive, proving our claim.

Finally, let c_3 be odd, $c_3=2c_3'+1$ say, with $c_3'\ge 1$. We claim that the value of $G(n,k)$ decreases if instead of $(c_1,c_2,c_3,\dots,c_n)$ we consider the tuple $(c_1,c_2+3c_3',1,\dots,c_n)$, This new tuple is an element of $\mathcal P_{n,k+c_3'}$. In order to prove the claim, we compare the contributions of the tuples to $G(n,k)$, ignoring the terms that are the same for both tuples. The (relevant) contribution of $(c_1, c_2, c_3, \dots, c_n)$ to $G(n,k)$ is

$$c_2 s_2(2) + c_3 s_2(3) - (c_2 - s_2(c_2)) - (c_3 - s_2(c_3)) = c_3 + s_2(c_2) + s_2(c_3') + 1. \tag{8.17}$$

On the other hand, the (relevant) contribution of $(c_1, c_2 + 3c_3', 1, \dots, c_n)$ to $G(n, k + c_3')$ is

$$- c_3' + (c_2 + 3c_3')s_2(2) + s_2(3) - (c_2 + 3c_3' - s_2(c_2 + 3c_3')) \\ = -c_3' + s_2(c_2 + 3c_3') + 2. \tag{8.18}$$

The difference of (8.17) and (8.18) is the same as (8.16), of which we already know that it is positive.

We are now in the position to finish the proof of the lemma. Our tuple $(c_1, c_2, \dots, c_n)$ may be one where $c_i = 0$ for $i \geq 3$. Then $c_1 = n - 2c_2$, $n - k = (c_1 + 2c_2) - (c_1 + c_2) = c_2$, and $c_2 \geq 3$ by assumption. The assertion of the lemma then follows from Lemma 27. On the other hand, our tuple $(c_1, c_2, \dots, c_n)$ may be one where $c_3 = 1$ and $c_i = 0$ for $i \geq 4$. Then $c_1 = n - 2c_2 - 3$, and $n - k = (c_1 + 2c_2 + 3) - (c_1 + c_2 + 1) = c_2 + 2$. The assertion of the lemma then follows from Lemma 28. If we are not in one of these two cases, then we apply the above described reductions repeatedly until we arrive at a tuple which belongs to one of these two cases. Since the value of $G(n,k)$ never increases while the value of c_1 remains invariant when doing these reductions, Lemmas 27 and 28 again establish the assertion of the lemma.

The proof is now complete. □

Before we are able to state and prove the main result of this section, we need an auxiliary integrality assertion on a certain product/quotient of factorials.

Lemma 30 ([1, Theorem 13.2])**.** *Let N and K be positive integers such that $N \geq K$. For all tuples $(c_i)_{1 \leq i \leq N}$ of integers in $\mathcal{P}_{N,K}$ — that is, satisfying* (6.2) *and* (6.3) *— the quantity*

$$\frac{N!}{\prod_{i=1}^{N} i!^{c_i} c_i!}$$

is an integer, and it equals the number of partitions of the set $\{1, 2, \dots, N\}$ into c_i blocks of size i, for $i = 1, 2, \dots, N$.

We are now in the position to embark on the proof of periodicity of $v(n)$ as defined in (2.5) modulo powers of 2. The next theorem treats the "generic" case where $e \geq 3$, whereas Theorem 32 handles the remaining cases where $e = 1$ or $e = 2$. Both theorems provide in fact polynomial refinements.

Theorem 31. *Let $x(j)$, $j = 0, 1, 2, \dots,$ be a sequence of integers with $x(0) = 1$, $x(1)$ and $x(2)$ odd. Then the coefficients $v_{\mathbf{x}}(n)$ in the expansion*

$$\sum_{n \geq 0} \frac{v_{\mathbf{x}}(n)}{2^n\,(2n)!} t^n = \left(1 + \sum_{j \geq 1} \frac{x(j)}{(2j)!} t^{2j}\right)^{1/2} \tag{8.19}$$

are integers. Moreover, for all integers $e \geq 3$, the sequence $(v_{\mathbf{x}}(n))_{n \geq 0}$ is purely periodic modulo 2^e with (not necessarily minimal) period length 2^{e-1}.

Remark. Computer experiments suggest that, in fact, the period length of 2^{e-1} *is* minimal.

Proof of Theorem 31. We compute the defining expansion for the coefficients $v_{\mathbf{x}}(n)$:

$$\begin{aligned}\sum_{n\ge0}\frac{v_{\mathbf{x}}(n)}{2^n(2n)!}t^n&=\left(1+\sum_{j\ge1}\frac{x(j)}{(2j)!}t^j\right)^{1/2}\\&=\sum_{k\ge0}\binom{1/2}{k}\left(\sum_{j\ge1}\frac{x(j)}{(2j)!}t^j\right)^k\\&=1+\sum_{k\ge1}(-1)^{k-1}\frac{\prod_{j=1}^{k-1}(2j-1)}{2^k\,k!}\sum_{c_1+c_2+\dots=k}\frac{k!}{c_1!\,c_2!\cdots}\prod_{i\ge1}\frac{x^{c_i}(i)}{(2i)!^{c_i}}t^{ic_i}.\end{aligned}$$

By comparing coefficients of t^n, we obtain

$$v_{\mathbf{x}}(n)=\sum_{k\ge1}\sum_{(c_i)\in\mathcal{P}_{n,k}}(-1)^{k-1}\left(\prod_{j=1}^{k-1}(2j-1)\right)2^{n-k}\frac{(2n)!}{2!^{c_1}c_1!\,4!^{c_2}c_2!\cdots(2n)!^{c_n}c_n!}\prod_{i=1}^{n}x^{c_i}(i),\tag{8.20}$$

where $\mathcal{P}_{n,k}$ is defined around (8.7)–(8.8). For convenience, we denote the summand in the above double sum by $S(n,k,(c_i))$, that is, we set

$$S(n,k,(c_i)):=(-1)^{k-1}\left(\prod_{j=1}^{k-1}(2j-1)\right)2^{n-k}\frac{(2n)!}{2!^{c_1}c_1!\,4!^{c_2}c_2!\cdots(2n)!^{c_n}c_n!}\prod_{i=1}^{n}x^{c_i}(i)\tag{8.21}$$

for some positive integer k and $(c_i)\in\mathcal{P}_{n,k}$. The fraction in the expression in (8.20) (and in (8.21)) is an integer since, by Lemma 30, it is the number of all partitions of $\{1,2,\dots,2n\}$ into c_i blocks of size $2i$, $i=1,2,\dots,n$. If this property is used in (8.20), then this establishes the integrality assertion of the theorem.

Now, let $n<2^{e-1}$. We want to prove that

$$v_{\mathbf{x}}(n+a2^{e-1})\equiv v_{\mathbf{x}}(n)\pmod{2^e},\tag{8.22}$$

for all positive integers a. Using our short notation for the summand in (8.20), we have

$$v_{\mathbf{x}}\big(n+a2^{e-1}\big)=\sum_{k\ge1}\sum_{(\tilde c_i)\in\mathcal{P}_{n+a2^{e-1},k}}S(n+a2^{e-1},k,(\tilde c_i)).\tag{8.23}$$

We are going to prove the finer congruences

$$S(n+a2^{e-1},k,(\tilde c_i))\equiv 0 \pmod{2^e},\quad \text{if } \tilde c_1<a2^{e-1},\\ (\tilde c_i) \text{ not in cases (8.29)–(8.31)}, \tag{8.24}$$

$$S(n+a2^{e-1},n+a2^{e-1},(n+a2^{e-1},0,\dots,0))\equiv S(n,n,(n,0,\dots,0)) \pmod{2^e}, \tag{8.25}$$

$$S(n+a2^{e-1},k+a2^{e-1},(\tilde c_i))\equiv S(n,k,(c_1,\tilde c_2,\dots,\tilde c_n)) \pmod{2^e}\\ \text{with } \tilde c_1=c_1+a2^{e-1}, \text{ and } (\tilde c_i) \text{ not in cases (8.29)–(8.31)}, \tag{8.26}$$

$$\begin{aligned} S(n+a2^{e-1},&n+a2^{e-1}-1,(n+a2^{e-1}-2,1,0,\dots,0))\\ &+S(n+a2^{e-1},n+a2^{e-1}-2,(n+a2^{e-1}-4,2,0,\dots,0))\\ &\equiv S(n,n-1,(n-2,1,0,\dots,0))\\ &\quad + S(n,n-2,(n-4,2,0,\dots,0)) \pmod{2^e}. \end{aligned} \tag{8.27}$$

In the last congruence, undefined terms (terms $S(n,k,(\tilde c_i))$ with negative $\tilde c_1$) have to be understood as being zero.

We claim that (8.24)–(8.27) together imply (8.22), and thus the theorem. In order to prove this, we consider the summand $S(n+a2^{e-1},k,(\tilde c_i))$ on the right-hand side of (8.23), when taken modulo 2^e, for the various choices of k and tuples $(\tilde c_i)$. If $\tilde c_1<a2^{e-1}$, then, by (8.24), the corresponding summand vanishes modulo 2^e. On the other hand, if $\tilde c_1\ge a2^{e-1}$, then, since $k\ge \tilde c_1$, we must also have $k\ge a2^{e-1}$. Consequently, we may apply (8.25) and (8.26) to conclude that

$$S(n+a2^{e-1},k,(\tilde c_i))\equiv S(n,k-a2^{e-1},(c_1,\tilde c_2,\dots,\tilde c_n)) \pmod{2^e}, \tag{8.28}$$

except if we are in cases (8.30) or (8.31). However, for those cases the congruence (8.27) applies. It shows that, even though the congruence (8.28) may not hold for an individual summand in case (8.30) or (8.31), if they are combined then the corresponding reduction in (8.28) is allowed. Altogether, we arrive at

$$\begin{aligned} v_{\mathbf x}\big(n+a2^{e-1}\big) &= \sum_{k\ge1}\sum_{(\tilde c_i)\in\mathcal P_{n+a2^{e-1},k}} S(n+a2^{e-1},k,(\tilde c_i))\\ &\equiv \sum_{k\ge a2^{e-1}+1}\sum_{(c_i)\in\mathcal P_{n,k-a2^{e-1}}} S(n+a2^{e-1},k-a2^{e-1},(c_i)) \pmod{2^e}\\ &\equiv v_{\mathbf x}(n) \pmod{2^e}, \end{aligned}$$

thus confirming the claim.

Now we provide the proofs of the crucial congruences (8.24)–(8.27).

Proof of (8.24). If we use Lemma 29 with n replaced by $n+a2^{e-1}$ and $c_i=\tilde c_i$ for all i, then we see that $S(n+ap^{e-1},k,(\tilde c_i))$ is divisible by

$$2^{1+\max_{\tilde c_1<i\le n+a2^{e-1}} v_2(i)},$$

with three exceptions, namely

$$(\tilde c_1,\tilde c_2,\dots,\tilde c_n)=(n+a2^{e-1},0,\dots,0), \tag{8.29}$$

$$(\tilde c_1,\tilde c_2,\dots,\tilde c_n)=(n+a2^{e-1}-2,1,0,\dots,0), \tag{8.30}$$

$$(\tilde c_1,\tilde c_2,\dots,\tilde c_n)=(n+a2^{e-1}-4,2,0,\dots,0). \tag{8.31}$$

In particular, if $\tilde c_1 < a2^{e-1}$, and if (8.29)–(8.31) do not apply, then in the range $\tilde c_1 < i \le n+a2^{e-1}$ we will find that $i=a2^{e-1}$, and, consequently, $S(n+a2^{e-1},k,(\tilde c_i))$ is divisible by 2^e, as desired.

