SOME 2-ADIC INTEGERS RELATED TO THE ODD PART OF $2^e!$

DONALD M. DAVIS

ABSTRACT. The odd part of $2^e!$ as $e \to \infty$ leads to a 2-adic integer z. The bits of z were publicized in OEIS-A359349, where two conjectures were made, relevant to computing z. We prove both of those conjectures. A second 2-adic integer, the limit of $((2^e-1)!!-1)/2^e$, plays a key role in one proof.

1. INTRODUCTION

In [1], the author noted that the odd part of $2^e!$ and of $2^{e-1}!$ agree mod 2^e, and so the 2-adic limit as e approaches ∞ is a 2-adic integer, which we will call z. In OEIS-A359349([2]), the author and Jon E. Schoenfield publicized the sequence of bits of z and made two conjectures. One involved a relationship between the bits of z and some of the unstable bits in the odd part of $2^e!$, while the other leads to a more efficient way of computing z. In this paper we prove both conjectures and some generalizations.

In this introductory section, we review the two conjectures, stating them as theorems. In Sections 2 and 3, we prove generalizations of both.

Let $\nu(n)$ denote the exponent of 2 in the prime factorization of n, and $\text{od}(n) = 2/2^{\nu(n)}$ the odd part of n. Then $\text{od}(2^e!) = 2^e!/2^{2^e-1}$. In Figure 1 we tabulate the first 40 bits in the backward binary expansion (BBE) of $\text{od}(2^e!)$ for $2 \le e \le 30$. In [2], a larger table (64 bits for $e \le 40$) was presented.

Bits 0 through e of $\text{od}(2^e!)$ are *stable*; they agree with those of z. The *unstable* bits of $\text{od}(2^e!)$ are those in position $\ge e+1$; they appear to the right of the space in Figure 1. Note that, for $e > d$, the first d unstable bits of $\text{od}(2^e!)$ occur in the same positions as the last d stable bits of $\text{od}(2^{e+d}!)$. The latter are the stable bits of z in position

Date: October 24, 2025.
Key words and phrases. 2-adic integers, 2-powers, factorials.
2000 *Mathematics Subject Classification*: 11A15, 11E95, 11B50.

2	110 00000000000000000000000000000000000000
3	1101 11001000000000000000000000000000000000
4	11010 11101110111011100000110010000000000
5	110100 10110011101000110000011010100010001
6	1101000 00000000110100011010001011001111 0
7	11010001 10010101001010001010001101011100
8	110100010 01111001110010001100000100111101
9	1101000101 00011010111011000000101100001 1
10	11010001011 10101101100010111001010101001
11	110100010110 00100111111101011110101101 11
12	1101000101101 11011111000000110011101101 1
13	11010001011010 11100001101100011101011000
14	110100010110100 10110011110111101101000 01
15	1101000101101000 00001111010000010011000 0
16	11010001011010001 10000001011001001111011
17	110100010110100010 01010010000111010010 01
18	1101000101101000101 01110100100000000001 0
19	11010001011010001011 00000101101001010101
20	110100010110100010111 10011011111011111101
21	1101000101101000101110 011011110000010111
22	11010001011010001011101 00100001101011100
23	1101000101101000101110 11 1101001111111011
24	11010001011010001011101 10 111101110010100
25	1101000101101000101110 1100 10000001111101
26	1101000101101000101110 11000 0101001100111
27	1101000101101000101110 110001 011101101100
28	1101000101101000101110 110011 00000011011
29	1101000101101000101110 1100111 1001011000
30	1101000101101000101110 1100011 10 011111001

Table 1: first 32 bits in BBE of od($2^e!$)

$e+1$ through $e+d$. Let uns(e,d) and stab$(e+1,d)$ denote the numbers whose BBE's are these sequences of d bits. The following theorem was the first conjecture of [2].