Proof of (8.25). By definition, we have

$$\begin{aligned}
S(n+a2^{e-1},&\,n+a2^{e-1},(n+a2^{e-1},0,\dots,0))\\
&=(-1)^{n+a2^{e-1}-1}\left(\prod_{j=1}^{n+a2^{e-1}-1}(2j-1)\right)(2n+a2^e-1)!!\,x^{n+a2^{e-1}}(1)\\
&=(-1)^{n-1}(2n+a2^e-3)!!\,(2n+a2^e-1)!!\,x^{n+a2^{e-1}}(1)
\end{aligned}$$

and

$$S(n,n,(n,0,\dots,0))=(-1)^{n-1}(2n-3)!!\,(2n-1)!!\,x^n(1).$$

By assumption, the number $x(1)$ is odd. Hence, Euler's theorem and the fact that $\varphi(2^e)=2^{e-1}$ imply that

$$x^{2^{e-1}}(1)\equiv 1 \pmod{2^e}.$$

Furthermore, we have

$$\begin{aligned}
(2n+a2^e-1)!!&=(2n-1)!!\prod_{j=0}^{a-1}(2n+j2^e+1)(2n+j2^e+3)\cdots(2n+(j+1)2^e-1)\\
&\equiv(2n-1)!! \pmod{2^e},
\end{aligned} \tag{8.32}$$

since, for each j, the factors inside the product in the first line form a complete set of representatives of the multiplicative group $(\mathbb{Z}/2^e\mathbb{Z})^\times$. An analogous relation holds for $(2n+a2^e-3)!!$ and $(2n-3)!!$. Altogether, this establishes the congruence (8.25).

Proof of (8.26). Replace n by $n+a2^{e-1}$, and c_1 by c_1+a2^{e-1} in (8.21). Since $(c_1+a2^{e-1},c_2,\dots)\in P_{n+a2^{e-1},k}$, the c_i's must vanish for $i>n$. Furthermore, we have $k\ge c_1+a2^{e-1}$, which allows us to write $k=k'+a2^{2-1}$ for some non-negative integer k'. Hence, under these substitutions and simplifications, and writing k instead of k' in abuse of notation, we obtain

$$\begin{aligned}
S(n+a2^{e-1},k+a2^{e-1},(\tilde c_i))&=(-1)^{k+a2^{e-1}-1}\left(\prod_{j=1}^{k+a2^{e-1}-1}(2j-1)\right)\\
&\times 2^{n-k}\frac{(2n+a2^e)!}{2!^{c_1+a2^{e-1}}(c_1+a2^{e-1})!\,4!^{c_2}c_2!\cdots n!^{c_n}c_n!}x^{a2^{e-1}}(1)\prod_{i=1}^n x^{c_i}(i),
\end{aligned} \tag{8.33}$$

with $(c_i) \in \mathcal{P}_{n,k}$. We are interested in the residue class of this expression modulo 2^e. As in (8.32), elementary number theory tells us that

$$\prod_{j=1}^{k+a2^{e-1}-1}(2j-1) \equiv \prod_{j=1}^{k-1}(2j-1) \pmod{2^e}.$$

Furthermore, we know that $x(1)$ is odd by assumption. Therefore the expression (8.33) simplifies to

$$S(n+a2^{e-1}, k+a2^{e-1}, (\tilde{c}_i)) \equiv (-1)^{k-1}\left(\prod_{j=1}^{k-1}(2j-1)\right)$$
$$\times\, 2^{n-k}\frac{(2n+a2^e)!\,c_1!}{(2n)!\,2^{a2^{e-1}}(c_1+a2^{e-1})!}\frac{(2n)!}{2!^{c_1}c_1!\,4!^{c_2}c_2!\cdots n!^{c_n}c_n!}\prod_{i=1}^{n}x^{c_i}(i) \pmod{2^e}. \quad (8.34)$$

We have

$$\frac{(2n+a2^e)!\,c_1!}{(2n)!\,2^{a2^{e-1}}(c_1+a2^{e-1})!} = \frac{(n+a2^{e-1})!\,(2n+a2^e-1)!!\,c_1!}{n!\,(2n-1)!!\,(c_1+a2^{e-1})!}.$$

Since, again by elementary number theory,

$$\frac{(2n+a2^e-1)!!}{(2n-1)!!} \equiv 1 \pmod{2^e},$$

we may conclude that

$$\frac{(2n+a2^e)!\,c_1!}{(2n)!\,2^{a2^{e-1}}(c_1+a2^{e-1})!} \equiv \frac{(n+a2^{e-1})!\,c_1!}{n!\,(c_1+a2^{e-1})!} \pmod{2^e}$$
$$\equiv \prod_{i=c_1+1}^{n}\frac{i+a2^{e-1}}{i} \pmod{2^e}$$
$$\equiv \prod_{i=c_1+1}^{n}\frac{(i\cdot 2^{-v_2(i)})+a2^{e-v_2(i)-1}}{i\cdot 2^{-v_2(i)}} \pmod{2^e}.$$

If this is substituted back in (8.34), then we see that

$$S(n+a2^{e-1}, k+a2^{e-1}, (\tilde{c}_i))$$
$$\equiv (-1)^{k-1}\left(\prod_{j=1}^{k-1}(2j-1)\right)\left(\prod_{i=c_1+1}^{n}\frac{(i\cdot 2^{-v_2(i)})+a2^{e-v_2(i)-1}}{i\cdot 2^{-v_2(i)}}\right)$$
$$\cdot\, 2^{n-k}\frac{(2n)!}{2!^{c_1}c_1!\,4!^{c_2}c_2!\cdots n!^{c_n}c_n!}\prod_{i=1}^{n}x^{c_i}(i) \pmod{2^e}. \quad (8.35)$$

The reader should note that we wrote the first product over i in this particular form in order to make certain that the expressions $i\cdot 2^{-v_2(i)}$ in the denominator are odd numbers.

At this point, we would like to simplify the terms $(i\cdot 2^{-v_2(i)})+a2^{e-v_2(i)-1}$ to $i\cdot 2^{-v_2(i)}$. For, assuming the validity of this simplification, the first product over i on the right-hand side of (8.35) would simplify to 1, and the remaining terms exactly equal $S\big(n,k,(c_i)\big)$.

We claim that this simplification is indeed allowed. For, by Lemma 29, we know that the second line in (8.35) is an integer which is divisible by

$$2^{1+\max_{c_1<i\le n} v_2(i)}.$$

Hence, instead of computing modulo 2^e, we may reduce the first line of (8.35) modulo

$$2^{e-1-\max_{c_1<i\le n} v_2(i)}.$$

(It should be observed that the exponent is non-negative since we assumed from the beginning that $n < 2^{e-1}$.) This is exactly what we need to perform the desired simplification, and the first product over i drops out. What remains is exactly $S(n,k,(c_1,\tilde c_2,\dots,\tilde c_n))$.

Proof of (8.27). Here, instead of Lemma 29, we can only use the slightly weaker Corollaries 25 and 26.

We discuss first the "generic case", namely when $n\ge 4$, where all terms in (8.27) are defined. Let us begin with the term

$$S(n+a2^{e-1},n+a2^{e-1}-1,(n+a2^{e-1}-2,1,0,\dots,0)).$$

The corresponding expression on the right-hand side of (8.35) contains the product

$$\prod_{i=(n-2)+1}^{n}\frac{(i\cdot 2^{-v_2(i)})+a2^{e-v_2(i)-1}}{i\cdot 2^{-v_2(i)}}$$
$$=\frac{\big(((n-1)\cdot 2^{-v_2(n-1)})+a2^{e-v_2(n-1)-1}\big)\big((n\cdot 2^{-v_2(n)})+a2^{e-v_2(n)-1}\big)}{(n-1)\cdot 2^{-v_2(n-1)}\,n\cdot 2^{-v_2(n)}}. \quad (8.36)$$

If $n\equiv 0 \pmod 4$, then Corollary 25 says that the last line in (8.35) (which in particular contains the prefactor 2^{n-k}) is (exactly) divisible by $2\cdot 2^{v_2(n)-1}=2^{v_2(n)}$, and hence we may consider the numerator in (8.36) modulo $2^{e-v_2(n)}$. Since

$$((n-1)\cdot 2^{-v_2(n-1)})+a2^{e-v_2(n-1)-1}\equiv((n-1)\cdot 2^{-v_2(n-1)}) \pmod{2^{e-1}}$$

(with $v_2(n-1)=0$), the product (8.36) reduces to

$$\prod_{i=n-1}^{n}\frac{(i\cdot 2^{-v_2(i)})+a2^{e-v_2(i)-1}}{i\cdot 2^{-v_2(i)}}\equiv\frac{(n\cdot 2^{-v_2(n)})+a2^{e-v_2(n)-1}}{n\cdot 2^{-v_2(n)}} \pmod{2^e}$$
$$\equiv 1+\frac{a2^{e-v_2(n)-1}}{n\cdot 2^{-v_2(n)}} \pmod{2^e}.$$

When substituted back in (8.35), this shows that

$$S(n+a2^{e-1},n+a2^{e-1}-1,(n+a2^{e-1}-2,1,0,\dots,0))$$
$$\equiv S(n,n-1,(n-2,1,0,\dots,0))+u_1\frac{a2^{e-v_2(n)-1}}{n\cdot 2^{-v_2(n)}} \pmod{2^e},$$

where u_1 is an odd integer. Here it is important that $x(1)$ and $x(2)$ are odd, which they are by assumption.

An analogous discussion for the other term on the left-hand side of (8.27), using Corollary 26, leads to

$$S(n+a2^{e-1}, n+a2^{e-1}-2, (n+a2^{e-1}-4, 2, 0, \dots, 0)) \\ \equiv S(n, n-2, (n-4, 2, 0, \dots, 0)) + u_2 \frac{a2^{e-v_2(n)-1}}{n \cdot 2^{-v_2(n)}} \pmod{2^e},$$

where u_2 is an odd integer. Together, the last two congruences establish (8.27).

The discussions for the other congruence classes of n modulo 4 are just minor variations of the above arguments and are therefore omitted here.

Finally, we address the remaining cases of "small" n, namely $0 \le n < 4$, when one or both terms on the right-hand side of (8.27) contain negative parameter values, in which case they are declared to be zero by definition. We exemplify what has to be done in these cases by going through the case where $n = 1$. All other cases may be handled in a similar manner.

Corollary 25 with n replaced by $1 + a2^{e-1}$, together with the assumption that all $x(i)$'s are odd, implies that

$$S(n+a2^{e-1}, n+a2^{e-1}-1, (n+a2^{e-1}-2, 1, 0, \dots, 0)) \equiv \begin{cases} 2^{e-1} \pmod{2^e}, & \text{if } a \text{ is odd}, \\ 0 \pmod{2^e}, & \text{if } a \text{ is even}. \end{cases}$$

Likewise, Corollary 26 with n replaced by $1 + a2^{e-1}$, together with the assumption that all $x(i)$'s are odd, implies that

$$S(n+a2^{e-1}, n+a2^{e-1}-2, (n+a2^{e-1}-4, 2, 0, \dots, 0)) \equiv \begin{cases} 2^{e-1} \pmod{2^e}, & \text{if } a \text{ is odd}, \\ 0 \pmod{2^e}, & \text{if } a \text{ is even}. \end{cases}$$

Together, this establishes (8.27) in the considered case.

This finishes the proof of the theorem. □

Our next result generalises [11, Theorem 1(i)].

Theorem 32. *Let $x(j)$, $j = 0, 1, 2, \dots$, be integers with $x(0) = 1$ and $x(1)$ odd. Then the sequence $(v_{\mathbf{x}}(n))_{n \ge 0}$, with the coefficients $v_{\mathbf{x}}(n)$ being defined in* (8.19), *when taken modulo* 2, *is the all-*1*-sequence. Modulo* 4, *the sequence is purely periodic with period length* 4, *the first few values of the sequence* (*modulo* 4) *being given by*

$$1,\ x(1),\ 3,\ x(1)+2,\ 1,\ \dots. \tag{8.37}$$

Proof. It suffices to treat the case of modulus 4 since, because of the assumption that $x(1)$ is odd, it implies the assertion for the modulus 2.

We prove the claim in the statement of the theorem by induction on n.

We use the recurrence (2.6) for the induction step. We may assume that $n \ge 4$. We rewrite the recurrence (2.6) modulo 4 in the form

$$0 \equiv -\sum_{m=0}^{\lceil n/2 \rceil - 1} \binom{2n}{2m} v(m)v(n-m) - \frac{1}{2}\chi(n \text{ even}) \binom{2n}{n} v^2(n/2) \pmod 4,$$

where $\chi(\mathcal{A}) = 1$ if $\mathcal{A}$ is true and $\chi(\mathcal{A}) = 0$ otherwise. Since the central binomial coefficient is divisible by 2 for $n \ge 1$, we see that, for the induction, we may simply substitute the claimed mod-4 values of $v(m)$ for $m = 0, 1, \dots, n$ in

$$\frac{1}{2}\sum_{m=0}^{n}\binom{2n}{2m}v(m)v(n-m), \tag{8.38}$$

and check that the resulting expression is divisible by 4.

We substitute the values from (8.37) in the expression (8.38), to get

$$\frac{1}{2}\sum_{m\equiv 0 \pmod 4}\binom{2n}{2m}+\frac{x(1)}{2}\sum_{m\equiv 1 \pmod 4}\binom{2n}{2m} \\ +\frac{3}{2}\sum_{m\equiv 2 \pmod 4}\binom{2n}{2m}+\frac{x(1)+2}{2}\sum_{m\equiv 3 \pmod 4}\binom{2n}{2m}. \tag{8.39}$$

Next we recall the well-known (and easily derived) fact that

$$\sum_{m\equiv r \pmod 8}\binom{N}{m}=\frac{1}{8}\sum_{j=0}^{7}\omega^{-rj}(1+\omega^j)^N,$$

where $\omega = \frac{1+\mathbf{i}}{\sqrt{2}}$ is a primitive eighth root of unity (with $\mathbf{i} = \sqrt{-1}$). Using this in (8.39), we obtain

$$\frac{1}{16}\sum_{j=0}^{7}(1+\omega^j)^{2n}+\frac{x(1)}{16}\sum_{j=0}^{7}(-\mathbf{i})^j(1+\omega^j)^{2n} \\ +\frac{3}{16}\sum_{j=0}^{7}(-1)^j(1+\omega^j)^{2n}+\frac{x(1)+2}{16}\sum_{j=0}^{7}\mathbf{i}^j(1+\omega^j)^{2n}.$$

Now we multiply this expression by z^n and sum the result over all $n \ge 0$. After evaluating all the appearing geometric series and simplifying, we obtain

$$\frac{(x(1)+3)\,(1-7z+21z^2-35z^3+34z^4-42z^5-28z^6-8z^7)}{1-8z+28z^2-56z^3+68z^4-112z^5-112z^6-64z^7}. \tag{8.40}$$

Here, we should first observe that the factor $x(1)+3$ is even, since $x(1)$ is odd by assumption. Furthermore, the denominator has the form $1 + 2f(z)$, where $f(z)$ is a polynomial with integer coefficients, and the coefficients of z^4, z^5, z^6, and z^7 in the numerator are all even. It is not difficult to see that, together, this implies that in the series expansion of (8.40) the coefficients of z^n is divisible by 4 for $n \ge 4$. □

9. The inverse of the matrix R modulo powers of 2

In this section, we prove periodicity of the matrix entries $R^{-1}(k+2n, k)$ (given by Proposition 2) modulo powers of 2, when considered as a sequence indexed by k. Moreover, this result comes again with a precise statement on period lengths. Our starting point is a modified version of the expansion (6.1), namely (9.2). Also here, the main result of this section concerns a polynomial refinement. More precisely, in this refinement, the number $u(j)$ gets replaced by a variable $y(j)$, $j = 0, 1, \dots$, with the only restriction that $y(0) = 1$.

Theorem 33. *Let $y(j)$, $j = 0, 1, 2, \dots,$ be integers with $y(0) = 1$. Furthermore, define coefficients $R_y^{-1}(n, k)$ by*

$$R_y^{-1}(n,k) = 2^{(n-k)/2} \frac{(n-1)!}{(k-1)!} \left\langle t^{-k} \right\rangle U_y^{-n}(t), \tag{9.1}$$

where

$$U_y(t) := \sum_{j \ge 0} \frac{y(j)}{(2j+1)!} t^{2j+1}.$$

Here again, the case $k = 0$ has to be interpreted as $R_y^{-1}(0,0) = 1$ and $R_y^{-1}(n,0) = 0$ for $n \ge 1$. Then, for fixed n and any 2-power 2^e, the sequence $\big(R_y^{-1}(k+2n,k)\big)_{k \ge 0}$ is purely periodic modulo 2^e with (not necessarily minimal) period length 2^e.

Proof. By the definition (9.1) and the computation in (6.1) with u replaced by y, n replaced by $n+k$, and k replaced by $k/2$, in this order, we obtain

$$R_y^{-1}(2n+k,k) = \sum_{m \ge 0} \sum_{\substack{(c_i) \in \mathcal{P}^o_{2n+m,m} \\ c_1 = 0}} (-1)^m 2^n \binom{2n+m+k-1}{2n+m} \\ \cdot \frac{(2n+m)!}{3!^{c_3} c_3! \, 5!^{c_5} c_5! \cdots (2n+1)!^{c_{2n+1}} c_{2n+1}!} \prod_{i=1}^{2n+1} y^{c_i}\left(\tfrac{i-1}{2}\right), \tag{9.2}$$

with $\mathcal{P}^o_{N,K}$ having been defined below (6.1). Here, we observe that $\mathcal{P}^o_{2n+m,m}$ is empty for $m > n$. Indeed, for $(c_i) \in \mathcal{P}^o_{2n+m,m}$ with $c_1 = 0$, we have

$$3m = 3 \sum_{i=1}^{2n+1} c_i \le \sum_{i=1}^{2n+1} i c_i = 2n + m, \tag{9.3}$$

and hence $m \le n$. Consequently, we may restrict the sum over m in (9.2) to $m = 0, 1, \dots, n$.

We want to consider $R_y^{-1}(2n+k,k)$ for fixed n as a function in k. Inspection of the last expression in (9.2) reveals that, since the sum over m is finite, $R_y^{-1}(2n+k,k)$ is a polynomial in k with rational coefficients. Hence, it is certainly periodic modulo 2^e (and, more generally, modulo any modulus M). In order to find a bound on the period length, we must perform a 2-adic analysis of the expression in (9.2).

We may rewrite (9.2) as follows:

$$R_y^{-1}(2n+k,k)=\sum_{m\ge0}\sum_{\substack{(c_i)\in\mathcal P^o_{2n+m,m}\\ c_1=0}}(-1)^m2^n\frac{(2n+m+k-1)(2n+m+k-2)\cdots k}{(2n)!}\\ \cdot\frac{(2n)!}{2!^{c_3}c_3!\,4!^{c_5}c_5!\cdots(2n)!^{c_{2n+1}}c_{2n+1}!}\prod_{i=1}^{2n+1}\left(\frac{y\binom{i-1}{2}}{i}\right)^{c_i}\\ =\sum_{m\ge0}\sum_{\substack{(c_i)\in\mathcal P^o_{2n+m,m}\\ c_1=0}}(-1)^m\frac{(2n+m+k-1)(2n+m+k-2)\cdots k}{n!\,(2n-1)!!}\\ \cdot\frac{(2n)!}{2!^{c_3}c_3!\,4!^{c_5}c_5!\cdots(2n)!^{c_{2n+1}}c_{2n+1}!}\prod_{i=1}^{2n+1}\left(\frac{y\binom{i-1}{2}}{i}\right)^{c_i}. \qquad (9.4)$$

We want to consider (9.4) modulo 2^e, and our goal is to show that, modulo 2^e, this expression is periodic with period length 2^e as a (polynomial) function in k.

Now, the first term in the last line of (9.4) is an integer due to the fact that

$$\sum_{i=1}^{2n+1}(2i)c_i=\sum_{i=1}^{2n+1}(2i+1)c_i-\sum_{i=1}^{2n+1}c_i=(2n+m)-m=2n,$$

which allows the application of Lemma 30 with (c_i) replaced by

$$(0,c_3,0,c_5,0,\dots,0,c_{2n+1}).$$

The product over i in the last line of (9.4) is a rational number with an odd denominator, since $c_i=0$ for all even i. Thus, the last line of (9.4) represents a rational number with an odd denominator, which has a non-negative 2-adic valuation. Likewise, the term $(2n-1)!!$ in the denominator of the expression in the first line of (9.4) is an odd number, and consequently also does not influence the 2-adic analysis of this expression.

We substitute $k+2^e$ in place of k in the remaining terms in the first line of (9.4) (ignoring the sign $(-1)^m$), and compute

$$\frac{(2n+m+k+2^e-1)(2n+m+k+2^e-2)\cdots(k+2^e)}{n!}\\ =\binom{2n+m+k+2^e-1}{n}(n+m+k+2^e-1)(n+m+k+2^e-2)\cdots(k+2^e)\\ \equiv\binom{2n+m+k+2^e-1}{n}(n+m+k-1)(n+m+k-2)\cdots k\pmod{2^e}\\ =(2n+m+k+2^e-1)(2n+m+k+2^e-2)\cdots(n+m+k+2^e)\\ \times(n+m+k-1)(n+m+k-2)\cdots(n+k)\binom{n+k-1}{n}\pmod{2^e}\\ \equiv\frac{(2n+m+k-1)(2n+m+k-2)\cdots k}{n!}\pmod{2^e}.$$

If we use this congruence in (9.4), then the periodicity of this expression in k with period length 2^e becomes apparent.

This finishes the proof of the theorem. ☐

10. The sequence $(d(n))_{n\ge 0}$ modulo powers of 2

Now we are in the position to prove our second main result, namely Part 3 of Theorem 1.