Theorem 1.1. *There is a 2-adic integer K such that, for all d and $e > d$*

$$\text{uns}(e,d) + K \equiv \text{stab}(e+1,d).$$

Example 1.2. *The BBE of K begins* 1011011*. The BBE's of* $\mathrm{uns}(17,7)$ *and* $\mathrm{stab}(18,7)$ *are* 0101001 *and* 1110110*, respectively. After reversing the order of the bits, the theorem is easily verified in this case.*

This relationship between the stable and unstable parts is, at least, a curiosity. It could be useful in calculations. We will see in Section 2 that the first d bits of K can be determined from d bits of z and d bits of another 2-adic integer w. So, for example, bits 18 through 24 of z can be determined from $\mathrm{od}(2^{17}!)$ and $K \bmod 2^7$, which is an easier calculation than $\mathrm{od}(24!)$.

Let $\mathrm{odpr}(\ell, m)$ denote the product of all odd integers j satisfying $\ell \le j \le m$, and let

$$h(m) = \mathrm{odpr}(2^{m-1}+1, 2^m-1).$$

We begin with the following elementary proposition.

Proposition 1.3. *For any $e \ge 1$,*

$$\mathrm{od}(2^e!) = \prod_{m=2}^{e} h(m)^{e+1-m}.$$

Proof. Each factor j of $h(m)$ occurs with coefficient 2^i for $0 \le i \le e-m$ in $2^e!$. ■

This yields a method of computing $\mathrm{od}(2^e!) \bmod 2^B$, reducing mod 2^B at each step. The following theorem, which was the second conjecture of [2], makes it more efficient.

Theorem 1.4. *If $2 \le m-1 \le B \le 3m-7$, and $d = 2 + \lfloor \frac{B-m}{2} \rfloor$, then*

$$h(m) \equiv \mathrm{odpr}(2^{m-1}+1, 2^{m-1}+2^d-1)^{2^{m-1-d}} \pmod{2^B}.$$

The advantage is that now $h(m)$ requires $2^{d-1}+m-2-d$ multiplications (always reducing mod 2^B) compared with $2^{m-2}-1$ multiplications.

2. A formula for the 2-adic integer K of Theorem 1.1

In this section, we prove Theorem 1.1 and give a formula for the 2-adic integer K that occurs in it. We begin by reviewing the proof in [1] of existence of the 2-adic integer z, as some of the ingredients will be useful later.

Lemma 2.1. *Let* $I_e = \{i : 2^{e-1} < i \leq 2^e\}$ *and* $S_e = \{j : j \text{ odd and } 1 \leq j < 2^e\}$. *Then* $\mathrm{od} : I_e \to S_e$ *is bijective.*

Proof. The inverse function ϕ is defined by $\phi(u) = 2^t u$ where $t = \max\{k : 2^k u \leq 2^e\}$. ■

Lemma 2.2. *If* $e \geq 3$, *the product of all odd positive integers less than* 2^e *is* $\equiv 2^e + 1 \pmod{2^{e+1}}$.

Proof. We begin with the proof from [3, Lemma 1] that the product is 1 mod 2^e. Pair each element with its inverse in $\mathbb{Z}/2^e$. Only ± 1 and $2^{e-1} \pm 1$ equal their own inverse, and their product is 1.

Let P be the set of pairs (a, b) with $a < b < 2^e$ odd and $ab \equiv 2^e + 1 \bmod 2^{e+1}$. If $(a, b) \in P$, so is $(2^e - b, 2^e - a)$ since $a + b$ is even. Moreover, $(a, b) \neq (2^e - b, 2^e - a)$ since, if so, then $a(2^e - a) \equiv 2^e + 1 \bmod 2^{e+1}$, which cannot occur since $a^2 \equiv 1 \bmod 8$. Thus the cardinality of P is even, and the product of all ab with $(a, b) \in P$ is 1 mod 2^{e+1}. Other pairs (c, d) with $cd \equiv 1 \bmod 2^e$ have $cd \equiv 1 \bmod 2^{e+1}$. Finally we have 1, $2^e - 1$, and $2^{e-1} \pm 1$, whose product is $\equiv 2^e + 1 \bmod 2^{e+1}$. ■

Corollary 2.3. *For* $e \geq 3$, $\mathrm{od}(2^{e-1}!) \equiv \mathrm{od}(2^e!) \pmod{2^e}$.