Theorem 34. *The sequence $(d(n))_{n\ge0}$, when taken modulo any fixed 2-power 2^e with $e \ge 3$, is purely periodic with (not necessarily minimal) period length 2^{e-1}. Modulo 4, the sequence is purely periodic with period length 4, the first few values of the sequence (modulo 4) being given by*

$$1, 1, 3, 3, 1, \dots .$$

Proof. Suppose first that $e \ge 3$. By (9.2) with $y(i) = u(i)$ for all i, we have $R^{-1}(2n, 2k) \equiv 0 \pmod{2^e}$ for $n \ge k + e$, due to the factor 2^{n-k} that arises under the corresponding substitution. Thus, the relation (2.12) becomes

$$\begin{aligned} d(n) &\equiv \sum_{k=\max\{0,n-e+1\}}^{n} R^{-1}(2n, 2k)v(k) \pmod{2^e} \\ &\equiv \sum_{k=0}^{\min\{n,e-1\}} R^{-1}(2n, 2n-2k)v(n-k) \pmod{2^e}. \end{aligned} \tag{10.1}$$

By Theorem 31 with $x(j) = \prod_{\ell=1}^{j}(4\ell-3)^2$ for all j, the sequence $(v(n))_{n\ge0}$ is (purely) periodic modulo 2^e with period length 2^{e-1}, and, by Theorem 33 with $y(j) = u(j)$ for all j, k and n interchanged, and subsequently n replaced by $2n-2k$, the sequence $\big(R^{-1}(2n, 2n-2k)\big)_{n\ge0}$ is (purely) periodic modulo 2^e with period length 2^{e-1}. There is a little detail that needs to be addressed here: what is the meaning of $R^{-1}(2n, 2n-2k)$ if $n < k$? So far we have not given a meaning to this in that case. However, the expression for $R^{-1}(2n+k, k)$ provided by (9.2) makes it easy to define the appropriate extension. Namely, as we said earlier, this expression is a polynomial in k and therefore it gives a meaning to $R^{-1}(2n+k, k)$ for all — positive or negative — integers k. Moreover, as long as $-2n \le k < 0$, the term $R^{-1}(2n+k, k)$ vanishes because of the appearance of the binomial coefficient $\binom{2n+m+k-1}{2n+m}$ in (9.2). Furthermore, the periodicity argument still applies to the extended sequence. Altogether, this allows us to relax the upper bound on the summation index k in (10.1) to

$$d(n) = \sum_{k=0}^{e-1} R^{-1}(2n, 2n-2k)v(n-k) \pmod{2^e}.$$

The above arguments show in particular that each summand on the right-hand side is (purely) periodic modulo 2^e with (not necessarily minimal) period length 2^{e-1}. Since these are finitely many summands, the same must hold for $d(n)$.

The assertion of the theorem concerning the behaviour of the sequence modulo 4 is a direct consequence of Theorem 32 with $x(1) = 1$ and Theorem 33 with $y(j) = u(j)$ for all j. ☐

11. The inverse of the matrix $\mathbf{R}$ modulo prime powers p^e with $p \equiv 1 \pmod 4$

This section prepares for the proof of our third main result, given in the subsequent section. The goal is to establish periodicity of $R^{-1}(2n, 2k)$ modulo powers of a prime p with $p \equiv 1 \pmod 4$, when considered as a sequence in n. This will eventually be achieved in Theorem 41. Similar to Section 9, we actually prove a polynomial refinement in which the number $u(j)$ that appears in the definition of the matrix entries $R^{-1}(2n, 2k)$ (cf. (2.11)) is replaced by an integer $y(j)$, $j = 0, 1, \dots$, with the restriction that $y(j)$ is divisible by p^e for $j \ge \lceil ep/2 \rceil$. The corresponding analysis is the most demanding one in this article. Already the final periodicity result in (11.21) (with "supporting" powers $p^{\lfloor 2k/p \rfloor}$ on both sides) indicates that matters are much more delicate here. While our starting point is again the expansion (9.2) (with the appropriate substitutions; see (11.22)), the analysis of the summand modulo powers of p is much more intricate here. The corresponding auxiliary results are the subject of Lemmas 35–40.

We start with a lower bound for the p-adic valuation of the summand in (11.22) in the "generic" case.

Lemma 35. *Let p be a prime with $p \equiv 1 \pmod 4$ and let $\big(y(n)\big)_{n \ge 0}$ be an integer sequence with the property that $v_p\big(y(n)\big) \ge e$ for $n \ge \left\lceil \frac{ep}{2} \right\rceil$. For all positive integers n and k, and non-negative integers m and c_i, $1 \le i \le 2n-2k$, with $\sum_{i=1}^{2n-2k} i c_i = 2n - 2k + m$, $\sum_{i=1}^{2n-2k} c_i = m$, and $c_i = 0$ for all even i, we have*

$$v_p\left(\frac{(2n+m-1)!}{(2k-1)!\prod_{i=1}^{2n-2k} i!^{c_i}\, c_i!}\prod_{i=1}^{2n-2k} y^{c_i}\left(\tfrac{i-1}{2}\right)\right)$$
$$\ge \#\Big(\text{carries when adding } (2n+m-1-pc_p)_p \text{ and } (pc_p)_p\Big)$$
$$+\#\Big(\text{carries when adding } (2n-2k+m-pc_p)_p \text{ and } (2k-1)_p\Big)$$
$$+\tfrac{1}{2(p-1)}(2n-2k+m-pc_p) - \tfrac{1}{p-1}s_p(2n-2k+m-pc_p). \quad (11.1)$$

Remark 36. For non-negative integers N, we have

$$\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) \ge -\tfrac{1}{2}.$$

Thus, although the last line in (11.1) can be negative, the sum of the two numbers of carries on the right-hand side of (11.1) is still a lower bound for the p-adic valuation on the left-hand side since the latter is an integer.

Proof of Lemma 35. By Legendre's formula in Lemma 3, the p-adic valuation on the left-hand side of (11.1) equals

$$\begin{aligned} v_p\left(\frac{(2n+m-1)!}{(2k-1)!\prod_{i=1}^{2n-2k} i!^{c_i}\, c_i!}\prod_{i=1}^{2n-2k} y^{c_i}\left(\tfrac{i-1}{2}\right)\right) &= \frac{1}{p-1}\Bigg(2n-2k+m-s_p(2n+m-1)+s_p(2k-1) \\ &\quad -\sum_{i=1}^{2n-2k}\Big(c_i i - c_i s_p(i) + c_i - s_p(c_i)\Big)\Bigg) + \sum_{i=1}^{2n-2k} c_i v_p\Big(y\big(\tfrac{i-1}{2}\big)\Big). \end{aligned} \tag{11.2}$$

We consider the terms involving c_i on the right-hand side of (11.2) separately. Concerning these, we claim that the following lower bound holds for all odd $i \geq 3$ with $i \neq p$:

$$\frac{1}{p-1}\big(-(i+1)c_i + c_i s_p(i) + s_p(c_i)\big) + c_i v_p\Big(y\big(\tfrac{i-1}{2}\big)\Big) \geq -\frac{i c_i}{2(p-1)}. \tag{11.3}$$

Multiplying both sides by $2(p-1)$ and using our divisibility assumption for $y\big(\frac{i-1}{2}\big)$, we see that the above claim will follow from the estimate

$$-(i+2)c_i + 2c_i s_p(i) + 2s_p(c_i) + 2(p-1)c_i\left\lfloor \tfrac{i-1}{p}\right\rfloor \geq 0.$$

This inequality can now indeed easily be verified for $3 \leq i < p$, for $p < i < 2p$, for $i = 2p+1$, and finally for $2p+3 \leq i$ making use of the simple inequality $\left\lfloor \frac{i-1}{p}\right\rfloor \geq \frac{i-p}{p}$. This proves our claim in (11.3).

We use (11.3) in (11.2) for $i \neq p$, keeping the terms for $i = p$ unchanged. Thereby, we obtain

$$\begin{aligned} v_p\left(\frac{(2n+m-1)!}{(2k-1)!\prod_{i=1}^{2n-2k} i!^{c_i}\, c_i!}\prod_{i=1}^{2n-2k} y^{c_i}\left(\tfrac{i-1}{2}\right)\right) &\geq \frac{1}{p-1}\left(2n-2k+m-pc_p+s_p(c_p)-s_p(2n+m-1)+s_p(2k-1)-\frac{1}{2}\sum_{\substack{i=1\\ i\neq p}}^{2n-2k} i c_i\right) \\ &= \frac{1}{2(p-1)}(2n-2k+m-pc_p) + \frac{1}{p-1}\big(s_p(pc_p)-s_p(2n+m-1)+s_p(2k-1)\big) \\ &= \frac{1}{2(p-1)}(2n-2k+m-pc_p) - \frac{1}{p-1}s_p(2n-2k+m-pc_p) \\ &\quad + \frac{1}{p-1}\big(s_p(pc_p)+s_p(2n+m-1-pc_p)-s_p(2n+m-1)\big) \\ &\quad + \frac{1}{p-1}\big(s_p(2k-1)+s_p(2n-2k+m-pc_p)-s_p(2n+m-1-pc_p)\big). \end{aligned} \tag{11.4}$$

By Lemma 5, the next-to-last line in (11.4) equals the first number of carries that appears on the right-hand side of (11.1), while the last line in (11.4) equals the second number of carries on the right-hand side of (11.1). Thus, we have established (11.1). $\square$

In a special case, the bound from the previous lemma can be slightly improved.

Lemma 37. *To the assumptions of Lemma* 35 *we add the conditions that* $c_i = 0$ *for* $i \ge 2p$ *and that* $c_i < p$ *for* $1 \le i < p$ *and for* $p < i < 2p$. *Then we have*

$$v_p\left(\frac{(2n+m-1)!}{(2k-1)!\prod_{i=1}^{2n-2k} i!^{c_i}\, c_i!}\prod_{i=1}^{2n-2k} y^{c_i}\left(\tfrac{i-1}{2}\right)\right)$$
$$\ge \#\Big(\text{carries when adding } (2n+m-1-pc_p)_p \text{ and } (pc_p)_p\Big)$$
$$+\#\Big(\text{carries when adding } (2n-2k+m-pc_p)_p \text{ and } (2k-1)_p\Big)$$
$$+\tfrac{1}{p-1}(2n-2k+m-pc_p) - \tfrac{1}{p-1}s_p(2n-2k+m-pc_p). \quad (11.5)$$

Remark 38. The only difference between (11.5) and (11.1) is a "missing" factor of 2 in the denominator of the first term in the last line of (11.5). Now, by Legendre's formula in Lemma 3, this last line equals the p-adic valuation of $(2n-2k+m-pc_p)!$ and is therefore non-negative (as opposed to the last line in (11.1); cf. Remark 36).

Proof of Lemma 37. We use again the identity (11.2). At this point, we observe that the additional conditions on the c_i's imply that the contribution of c_i with $1 \le i < 2p$ and $i \ne p$ in (11.2) is non-negative. Indeed, this contribution is

$$-\frac{1}{p-1}\big(c_i i - c_i s_p(i) + c_i - s_p(c_i)\big) + c_i v_p\Big(y\big(\tfrac{i-1}{2}\big)\Big)$$
$$= -\frac{1}{p-1}\big(ic_i - c_i s_p(i)\big) + c_i v_p\Big(y\big(\tfrac{i-1}{2}\big)\Big). \quad (11.6)$$

since $c_i < p$. If $i < p$, then we have $s_p(i) = i$ and hence the value in (11.6) is non-negative. If, on the other hand, $p < i < 2p$, then we have $s_p(i) = i - p + 1$ and $v_p\Big(y\big(\tfrac{i-1}{2}\big)\Big) \ge 1$, and therefore the value in (11.6) is again non-negative.

For the remaining terms in (11.2), we compute

$$\frac{1}{p-1}\big(2n-2k+m-s_p(2n+m-1)+s_p(2k-1)-pc_p+s_p(c_p)\big)$$
$$= \frac{1}{p-1}(2n-2k+m-pc_p) - \frac{1}{p-1}s_p(2n-2k+m-pc_p)$$
$$+\frac{1}{p-1}\big(s_p(2n+m-1-pc_p)+s_p(pc_p)-s_p(2n+m-1)\big)$$
$$+\frac{1}{p-1}\big(s_p(2n-2k+m-pc_p)+s_p(2k-1)-s_p(2n+m-1-pc_p)\big). \quad (11.7)$$

By Lemma 5, the last line is the number of carries that appears in the next-to-last line in (11.5). For the same reason, the next-to-last line in (11.7) is the number of carries that appears in the third line from below in (11.5). This completes the proof. $\square$

The next lemma collects together several auxiliary inequalities that concern the right-hand side of (11.1). They will be used in subsequent arguments.