Proof. By Lemmas 2.1 and 2.2,

$$\frac{\mathrm{od}(2^e!)}{\mathrm{od}(2^{e-1}!)} = \prod_{i \in I_e} \mathrm{od}(i) = \prod_{j \in S_e} j \equiv 1 \pmod{2^e}.$$

■

Corollary 2.4. *There is a 2-adic integer* z *which equals* $\mathrm{od}(2^{e-1}!)$ *mod* 2^e.

Remark 2.5. The stronger (mod 2^{e+1}) part of Lemma 2.2 was not needed here, but will be used shortly.

A stronger version of the next result will be proved in Theorem 3.1.

Proposition 2.6. *With* S_e *as above,*

$$\prod_{i \in S_e} i \equiv \prod_{i \in S_e} (2^e + i) \pmod{2^{2e}}.$$

Proof. If S is a set of cardinality n, let $\widehat{\sigma}_i(S) = \sigma_{n-i}(S)$, where σ is the usual elementary symmetric polynomial. Then $\widehat{\sigma}_1(S_e)$ is divisible by 2^e since, for odd $j \leq 2^{e-1}-1$,

$$\prod_{\substack{i\in S_e\\ i\neq j}} i + \prod_{\substack{i\in S_e\\ i\neq 2^e-j}} i \text{ is divisible by } 2^e.$$

We have

$$\prod_{i\in S_e}(2^e+i) - \prod_{i\in S_e} i = \sum_{j>0} 2^{je}\widehat{\sigma}_j(S_e) \equiv 2^e\widehat{\sigma}_1(S_e) \equiv 0 \pmod{2^{2e}}.$$

■

Let $(2^e-1)!! = \mathrm{odpr}(1, 2^e-1)$.

Corollary 2.7. *For $e \geq 2$,* $\dfrac{(2^e-1)!!-1}{2^e} \equiv \dfrac{(2^{e+1}-1)!!-1}{2^{e+1}} \pmod{2^{e-1}}$.

Proof. By Lemma 2.2, the two expressions are odd integers. We will show that their ratio is $\equiv 1 \bmod 2^{e-1}$. Let $A = (2^e-1)!!-1$. By Lemma 2.2, $A = 2^e u$ with u odd. By Proposition 2.6, $\mathrm{odpr}(2^e+1, 2^{e+1}-1) = A+1+k2^{2e}$ for some integer k. The desired ratio is

$$\begin{aligned}&\frac{(A+1)(A+1+k2^{2e})-1}{2A}\\ &= \frac{A^2+2A+(A+1)k2^{2e}}{2A} = 2^{e-1}u + 1 + \frac{(A+1)k2^{2e}}{2^{e+1}u} \equiv 1 \pmod{2^{e-1}}.\end{aligned}$$

■

Definition 2.8. *We define w to be the 2-adic integer which equals* $\dfrac{(2^e-1)!!-1}{2^e}$ *mod* 2^{e-1}.

The binary expansion of w ends $\cdots 1001110011001$.

We have introduced two 2-adic integers, z and w. The next result shows that their product equals the difference of the unstable parts of consecutive rows of Figure 1 in a metastable range.

Theorem 2.9. *The difference of the unstable parts of* $\mathrm{od}(2^e!)$ *and* $\mathrm{od}(2^{e-1}!)$*, i.e.,* $\dfrac{\mathrm{od}(2^e!)-\mathrm{od}(2^{e-1}!)}{2^e}$*, is congruent mod* 2^{e-1} *to* $w\cdot z$.

Proof. By Lemma 2.1, we have $(2^e-1)!! = \dfrac{\mathrm{od}(2^e!)}{\mathrm{od}(2^{e-1}!)}$. Thus

$$\frac{(2^e-1)!!-1}{2^e} = \frac{\mathrm{od}(2^e!)-\mathrm{od}(2^{e-1}!)}{2^e\,\mathrm{od}(2^{e-1}!)},$$

so

$$\frac{(2^e-1)!!-1}{2^e}\cdot \mathrm{od}(2^{e-1}!) = \frac{\mathrm{od}(2^e!)-\mathrm{od}(2^{e-1}!)}{2^e}.$$

The result follows now from Corollary 2.4 and Definition 2.8. ■

Example 2.10. *The binary expansion of zw ends $\cdots 011000010011$. The numbers $\mathrm{od}(2^7!)$ and $\mathrm{od}(2^6!)$ agree mod 2^7. Beginning in the 2^7 position, the binary expansion of $\mathrm{od}(2^7!)$ ends $\cdots 1010011$, while that of $\mathrm{od}(2^6!)$ ends with eight 0's. The difference agrees with zw mod 2^6.*

We now state the main theorem of this section.

Theorem 2.11. *The 2-adic integer K of Theorem 1.1 equals $-zw$.*

Proof of Theorems 1.1 and 2.11. The difference $\mathrm{stab}(e+1,d)-\mathrm{uns}(e,d)$, as described in the paragraph preceding Theorem 1.1, equals $\dfrac{\mathrm{od}(2^{e+d}!)-\mathrm{od}(2^e!)}{2^{e+1}} \bmod 2^d$. We have

$$\begin{aligned}
&\frac{\mathrm{od}(2^{e+d}!)-\mathrm{od}(2^e!)}{2^{e+1}}\\
&= \sum_{i=1}^{d} \frac{\mathrm{od}(2^{e+i}!)-\mathrm{od}(2^{e+i-1}!)}{2^{e+1}}\\
&= \sum_{i=1}^{d} 2^{i-1}\frac{\mathrm{od}(2^{e+i}!)-\mathrm{od}(2^{e+i-1}!)}{2^{e+i}}\\
&\equiv \sum_{i=1}^{d} 2^{i-1} zw \pmod{2^e}\\
&\equiv \sum_{i=1}^{\infty} 2^{i-1} zw \pmod{2^d}\\
&= -zw.
\end{aligned}$$

■

Example 2.12. *The binary expansion of $-zw$ ends $\cdots 010111101101$. Add that to the binary number obtained by reversing the order of the first 12 bits after the space on line 14 of Figure 1, and you obtain the binary number obtained by reversing the order of the last 12 bits before the space on line 26.*

3. Proof of Theorem 1.4

In this section, we prove Theorem 1.4 and some mild generalizations. The bulk of our work is the following strengthening of Proposition 2.6, the proof of which appears later.

Theorem 3.1. *With S_e as defined in Lemma 2.1, and A any integer,*

$$\prod_{i\in S_e}(A2^e+i)\equiv\prod_{i\in S_e} i \pmod{2^{3e-1}}.$$

Corollary 3.2. *For any integers A, B, and j,*

$$\prod_{i\in S_e}(A2^e+i)^{2^j}\equiv\prod_{i\in S_e}(B2^e+i)^{2^j} \pmod{2^{3e-1+j}}.$$

Proof. It is elementary that if $\alpha\equiv\beta \bmod 2t$, then $\alpha^2\equiv\beta^2 \bmod 4t$. We apply this iteratively to Theorem 3.1, and then both expressions in the corollary are congruent to $\prod i^{2^j}$. ■

Proof of Theorem 1.4. We write the conjectured congruences in succession, beginning

$$\operatorname{odpr}(2^{m-1}+1,2^m-1)\equiv\operatorname{odpr}(2^{m-1}+1,2^{m-1}+2^{m-2}-1)^2 \quad (2^{3m-7})$$
$$\operatorname{odpr}(2^{m-1}+1,2^{m-1}+2^{m-2}-1)^2\equiv\operatorname{odpr}(2^{m-1}+1,2^{m-1}+2^{m-3}-1)^{2^2} \quad (2^{3m-9})$$

with arbitrary entry

$$\operatorname{odpr}(2^{m-1}+1,2^{m-1}+2^{d+1}-1)^{2^{m-2-d}}\equiv\operatorname{odpr}(2^{m-1}+1,2^{m-1}+2^d-1)^{2^{m-1-d}} \quad (2^{2d+m-3}).$$