Lemma 39. *Let p be a prime with $p \equiv 1 \pmod 4$ and N and ℓ non-negative integers with $p^\ell \le N < p^{\ell+1}$. Then*

$$\left\lfloor \frac{N}{p} \right\rfloor \ge \ell, \qquad \text{for } \ell \ge 0, \tag{11.8}$$

$$\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) > \tfrac{N}{2p} - \tfrac{3}{2}, \qquad \text{for } \ell \ge 0, \tag{11.9}$$

$$\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) \ge \ell + \tfrac{3}{8}, \qquad \text{for } \ell \ge 2, \tag{11.10}$$

$$\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) \ge \ell, \qquad \text{for } \ell \ge 1 \text{ and } N \ge p^\ell(p-1), \tag{11.11}$$

$$\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) > 0, \qquad \text{for } 2p \le N < p^2. \tag{11.12}$$

Proof. The first inequality is obvious.

For the proof of (11.9), we write $N = n_0 + n_1 p + n_2 p^2$ with $0 \le n_0, n_1 < p$ and $n_2 \ge 0$, and then estimate the difference of the left-hand side and $N/(2p)$,

$$\begin{aligned}
\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) - \tfrac{N}{2p} &= \tfrac{N}{2p(p-1)} - \tfrac{1}{p-1}s_p(N) \\
&= \tfrac{1}{2p(p-1)}\big(n_0 + n_1 p + n_2 p^2 - 2pn_0 - 2pn_1 - 2ps_p(n_2)\big) \\
&\ge \tfrac{1}{2p(p-1)}\big(-n_0(2p-1) - n_1 p + n_2(p^2 - 2p)\big) \\
&\ge -\tfrac{2p-1}{2p} - \tfrac{1}{2} > -\tfrac{3}{2},
\end{aligned}$$

as desired.

In order to show (11.10), let $N = n_0 + n_1 p + \cdots + n_\ell p^\ell$ with $0 \le n_i < p$ for all i and $n_\ell > 0$. Then we have

$$\begin{aligned}
\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) &= \tfrac{1}{2(p-1)}\big(n_0 + n_1 p + \cdots + n_\ell p^\ell\big) - \tfrac{1}{p-1}(n_0 + n_1 + \cdots + n_\ell) \\
&= \tfrac{1}{2(p-1)}\big(-n_0 + n_1(p-2) + \cdots + n_\ell(p^\ell - 2)\big) \\
&\ge \tfrac{1}{2(p-1)}\big(-(p-1) + (p^\ell - 2)\big) \qquad (11.13) \\
&= \tfrac{1}{2(p-1)}(p^\ell - 2) - \tfrac{1}{2}. \qquad (11.14)
\end{aligned}$$

Now, it is a simple exercise to show that

$$p^\ell \ge 2(p-1)\ell + p^2 - 4p + 4, \quad \text{for } \ell \ge 2 \text{ and } p \ge 5.$$

We use this in (11.14) to get

$$\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) \ge \ell + \tfrac{1}{2(p-1)}(p^2 - 4p + 2) - \tfrac{1}{2} = \ell + \tfrac{1}{2}(p-4) - \tfrac{1}{2(p-1)} \ge \ell + \tfrac{3}{8},$$

since $p \ge 5$.

For the proof of the strengthening in (11.11), we observe that, instead of the last line in (11.14), we may improve that lower bound to

$$\tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) \ge \tfrac{1}{2(p-1)}\big(-(p-1) + (p-1)(p^\ell - 2)\big) = \tfrac{1}{2}(p^\ell - 3).$$

The fact that this is at least ℓ for $\ell \ge 1$ and $p \ge 5$ is straightforward to verify.

Finally we turn to the proof of (11.12). We write $N = n_0 + n_1 p$ with $0 \le n_0 < p$ and $2 \le n_1 < p$, and compute

$$\begin{aligned} \tfrac{1}{2(p-1)}N - \tfrac{1}{p-1}s_p(N) &= \tfrac{1}{2(p-1)}(n_0 + n_1 p) - \tfrac{1}{p-1}(n_0 + n_1)\\ &= \tfrac{1}{2(p-1)}\big(-n_0 + n_1(p-2)\big)\\ &\ge \tfrac{1}{2(p-1)}\big(-(p-1) + 2(p-2)\big)\\ &= \tfrac{1}{2(p-1)}\big(p-3\big) > 0, \end{aligned}$$

since $p \ge 5$.

This completes the proof of the lemma. □

The purpose of the lemma below is to "convert" the lower bound from Lemmas 35 and 37 into a form that is needed in the proof of the upcoming Theorem 41.

Lemma 40. *Let p be a prime with $p \equiv 1 \pmod 4$ and let $\big(y(n)\big)_{n\ge0}$ be an integer sequence with the property that $v_p\big(y(n)\big) \ge e$ for $n \ge \lceil \frac{ep}{2} \rceil$. For all positive integers n and k, and non-negative integers m and c_i, $1 \le i \le 2n-2k$, with $\sum_{i=1}^{2n-2k} ic_i = 2n-2k+m$, $\sum_{i=1}^{2n-2k} c_i = m$, and $c_i = 0$ for all even i, we have*

$$\left\lfloor \frac{2k}{p} \right\rfloor + v_p\left(\frac{(2n+m-1)!}{(2k-1)!\prod_{i=1}^{2n-2k} i!^{c_i}\, c_i!} \prod_{i=1}^{2n-2k} y^{c_i}\left(\tfrac{i-1}{2}\right)\right) \ge 1 + \max_{c_p < i \le \lfloor (2n+m-1)/p \rfloor} v_p(i). \tag{11.15}$$

By convention, if $c_p = \lfloor (2n+m-1)/p \rfloor$ the right-hand side is interpreted as zero (so that the inequality is trivially true).

Proof. We proceed in a similar manner as in the proof of Lemma 27.

Choose α, β, and γ such that $2n+m-1 = n_0 p^\alpha + n_1$, with n_0 not divisible by p and $n_1 < p^{\beta+1}$, $p^\beta \le 2n+m-1-pc_p < p^{\beta+1}$, and $p^\gamma \le 2k-1 < p^{\gamma+1}$. These conditions imply that the p-adic representations can be schematically indicated as

$$\begin{array}{rl} & \quad\;\; \overset{\alpha}{\downarrow} \qquad\quad\; \overset{\beta}{\downarrow} \;\;\; \overset{\gamma}{\downarrow} \\ (2n+m-1)_p = & \dots ?\,0 \dots 0 * \dots\dots\, \dagger \\ (2n+m-1-pc_p)_p = & \qquad\qquad\;\; ? \dots\dots\, \dagger \\ (2k-1)_p = & \qquad\qquad\qquad\;\; ? \dots * \end{array} \tag{11.16}$$

with the meaning that the shown ? in the first line is the α-th digit counted from right (the counting starting with 0), that the left-most (non-zero) digit of the p-adic representation of $2n+m-1-pc_p$ is the β-th digit, and that the left-most (non-zero) digit of the p-adic representation of $2k-1$ is the γ-th digit. The symbol $*$ indicates an arbitrary digit (between 0 and $p-1$) — *not necessarily the same* in the first and in the third line, the symbol ? indicates an arbitrary *non-zero* digit (between 1 and $p-1$) — *not necessarily the same* in lines 1–3, while † indicates a digit which *is the same* in the first and in the second line. The reader is advised to consult (11.16) constantly while going through the subsequent arguments.

We first dispose of the simple case in which $\beta = 0$ (and hence $\gamma = 0$): in that case, by considering the schematic representation in (11.16), it becomes apparent that $c_p =$

$\lfloor (2n+m-1)/p \rfloor$. According to the convention that we have made in the statement of the lemma, there is nothing to prove. Hence, from now on, we assume that $\beta \ge 1$.

Now we distinguish two main cases, depending on the relative sizes of n_1 and $2n+m-1-pc_p$.

CASE 1: $n_1 < 2n+m-1-pc_p$. Here, by inspection of (11.16), we see that

$$\max_{c_p < i \le \lfloor (2n+m-1)/p \rfloor} v_p(i) = \alpha - 1, \tag{11.17}$$

since we obtain the p-adic representation of $\lfloor (2n+m-1)/p \rfloor$ by simply deleting the right-most digit (indicated by † in (11.16)) in the p-adic representation of $2n+m-1$, and since pc_p is the difference of the first two lines in (11.16).

On the other hand, by Lemma 35, the left-hand side of (11.15) is bounded below by

$$\begin{multlined} \left\lfloor \tfrac{2k}{p} \right\rfloor + \#\Big(\text{carries when adding } (2n+m-1-pc_p)_p \text{ and } (pc_p)_p\Big) \\ + \#\Big(\text{carries when adding } (2n-2k+m-pc_p)_p \text{ and } (2k-1)_p\Big) \\ + \tfrac{1}{2(p-1)}(2n-2k+m-pc_p) - \tfrac{1}{p-1} s_p(2n-2k+m-pc_p). \end{multlined} \tag{11.18}$$

Clearly, the number of carries when adding two numbers A and B in their p-adic representations equals the number of carries when performing the subtraction of, say, A from $A+B$. In view of this observation, inspection of (11.16) yields that the number of carries in the first line of (11.18) is at least $\alpha-\beta$. Hence, comparison of (11.15) with (11.17) shows that what remains to demonstrate is that

$$\begin{multlined} \left\lfloor \tfrac{2k}{p} \right\rfloor + \#\Big(\text{carries when adding } (2n-2k+m-pc_p)_p \text{ and } (2k-1)_p\Big) \\ + \tfrac{1}{2(p-1)}(2n-2k+m-pc_p) - \tfrac{1}{p-1} s_p(2n-2k+m-pc_p) \ge \beta. \end{multlined} \tag{11.19}$$

In order to accomplish this, we need to discuss several subcases.

If $\beta > \gamma+1$ and $\gamma \ge 0$, then $2n-2k+m-pc_p \ge p^\beta$ or $p^{\beta-1} \le 2n-2k+m-pc_p < p^\beta$. In the former case we may use (11.10) to conclude that the left-hand side of (11.19) is at least $\beta + \frac{3}{8}$, while in the latter case the number of carries in (11.19) must be at least 1 and $2n-2k+m-pc_p$ must be at least $(p-1)p^{\beta-1}$; consequently (11.11) leads to the conclusion that the left-hand side of (11.19) is at least $1+(\beta-1)=\beta$, both confirming the inequality in (11.19).

The case where $\beta = 1$ and $\gamma = 0$ needs a special treatment, to which we will come at the end of this discussion of subcases.

If $\beta = \gamma \ge 1$, then we use (11.8) to see that $\lfloor 2k/p \rfloor$ is at least $\gamma = \beta$, again confirming (11.19). We point out that for this conclusion we implicitly used the observation of Remark 36.

If $\beta = \gamma + 1$ and $\gamma \ge 1$, then either $2n-2k+m-pc_p \ge p^\beta$ or the number of carries in (11.19) is at least 1. In the former case, we may use (11.10) to see that the last line on the left-hand side of (11.19) is at least β, as desired. In the latter case, the inequality (11.8) specialised to $N = 2k > p^\gamma$ implies that the left-hand side of (11.19) is at least $1+\gamma = \beta$, again confirming (11.19). Here also, this conclusion requires implicitly the observation of Remark 36.

Finally we discuss the remaining case where $\beta=1$ and $\gamma=0$. Here, we have either $2p\le 2n-2k+m-pc_p<p^2$, or $p\le 2n-2k+m-pc_p<2p$, or $1\le 2n-2k+m-pc_p<p$. In the first case, the inequality (11.12) implies that the third line on the left-hand side of (11.19) is strictly positive. Since this is a lower bound for the left-hand side of (11.15), an integer, it is an effective lower bound of $1=\beta$, as desired. For the second and third cases, we observe that, since by assumption

$$2n-2k+m-pc_p=\sum_{\substack{i=1\\ i\ne p}}^{2n-2k} ic_i,$$

we must have $c_i=0$ for $i\ge 2p$, $c_i\le 1$ for $p<i<2p$, and $c_i<p$ for $3\le i<p$. Thus, the conditions of Lemma 37 are satisfied. We may therefore bound the left-hand side of (11.15) by

$$\begin{aligned}\#\Big(&\text{carries when adding } (2n+m-1-pc_p)_p \text{ and } (pc_p)_p\Big)\\ &+\#\Big(\text{carries when adding } (2n-2k+m-pc_p)_p \text{ and } (2k-1)_p\Big)\\ &\qquad+\tfrac{1}{p-1}(2n-2k+m-pc_p)-\tfrac{1}{p-1}s_p(2n-2k+m-pc_p). \qquad (11.20)\end{aligned}$$

We have already found that the number of carries in the first line is at least $\alpha-\beta=\alpha-1$. On the other hand, under the assumption on $2n-2k+m-pc_p$ in the second case, the expression in the third line equals 1. Together with (11.17), this confirms again (11.15). In the third case, there must be at least one carry when adding $2n-2k+m-pc_p$ and $2k-1$ in their p-adic representations, meaning that the second line in (11.20) equals 1. This again confirms (11.15).

Case 2: $n_1\ge 2n+m-1-pc_p$. Now, by inspection of (11.16), we see that

$$\max_{c_p<i\le\lfloor(2n+m-1)/p\rfloor} v_p(i)\le\beta-1.$$

A moment's thought will convince the reader that we are in exactly the same situation as in Case 1: we must either prove (11.19) or, in the case where $\beta=1$ and $\gamma=0$, show that the sum of the second and third lines in (11.20) is at least 1. Hence, the remaining steps are the same as the corresponding ones in Case 1, completing the proof. ☐

We are now in the position to prove the announced "twisted" periodicity of the matrix entries $R_y^{-1}(2n,2k)$ as given by (9.1) modulo prime powers p^e, when considered as a sequence in n.

Theorem 41. *Let p be a prime with $p\equiv 1 \pmod 4$ and let $\big(y(n)\big)_{n\ge0}$ be an integer sequence with the property that $v_p\big(y(n)\big)\ge e$ for $n\ge\lceil\frac{ep}{2}\rceil$. For all positive integers n, k, and e, we have*

$$\begin{aligned}p^{\lfloor 2k/p\rfloor}&R_y^{-1}\left(2n+p^{e-1}(p-1),2k\right)\\ &\equiv y^{p^{e-1}}\left(\tfrac{p-1}{2}\right)\cdot(-1)^{(p-5)/4}p^{\lfloor 2k/p\rfloor}R_y^{-1}(2n,2k) \pmod{p^e}, \quad \text{for } n\ge e+1. \qquad (11.21)\end{aligned}$$

In particular, if $y\big(\frac{p-1}{2}\big)$ is a quadratic residue modulo p and coprime to p, then the sequence $\big(p^{\lfloor 2k/p\rfloor}R_y^{-1}(2n,2k)\big)_{n\ge e+1}$, when taken modulo any fixed p-power p^e with $e\ge1$, is purely periodic with (not necessarily minimal) period length $\frac14 p^{e-1}(p-1)^2$.

Proof. The last assertion follows from Euler's theorem, the fact that $\varphi(p^e) = p^{e-1}(p-1)$, from our assumption that $y\big(\frac{p-1}{2}\big)$ is a quadratic residue modulo p and coprime to p, and the easily proven property that, if $c \equiv d \pmod p$, then $c^{p^{e-1}} \equiv d^{p^{e-1}} \pmod{p^e}$ for all positive integers e.

We turn to the proof of (11.21). Replacement of k by $2k$ and of n by $n-k$ in (9.2) leads to

$$R_y^{-1}(2n,2k) = \sum_{m\ge 0} \sum_{\substack{(c_i)\in\mathcal{P}^o_{2n-2k+m,m}\\ c_1=0}} (-1)^m 2^{n-k}\binom{2n+m-1}{2n-2k+m}$$

$$\cdot \frac{(2n-2k+m)!}{3!^{c_3}c_3!\,5!^{c_5}c_5!\cdots(2n-2k+1)!^{c_{2n-2k+1}}c_{2n-2k+1}!}\prod_{i=1}^{2n-2k+1} y^{c_i}\big(\tfrac{i-1}{2}\big) \pmod{p^e}. \quad (11.22)$$

The earlier observation in (9.3) also applies here — with n replaced by $n-k$ — so that $m \le n-k \le n$. In particular, the sum over m in (11.22) is finite.

The fraction in the expression in (11.22) is an integer since, by Lemma 30, it is the number of all partitions of $\{1,2,\dots,2n-2k+m\}$ into c_i blocks of size i, $i = 3,5,\dots,2n-2k+1$.

Let $T(n,k,m,(c_i))$ denote the summand in (11.22); that is,

$$T(n,k,m,(c_i)) := (-1)^m 2^{n-k}\frac{(2n+m-1)!}{(2k-1)!}$$

$$\times \frac{1}{3!^{c_3}c_3!\,5!^{c_5}c_5!\cdots(2n-2k+1)!^{c_{2n-2k+1}}c_{2n-2k+1}!}\prod_{i=1}^{2n-2k+1} y^{c_i}\big(\tfrac{i-1}{2}\big) \quad (11.23)$$

for a non-negative integer m and $(c_i)\in\mathcal{P}^o_{2n-2k+m,m}$ with $c_1 = 0$. In view of the previous observation, $T(n,k,m,(c_i))$ is an integer multiplied by a monomial in the $y(j)$'s.

We want to prove the periodicity assertion in (11.21). We are going to prove that, for all positive integers a, we have

$$p^{\lfloor 2k/p\rfloor}T\big(n+\tfrac12 ap^{e-1}(p-1),k,m,(c_i)\big) \equiv 0 \pmod{p^e}, \quad \text{for } n\ge e+1 \text{ and } c_p < ap^{e-1}, \quad (11.24)$$

and

$$p^{\lfloor 2k/p\rfloor}T\big(n+\tfrac12 ap^{e-1}(p-1),k,m+ap^{e-1},(\tilde c_i)\big)$$
$$\equiv y^{ap^{e-1}}\big(\tfrac{i-1}{2}\big)\cdot(-1)^{a(p-5)/4}p^{\lfloor 2k/p\rfloor}T\big(n,k,m,(c_i)\big) \pmod{p^e}, \quad \text{for } n < p^{e-1}(p-1), \quad (11.25)$$

with $\tilde c_p = c_p + ap^{e-1}$, and $\tilde c_i = c_i$ for all other i.

We claim that these two congruences together imply

$$p^{\lfloor 2k/p\rfloor}R_y^{-1}(2n,2k)$$
$$\equiv y^{ap^{e-1}}\big(\tfrac{p-1}{2}\big)\cdot(-1)^{a(p-5)/4}p^{\lfloor 2k/p\rfloor}R_y^{-1}\big(2n-ap^{e-1}(p-1),2k\big) \pmod{p^e}, \quad (11.26)$$

where a is maximal such that $n-\frac12 ap^{e-1}(p-1)\ge e+1$. It is obvious that, in its turn, this congruence implies (11.21), and thus the theorem.

In order to prove the claim, we rewrite the left-hand side of (11.26) in terms of our short notation (11.23),

$$p^{\lfloor 2k/p\rfloor} R_y^{-1}(2n,2k) = \sum_{m\ge 0} \sum_{\substack{(c_i)\in\mathcal P^o_{2n-2k+m,m}\\ c_1=0}} p^{\lfloor 2k/p\rfloor} T(n,k,m,(c_i)). \tag{11.27}$$

We now consider the summands $p^{\lfloor 2k/p\rfloor} T(n,k,m,(c_i))$ on the right-hand side for the various choices of m and (c_i). Let b be maximal such that $c_p - bp^{e-1} \ge 0$. If $b < a$, then we may use (11.24) with a replaced by $b+1$ to conclude that the corresponding summand on the right-hand side of (11.27) vanishes modulo p^e. On the other hand, if $b \ge a$, then we use (11.25) with n replaced by $n - \frac{1}{2}ap^{e-1}(p-1)$, m replaced by $m - ap^{e-1}$ (this is indeed non-negative since $m \ge c_p$), and c_p replaced by $c_p - ap^{e-1}$ to conclude that

$$\begin{aligned} &p^{\lfloor 2k/p\rfloor} T(n,k,m,(c_i))\\ &\equiv y^{ap^{e-1}}\left(\tfrac{p-1}{2}\right)\cdot(-1)^{a(p-5)/4} p^{\lfloor 2k/p\rfloor} T\left(n-\tfrac12 ap^{e-1}(p-1),k,m-ap^{e-1},(\hat c_i)\right) \pmod{p^e}, \end{aligned}$$

with $\hat c_p = c_p - ap^{e-1}$ and $\hat c_i = c_i$ for all other i. Thus, we obtain

$$\begin{aligned} p^{\lfloor 2k/p\rfloor} R_y^{-1}(2n,2k) &\equiv y^{ap^{e-1}}\left(\tfrac{p-1}{2}\right)\cdot(-1)^{a(p-5)/4}\\ &\times \sum_{m\ge 0} \sum_{\substack{(\hat c_i)\in\mathcal P^o_{2n-2k+m-ap^e,m-ap^{e-1}}\\ \hat c_1=0}} p^{\lfloor 2k/p\rfloor} T\left(n-\tfrac12 ap^{e-1}(p-1),k,m-ap^{e-1},(\hat c_i)\right)\\ &\pmod{p^e}, \end{aligned}$$

with a maximal such that $n - \frac{1}{2}ap^{e-1}(p-1) \ge e+1$. Recalling (11.27), we are then directly led to our claim (11.26).

Now we provide the proofs of the crucial congruences (11.24) and (11.25).

Proof of (11.24). Let $\lfloor 2k/p\rfloor = l$. If $l \ge e$, there is nothing to prove. Therefore, we assume $l < e$ from now on.

If

$$2\left(n+\tfrac12 ap^{e-1}(p-1)\right) - 2k + m - pc_p \ge (2e-2l+1)p,$$

then Lemma 35 with n replaced by $n + \frac12 ap^{e-1}(p-1)$ and (11.9) together imply that

$$v_p\big(T\big(n+\tfrac12 ap^{e-1}(p-1),k,m,(c_i)\big)\big) > \tfrac{(2e-2l+1)p}{2p} - \tfrac32 = e-l-1.$$

In other words, the left-hand side — being an integer — is at least $e-l$. In combination with $\lfloor 2k/p\rfloor = l$, this establishes (11.24) in this case.