After canceling, this becomes

$$\operatorname{odpr}(2^{m-1}+2^d+1,2^{m-1}+2^{d+1}-1)^{2^{m-2-d}}\equiv\operatorname{odpr}(2^{m-1}+1,2^{m-1}+2^d-1)^{2^{m-2-d}} \quad (2^{2d+m-3}).$$

We can restate this as

$$\prod_{i\in S_d}(2^{m-1}+2^d+i)^{2^{m-2-d}}\equiv\prod_{i\in S_d}(2^{m-1}+i)^{2^{m-2-d}} \pmod{2^{2d+m-3}},$$

and this is a consequence of Corollary 3.2. ■

We will prove the following two lemmas, from which Theorem 3.1 follows easily.

Lemma 3.3. $\widehat{\sigma}_1(S_e) \equiv 2^{2e-2} \pmod{2^{2e-1}}$.

Lemma 3.4. $\widehat{\sigma}_2(S_e) \equiv 2^{e-2} \pmod{2^{e-1}}$.

Proof of Theorem 3.1.

$$\prod_{i\in S_e}(A2^e+i) - \prod_{i\in S_e} i = \sum_{j>0}(A2^e)^j \widehat{\sigma}_j(S_e) \equiv 0 \pmod{2^{3e-1}}$$

by Lemmas 3.3 and 3.4, with the argument slightly different for the two parities of A. ■

Proof of Lemma 3.3.

$$\widehat{\sigma}_1(S_e) = \sum_{i=1}^{2^{e-2}-1}\left(\frac{(2^e-1)!!}{2i+1} + \frac{(2^e-1)!!}{2^e-1-2i}\right) = 2^e \sum_{i=1}^{2^{e-2}-1} \frac{(2^e-1)!!}{(2i+1)(2^e-1-2i)}.$$

Let $H_e = \displaystyle\sum_{i=1}^{2^{e-2}-1} \frac{(2^e-1)!!}{(2i+1)(2^e-1-2i)}$. We will prove by induction that $H_e \equiv 2^{e-2} \mod 2^{e-1}$, which implies the lemma.

The claim is true for $e = 2$. Assume it true for $e-1$. Mod 2^{e-1},

$$H_e \equiv \sum_{i=0}^{2^{e-2}-1} \frac{((2^{e-1}-1)!!)^2}{(2i+1)(2^{e-1}-2i-1)}.$$

The summands for i and $2^{e-2}-1-i$ are equal. Thus $H_e \equiv 2(2^{e-1}-1)!!H_{e-1} \mod 2^{e-1}$. By the induction hypothesis, we obtain $H_e \equiv 2^{e-2} \mod 2^{e-1}$, as desired. ■

We thank Andrew Granville for providing an alternate proof of Lemma 3.3.

The following results will be used in the proof of Lemma 3.4.

Lemma 3.5. *Of the 2^{e-1} numbers i^2 mod 2^e, $i \in S_e$, there are exactly four having each of the 2^{e-3} values less than 2^e and $\equiv 1$ mod 8.*

Proof. Each of the 2^{e-3} numbers is a quadratic residue, and so must occur as i^2 for some $i \in S_e$. It will occur in four ways since for odd $i < 2^{e-1}$, i, $2^{e-1}-i$, $i+2^{e-1}$, and $2^e - i$ are distinct numbers with the same square mod 2^e. Thus the claimed partitioning must hold. ■

Lemma 3.6. *For $e \geq 3$,*

$$\widehat{\sigma}_1(1, 9, \ldots, 2^e - 7, 1, 9, \ldots, 2^e - 7, 1, 9, \ldots, 2^e - 7, 1, 9, \ldots, 2^e - 7) \equiv 2^{e-1} \quad (2^e).$$