On the other hand, if

$$2\left(n+\tfrac12 ap^{e-1}(p-1)\right) - 2k + m - pc_p < (2e-2l+1)p,$$

then, since $m \ge c_p$ and $2k \le lp + (p-1)$, we infer

$$2n + ap^{e-1}(p-1) - lp - (p-1) - (p-1)c_p < (2e-2l+1)p.$$

Equivalently, we have

$$c_p > \tfrac{1}{p-1}\big(2n-2ep-p+lp\big) + ap^{e-1} - 1.$$

This entails

$$2\left(n+\tfrac{1}{2}ap^{e-1}(p-1)\right)+m-1\ge 2n+ap^{e-1}(p-1)+c_p-1$$
$$>2n+ap^e+\tfrac{1}{p-1}\big(2n-2ep-p+lp\big)-2.$$

Since, by assumption, we have $n\ge e+1$, it follows that

$$2\left(n+\tfrac{1}{2}ap^{e-1}(p-1)\right)+m-1>2(e+1)+ap^e+\tfrac{1}{p-1}\big(2(e+1)-2ep-p+lp\big)-2$$
$$=ap^e-1+\tfrac{1}{p-1}\big(1+lp\big).$$

As the left-hand side is an integer, we conclude that

$$2\left(n+\tfrac{1}{2}ap^{e-1}(p-1)\right)+m-1\ge ap^e. \tag{11.28}$$

Now we use Lemma 40 with n replaced by $n+\frac{1}{2}ap^{e-1}(p-1)$ to see that $p^{\lfloor 2k/p\rfloor}T\big(n+\frac{1}{2}ap^{e-1}(p-1),k,m,(c_i)\big)$ is divisible by

$$p^{1+\max_{c_p<i\le\lfloor(2n+ap^{e-1}(p-1)+m-1)/p\rfloor}v_p(i)}.$$

As $c_p<ap^{e-1}$, and since, by (11.28), we have $\lfloor(2n+ap^{e-1}(p-1)+m-1)/p\rfloor\ge ap^{e-1}$, in the range $c_p<i\le\lfloor(2n+ap^{e-1}(p-1)+m-1)/p\rfloor$ we will find $i=ap^{e-1}$, and consequently $p^{\lfloor 2k/p\rfloor}T\big(n+\frac{1}{2}ap^{e-1}(p-1),k,m,(c_i)\big)$ is divisible by p^e.

Proof of (11.25). We substitute $n+\frac{1}{2}ap^{e-1}(p-1)$ for n, $m+ap^{e-1}$ for m, and c_p+ap^{e-1} for c_p in the definition of $T(n,k,m,(c_i))$ in (11.23). After little manipulation, we get

$$T\left(n+\tfrac{1}{2}ap^{e-1}(p-1),k,m+ap^{e-1},(\tilde{c}_i)\right)$$
$$=y^{ap^{e-1}}\big(\tfrac{p-1}{2}\big)(-1)^{m+ap^{e-1}}2^{n+\frac{1}{2}ap^{e-1}(p-1)-k}\frac{(2n+m+ap^e-1)!}{(2k-1)!}$$
$$\times\frac{1}{3!^{c_3}c_3!\,5!^{c_5}c_5!\cdots(2n-2k+1)!^{c_{2n-2k+1}}c_{2n-2k+1}!}\cdot\frac{c_p!}{p!^{ap^{e-1}}\,(c_p+ap^{e-1})!}\prod_{i=1}^{2n-2k+1}y^{c_i}\big(\tfrac{i-1}{2}\big). \tag{11.29}$$

We have

$$(-1)^{p^{e-1}}=-1 \tag{11.30}$$

and

$$2^{p^{e-1}(p-1)/2}\equiv(-1)^{(p-1)/4}\pmod{p^e}, \tag{11.31}$$

since for $p\equiv 1\pmod 8$ the residue class of 2 is a quadratic residue modulo p, while for $p\equiv 5\pmod 8$ it is not. Furthermore, we have

$$(p-1)!^{p^{e-1}}\equiv -1\pmod{p^e}, \tag{11.32}$$

as is seen by a straightforward induction on e based on Wilson's theorem. If we use (11.30)–(11.32) in (11.29), then we obtain

$$T\left(n+a\tfrac{p^{e-1}(p-1)}{2},k,m+ap^{e-1},(\tilde c_i)\right)$$
$$\equiv y^{ap^{e-1}\binom{p-1}{2}}(-1)^{m+a\frac{p-1}{4}}2^{n-k}\frac{(2n+m+ap^e-1)!}{(2k-1)!}$$
$$\times\frac{1}{3!^{c_3}c_3!\,5!^{c_5}c_5!\cdots(2n-2k+1)!^{c_{2n-2k+1}}c_{2n-2k+1}!}\cdot\frac{c_p!}{p^{ap^{e-1}}(c_p+ap^{e-1})!}\prod_{i=1}^{2n-2k+1}y^{c_i\binom{i-1}{2}}$$
$$\pmod{p^e}.\quad(11.33)$$

We have

$$\frac{(2n+m+ap^e-1)!}{(2n+m-1)!}\,p^{-ap^{e-1}}=p^{-ap^{e-1}}(2n+m+ap^e-1)\cdots(2n+m+1)(2n+m)$$
$$=\frac{\lfloor(2n+m+ap^e-1)/p\rfloor!}{\lfloor(2n+m-1)/p\rfloor!}\cdot[(2n+m+ap^e-1)\cdots(2n+m+1)(2n+m)]_p,\quad(11.34)$$

where $[a\cdot b\cdots z]_p$ denotes the product $a\cdot b\cdots z$ in which all factors divisible by p are omitted. Now we observe that $[b\cdot(b+1)\cdots(b+p^e-1)]_p$ forms a complete set of representatives of the multiplicative group $(\mathbb{Z}/p^e\mathbb{Z})^\times$. Consequently, the product is congruent to -1 modulo p^e. The term $[\,.\,]_p$ on the right-hand side of (11.34) consists of a such products. Therefore,

$$\frac{(2n+m+ap^e-1)!}{(2n+m-1)!}\,p^{-ap^{e-1}}\equiv(-1)^a\frac{\lfloor(2n+m+ap^e-1)/p\rfloor!}{\lfloor(2n+m-1)/p\rfloor!}\pmod{p^e}.$$

If we substitute this in (11.33), then we get

$$T\left(n+a\tfrac{p^{e-1}(p-1)}{2},k,m+ap^{e-1},(\tilde c_i)\right)\equiv y^{ap^{e-1}\binom{p-1}{2}}(-1)^{m+a\frac{p-5}{4}}2^{n-k}\frac{(2n+m-1)!}{(2k-1)!}$$
$$\times\frac{\lfloor(2n+m+ap^e-1)/p\rfloor!}{(c_p+ap^{e-1})!}\frac{c_p!}{\lfloor(2n+m-1)/p\rfloor!}$$
$$\times\frac{1}{3!^{c_3}c_3!\,5!^{c_5}c_5!\cdots(2n-2k+1)!^{c_{2n-2k+1}}c_{2n-2k+1}!}\prod_{i=1}^{2n-2k+1}y^{c_i\binom{i-1}{2}}$$
$$\equiv y^{ap^{e-1}\binom{p-1}{2}}(-1)^{m+a\frac{p-5}{4}}2^{n-k}\frac{(2n+m-1)!}{(2k-1)!}\prod_{i=c_p+1}^{\lfloor(2n+m-1)/p\rfloor}\frac{i\cdot p^{-v_p(i)}+ap^{e-v_p(i)-1}}{i\cdot p^{-v_p(i)}}$$
$$\times\frac{1}{3!^{c_3}c_3!\,5!^{c_5}c_5!\cdots(2n-2k+1)!^{c_{2n-2k+1}}c_{2n-2k+1}!}\prod_{i=1}^{2n-2k+1}y^{c_i\binom{i-1}{2}}\pmod{p^e}.$$
$$(11.35)$$

The reader should note that we wrote the first product over i in this particular form in order to make sure that the expressions $i\cdot p^{-v_p(i)}$ in the denominator are coprime to p.

Similarly to the proof of (8.26), we would like to simplify the terms $(i\cdot p^{-v_p(i)})+ap^{e-v_p(i)-1}$ to $i\cdot p^{-v_p(i)}$. For, assuming the validity of this simplification, the first product over i on the right-hand side of (11.35) would simplify to 1, and the remaining terms exactly equal $y^{ap^{e-1}}\left(\frac{p-1}{2}\right)T\big(n,k,m,(c_i)\big)$.

We claim that this simplification is indeed allowed, *provided both sides of* (11.35) *are multiplied by* $p^{\lfloor 2k/p\rfloor}$. (The reader should go back to (11.25) to see that this is indeed what we need.) For, by Lemma 40, we know that the "prefactor" of the first product over i on the right-hand side of (11.35) (that is, the right-hand side of (11.35) without that first product over i), multiplied by $p^{\lfloor 2k/p\rfloor}$, is an integer that is divisible by

$$p^{1+\max_{cp<i\le\lfloor(2n+m-1)/p\rfloor} v_p(i)}.$$

Hence, instead of calculating modulo p^e, we may reduce the first product over i on the right-hand side of (11.35) modulo

$$p^{e-1-\max_{cp<i\le\lfloor(2n+m-1)/p\rfloor} v_p(i)}.$$

(It should be observed here that the exponent in the last displayed expression is non-negative. Indeed, as we observed at the beginning of this proof, we have $m\le n$. Furthermore, by assumption, we have $n<p^{e-1}(p-1)$. Together, this implies that $\lfloor(2n+m-1)/p\rfloor\le 3p^{e-1}<p^e$.) This is exactly what we need to perform the desired simplification and the first product over i drops out.

This completes the proof of the theorem. □

12. The sequence $(d(n))_{n\ge0}$ modulo prime powers p^e with $p\equiv1 \pmod 4$

We are now able to prove our third main result, this one concerning the periodicity of $d(n)$ modulo prime powers p^e with $p\equiv1 \pmod 4$, announced in Part (2) of Theorem 1.

Theorem 42. *Let p be a prime number with $p\equiv1 \pmod 4$, and let e be some positive integer. Then the sequence $\big(d(n)\big)_{n\ge e+1}$ is purely periodic modulo p^e with (not necessarily minimal) period length $\frac14p^{e-1}(p-1)^2$.*

Proof. We start by recalling (2.12), that is

$$d(n)=\sum_{k=0}^{n}R^{-1}(2n,2k)v(k). \tag{12.1}$$

By Theorem 19, we know that $v(k)\equiv0 \pmod{p^e}$ for $k\ge\left\lceil\frac{ep}{2}\right\rceil$. Consequently, we may truncate the sum in (12.1) when we consider both sides modulo p^e. In fact, Theorem 19 says more precisely that $v(k)=p^{\lfloor 2k/p\rfloor}V(k,p)$, where $V(k,p)$ is an integer. Altogether, this leads to

$$\begin{aligned}d(n)&\equiv\sum_{k=0}^{\lfloor ep/2\rfloor}R^{-1}(2n,2k)p^{\lfloor 2k/p\rfloor}V(k,p)\pmod{p^e}\\&\equiv\sum_{k=1}^{\lfloor ep/2\rfloor}R^{-1}(2n,2k)p^{\lfloor 2k/p\rfloor}V(k,p)\pmod{p^e},\quad\text{for } n\ge1.\end{aligned}\tag{12.2}$$

We are indeed allowed to ignore the summand for $k=0$ since $R^{-1}(2n,0)=0$ for $n\ge1$, cf. Proposition 2. By Theorem 41 with $y(k)=u(k)$ for all k (see in particular the last paragraph of the statement; Theorem 11 provides the properties of $u(k)$ required by the theorem), the sequence $\big(p^{\lfloor 2k/p\rfloor}R^{-1}(2n,2k)\big)_{n\ge e+1}$ is purely periodic when taken modulo p^e with (not necessarily minimal) period length $\frac{1}{4}p^{e-1}(p-1)^2$. Since, by (12.2), the sequence $\big(d(n)\big)_{n\ge e+1}$, when taken modulo p^e, is a finite linear combination of the sequences $\big(p^{\lfloor 2k/p\rfloor}R^{-1}(2n,2k)\big)_{n\ge e+1}$, $k=1,2,\dots$, it has the same periodicity behaviour. $\square$

It should be observed that the above argument, combined with (4.8), in fact proves a refinement of the periodicity of the sequence $\big(d(n)\big)_{n\ge e+1}$ that generalises (1.2), namely

$$d\left(n+\tfrac{p^{e-1}(p-1)}{2}\right)\equiv(-1)^{(p-5)/4}(3\cdot 7\cdot 11\cdots(2p-3))^{2p^{e-1}}d(n)\pmod{p^e},$$
$$\text{for } p\equiv 1 \pmod 4 \text{ and } n\ge e+1. \quad (12.3)$$

13. Some conjectures and speculations

In this final section, we report on some conjectures concerning congruence properties of the sequences $\big(u(n)\big)_{n\ge0}$, $\big(v(n)\big)_{n\ge0}$, and $\big(d(n)\big)_{n\ge0}$ that are suggested by extensive computer experiments. If true, they would further strengthen the results of our paper. Roughly speaking, the data suggest that it is possible to improve period lengths and bounds for odd prime powers p^e by a factor of 2. By contrast, it seems that, in our result in Section 10 on periodicity of $d(n)$ modulo powers of 2, the period length is the exact one.

Our first conjecture predicts that, for primes $p\equiv 3 \pmod 4$, the vanishing of $u(n)$ modulo p^e occurs by a factor of 2 earlier than proved in Theorem 9.

Conjecture 43. (1) *If $p\equiv 3 \pmod 4$ and $e\ge 1$, we have $u(n)\equiv 0 \pmod{p^{2e-1}}$ for $n\ge\left\lceil\frac{ep^2-1}{2}\right\rceil$.*

(2) *If $p\equiv 3 \pmod 4$ and $e\ge 2$, we have $u(n)\equiv 0 \pmod{p^{2e}}$ for $n\ge\frac{ep^2+(e-2)p}{2}$.*

(2a) *If $p\equiv 3 \pmod 4$, we have $u(n)\equiv 0 \pmod{p^2}$ for $n\ge\frac{p^2-1}{2}$.*

Remark. Computer experiments indicate that the above lower bounds can be improved in two sporadic cases:

(1) If $p\equiv 3 \pmod 4$, we have $u(n)\equiv 0 \pmod p$ for $n\ge\frac{p^2-p}{2}$.

(2) If $p\equiv 3 \pmod 4$, we have $u(n)\equiv 0 \pmod{p^6}$ for $n\ge\frac{3p^2-1}{2}$.

The next conjecture predicts an analogous strengthening of Theorem 17, again for primes $p\equiv 3 \pmod 4$.

Conjecture 44. (1) *If $p\equiv 3 \pmod 4$ and e is odd, we have $v(n)\equiv 0 \pmod{p^e}$ for $n\ge\frac{(ep+2)(p+1)}{4}$.*

(2) *If $p\equiv 3 \pmod 4$ and e is even, we have $v(n)\equiv 0 \pmod{p^e}$ for $n\ge\left\lceil\frac{ep^2}{4}\right\rceil$, "with very few exceptions." Based on data for $v(n)$ with $n\le 1500$, the only exceptions that we found were*

- *$p=7$ and $e=8$, where the correct lower bound is 102 instead of $\left\lceil\frac{8\cdot 7^2}{4}\right\rceil=98$;*

- $p = 7$ *and* $e = 24$, *where the correct lower bound is* 298 *instead of* $\left\lceil \frac{24\cdot 7^2}{4} \right\rceil = 294$*;*
- $p = 7$ *and* $e = 40$, *where the correct lower bound is* 494 *instead of* $\left\lceil \frac{40\cdot 7^2}{4} \right\rceil = 490$*;*
- $p = 11$ *and* $e = 36$, *where the correct lower bound is* 1095 *instead of* $\left\lceil \frac{36\cdot 11^2}{4} \right\rceil = 1089$*.*

For the sequence $\big(d(n)\big)_{n\ge0}$ and primes $p \equiv 3 \pmod 4$, it seems that Theorem 23 can be improved analogously.

Conjecture 45. *If* $p \equiv 3 \pmod 4$, *we have* $d(n) \equiv 0 \pmod {p^e}$ *for* $n \ge \left\lceil \frac{ep^2}{4} \right\rceil$.

For primes $p \equiv 1 \pmod 4$, it appears that the periodicity of $d(n)$ modulo p-powers can be refined in the following way, which would improve Theorem 42.

Conjecture 46. (1) *If* $p \equiv 1 \pmod 4$, *the sequence* $\big(d(n)\big)_{n\ge1}$, *taken modulo* p^e, *is (eventually) periodic with* (*not necessarily minimal*) *period length* $\frac{1}{8}p^{e-1}(p-1)^2$.

(2) *If* $p \equiv 1 \pmod 4$, *there exists a constant* $C_{p,e}$ *such that:*

(i) $d\big(n + \frac{p^{e-1}(p-1)}{4}\big) \equiv C_{p,e}d(n) \pmod {p^e}$ *for all* $n \ge 1$*;*

(ii) $C_{p,e}^{(p-1)/2} \equiv 1 \pmod {p^e}$.

Remark. (1) From computer data, it seems that $\big(d(n)\big)_{n\ge1}$ is actually *purely* periodic modulo p^e for a prime p with $p \equiv 1 \pmod 4$. However, that may be deceiving and just mean that one sees counter-examples only if one goes to very high prime powers p^e (which however is difficult since the computation of $d(n)$ for large n quickly exceeds the capacity of computers). In any case, with an arbitrary sequence $\big(y(n)\big)_{n\ge0}$ satisfying the conditions of Theorem 41, the congruence (11.21) is not true in general. Furthermore, recall that we proved pure periodicity of $d(n)$ modulo p^e only starting from $n = e + 1$. Phrased differently, if pure periodicity for $\big(d(n)\big)_{n\ge1}$ is true, then this would come from very special properties of the sequences $\big(u(n)\big)_{n\ge0}$ and $\big(v(n)\big)_{n\ge0}$.

(2) Item (2) above is a strengthening and generalisation of [13, Conj. 18(2)].

Concerning the matrix $\big(R(n,k)\big)_{n,k\ge0}$, we record the following — conjectural — congruence properties. Item (3) is a strengthening of Theorem 33 specialised to $y(k) = u(k)$ for all k.

Conjecture 47. (1) *For fixed* k *and any given prime power* p^e *with* $p \equiv 1 \pmod 4$, *the sequence* $(\mathbf{R}(2n+k,k))_{n\ge0}$, *when considered modulo* p^e, *is (purely) periodic.*

(2) *For fixed* k *and any given prime power* p^e *with* $p \equiv 3 \pmod 4$, *the sequence* $(\mathbf{R}(2n+k,k))_{n\ge0}$, *when considered modulo* p^e, *is eventually* 0.

(3) *For fixed* a *and any* 2*-power* 2^e, *the sequence* $\big(R^{-1}(2n+k,k)\big)_{k\ge0}$ *is periodic modulo* 2^e *with period length* 2^{e-3}.

An attentive reader may have observed earlier that we did not say anything about the behaviour of $u(n)$ modulo powers of 2. The reason is that we simply did not need to know more than $u(0) = 1$, and that $u(1)$ and $u(2)$ are odd, in order to prove periodicity of $\big(d(n)\big)_{n\ge0}$ modulo powers of 2. However, data suggest a high divisibility of $u(n)$ by powers of 2. Even much more seems to be true, namely a "hypergeometric" generalisation; see the conjecture below. This high divisibility might be necessary for a proof of Conjecture 47(3).

Conjecture 48. *Let $(u(n))_{n\ge 0}$ be defined by the recurrence (2.4). Then $\frac{u(n)}{(2n+1)!} \in \mathbb{Z}_2$. In other words, the rational number $\frac{u(n)}{(2n+1)!}$ can be written with an odd denominator. In particular, we have $v_2\big(u(n)\big) \ge 2n - \lceil \log_2(n) \rceil$. More generally, it seems that any quotient*

$$\frac{{}_2F_1\left[\begin{matrix}\frac{3}{4}+a, \frac{3}{4}+b\\ \frac{3}{2}+c\end{matrix}; 4t\right]}{{}_2F_1\left[\begin{matrix}\frac{1}{4}+d, \frac{1}{4}+e\\ \frac{1}{2}+f\end{matrix}; 4t\right]}$$

with a, b, c, d, e, f non-negative integers has coefficients in $\mathbb{Z}_2$.

Acknowledgement

We thank Tanay Wakhare for helpful correspondence. The authors also thank the Mathematische Forschungsinstitut Oberwolfach for the opportunity of an Oberwolfach Research Fellowship in August/September 2024, during which they succeeded to improve the divisibility results for primes $p \equiv 3 \pmod 4$ significantly.

References

[1] G. E. Andrews, *The Theory of Partitions*, Encyclopedia of Math. and its Applications, vol. 2, Addison–Wesley, Reading, 1976.
[2] G. E. Andrews, R. A. Askey, and R. Roy, *Special Functions*, The Encyclopedia of Mathematics and its Applications, vol. 71, Cambridge University Press, Cambridge, 1999.
[3] B. C. Berndt, *Ramanujan's Notebooks. Part V*, Springer–Verlag, New York, 1998.
[4] P. Guerzhoy, M. H. Mertens and L. Rolen, Periodicities for Taylor coefficients of half-integral weight modular forms, *Pacific J. Math.* **307** (2020), 137–157.
[5] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, *J. reine angew. Math.* **44** (1852), 93–146. Reprinted in: Collected Papers (edited by A. Weil), Vol. I, 485–538, Springer, New York, 1975.
[6] H. Larson and G. Smith, Congruence properties of Taylor coefficients of modular forms *Int. J. Number Theory* **10** (2014), 1501–1518.
[7] A. M. Legendre, *Essai sur la théorie des nombres*, 2nd ed., Courcier, Paris, 1808.
[8] C. O'Sullivan and M. S. Risager, Non-vanishing of Taylor coefficients and Poincaré series, *Ramanujan J.* **30** (2013), 67–100.
[9] F. Rodríguez Villegas and D. Zagier, Square roots of central values of Hecke L-series, in: *Advances in Number Theory*, Fernando Q. Gouvêa and Noriko Yui (eds.), Oxford Sci. Publ., The Clarendon Press, Oxford University Press, New York, 1993, pp. 81–99.
[10] D. Romik, The Taylor coefficients of the Jacobi theta constant θ_3, *Ramanujan J.* **52** (2020), 275–290.
[11] R. Scherer, Congruences modulo primes of the Romik sequence related to the Taylor expansion of the Jacobi theta constant θ_3, *Ramanujan J.* **54** (2021), 427–448.
[12] R. P. Stanley, *Enumerative Combinatorics*, vol. 2, Cambridge University Press, Cambridge, 1999.
[13] T. Wakhare, Romik's conjecture for the Jacobi theta function, *J. Number Theory* **215** (2020), 275–296.
[14] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, reprint of the 4th ed. (1927), Cambridge University Press, Cambridge, 1996.

Fakultät für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, A-1090 Vienna, Austria. WWW: http://www.mat.univie.ac.at/~kratt.

Fakultät für Mathematik, Universität Wien, Oskar-Morgenstern-Platz 1, A-1090 Vienna, Austria.