Proof. The proof is by induction. The claim is true for $e = 3$ and 4. $[\![\widehat{\sigma}_1(1, 1, 1, 1) = 4$ and $\widehat{\sigma}_1(1, 9, 1, 9, 1, 9, 1, 9) = 4 \cdot 9^4 + 4 \cdot 9^3 = 4 \cdot 9^3 \cdot 10.]\!]$ For arbitrary e, our expression equals $4 \cdot 9^3 \cdots (2^e - 7)^3 \cdot \widehat{\sigma}_1(1, 9, \ldots 2^e - 7)$. Because of the 4, we can consider $\widehat{\sigma}_1(1, 9, \ldots, 2^e - 7) \bmod 2^{e-2}$, so we obtain an odd multiple of $4 \cdot \Sigma$ with

$$\Sigma = \widehat{\sigma}_1(1, 9, \ldots, 2^{e-2} - 7, 1, 9, \ldots, 2^{e-2} - 7, 1, 9, \ldots, 2^{e-2} - 7, 1, 9, \ldots, 2^{e-2} - 7).$$

By the induction hypothesis, $\Sigma \equiv 2^{e-3} \bmod 2^{e-2}$, and so our desired expression is $\equiv 2^{e-1} \bmod 2^e$.

■

Proposition 3.7. $\displaystyle\sum_{i \in S_e} \frac{((2^e - 1)!!)^2}{i^2} \equiv 2^{e-1} \pmod{2^e}$.

Proof. By Lemma 3.5, it equals the expression in Lemma 3.6. ■

Proof of Lemma 3.4. Let $D_e = \{(a, b) \in S_e \times S_e : \ a < b\}$. Note that $\widehat{\sigma}_2(S_e) = \displaystyle\sum_{(a,b) \in D_e} \frac{(2^e - 1)!!}{a \cdot b}$, denoted by T_e. Write $T_e = T_{1,e} + T_{2,e}$, where

$$T_{1,e} = \sum_{\substack{(a,b) \in D_e \\ a \not\equiv b \ (2^{e-1})}} \frac{(2^e - 1)!!}{a \cdot b} \quad \text{and} \quad T_{2,e} = \sum_{\substack{(a,b) \in D_e \\ a \equiv b \ (2^{e-1})}} \frac{(2^e - 1)!!}{a \cdot b}.$$

Each summand of $T_{2,e}$ corresponds to a unique element of S_{e-1}, and so, mod 2^{e-1},

$$T_{2,e} \equiv \sum_{a \in S_{e-1}} \frac{((2^{e-1} - 1)!!)^2}{a^2} \equiv 2^{e-2} \pmod{2^{e-1}}$$

by Proposition 3.7.

We will prove $T_{1,e} \equiv 0 \bmod 2^{e-1}$ by induction. It is true when $e = 3$ as we obtain four summands, each with denominator 3. Assume validity for $e - 1$. Every element of D_{e-1} corresponds to four summands of $T_{1,e}$ which are equal mod 2^{e-1}. We obtain, mod 2^{e-1},

$$T_{1,e} \equiv 4 \sum_{(a,b) \in D_{e-1}} \frac{((2^{e-1} - 1)!!)^2}{a \cdot b} = 4(2^{e-1} - 1)!!(T_{1,e-1} + T_{2,e-1}) \equiv 0 \quad (2^{e-1}),$$

using the induction hypothesis for $4T_{1,e-1}$ and the already-proved result for $4T_{2,e-1}$.

■

References

[1] D.M.Davis, Binomial coefficients involving infinite powers of primes, Amer Math Monthly, **121** (2014) 734–737.
[2] D.M.Davis and J.E.Schoenfield, A359349-OEIS, May 2023.
[3] A.Granville, *Binomial coefficients modulo prime powers*, Can Math Soc Conf Proc **20** (1997) 253–275.

Department of Mathematics, Lehigh University, Bethlehem, PA 18015, USA
Email address: dmd1@lehigh.edu