DIOPHANTINE APPROXIMATION OF THE EXPONENTIAL FUNCTION AND SONDOW'S CONJECTURE

BRUCE C. BERNDT, SUN KIM, AND ALEXANDRU ZAHARESCU

ABSTRACT. We begin by examining a hitherto unexamined partial manuscript by Ramanujan on the diophantine approximation of $e^{2/a}$ published with his lost notebook. This diophantine approximation is then used to study the problem of how often the partial Taylor series sums of e coincide with the convergents of the (simple) continued fraction of e. We then develop a p-adic analysis of the denominators of the convergents of e and prove a conjecture of J. Sondow that there are only two instances when the convergents of the continued fraction of e coalesce with partial sums of e. We conclude with open questions about the zeros of certain p-adic functions naturally occurring in our proofs.

MSC: primary: 11J70; secondary: 11J17, 11J68

Keywords: diophantine approximation, approximation by partial sums of power series, exponential function, Sondow's Conjecture, continued fractions, supercongruences, p-adic analysis

1. INTRODUCTION

In his lost notebook [12], Ramanujan recorded three rough partial manuscripts on diophantine approximation. In this paper, our first goal is to discuss the partial manuscript on pages 266–267 of [12], in which Ramanujan examines the diophantine approximation of $e^{2/a}$, when a is a nonzero integer. At the top of page 266 is a note, "See Q. 784(ii) in volume. This goes further," which is in G. H. Hardy's handwriting. Question 784 is a problem on diophantine approximation submitted by Ramanujan to the *Journal of the Indian Mathematical Society* [9] [10, p. 334], in which Ramanujan offers diophantine approximations to $e^{2/a}$ and certain quadratic irrationalities. (Hardy's reference to "volume" evidently is to Ramanujan's *Collected Papers* [10].) It took more than a decade before A. A. Krishnaswami Aiyangar [1] published a partial solution, and T. Vijayaraghavan and G. N. Watson [16] published a complete solution to Question 784. In the partial manuscript at hand, not only did Ramanujan exceed the classical diophantine approximation and the further improvement in Question 784, but he also derived the best possible diophantine approximation for $e^{2/a}$. Such a theorem was first proved in print by C. S. Davis [5] in 1978, approximately 60 years after Ramanujan discovered it. Of course, Davis was unaware that his theorem was ensconced in Ramanujan's lost notebook. As we indicate in the sequel, Ramanujan's proof is different, and considerably more elementary, than Davis's proof.

The first author's research was partially supported by NSA grant H98230-11-1-0200.
The third author's research was partially supported by NSF grant DMS-0901621.

We next discuss our second primary aim, which is directly related to our first goal. In Section 4 we study instances when a convergent to the (simple) continued fraction of $e^{2/a}$, where a is a nonzero integer, is also a partial sum of the Taylor series for $e^{2/a}$, i.e.,

$$e^{2/a} = \sum_{k=0}^{\infty} \frac{2^k}{a^k k!}.$$

J. Sondow [14] conjectured that only two partial sums

$$\frac{A_n}{n!} := \sum_{k=0}^{n} \frac{1}{k!}$$

are convergents to the continued fraction of e. In the sequel, we refer to this statement as *Sondow's Conjecture*. Sondow and K. Schalm [15] proved, among other things, that almost all partial sums $A_n/n!$ of the Taylor series for e are not convergents to the (simple) continued fraction of e.

Using the Ramanujan–Davis theorems on the diophantine approximation to $e^{2/a}$ and a sharper form of Sondow and Schalm's ideas, we next show that in the first n convergents to the continued fraction of $e^{2/a}$ at most $O_a(\log n)$ of them are also partial sums of the Taylor series of $e^{2/a}$, which significantly improves the theorem of Sondow and Schalm in the special case $a = 2$. Some of the ideas in this section are also employed by the present authors in their examination of the diophantine approximation of a variety of exponential generating functions at rational arguments by their partial sums [3].

We then embark on a careful study of the denominators q_m of the convergents of the continued fraction of e. In Sections 5–7, we establish several important congruences for the denominators q_m, and define and accentuate a special class of primes $\mathcal{B}$ for which the congruences in Proposition 7.2 below are valid. In a deeper analysis in Section 8, we demonstrate that the numbers q_m satisfy certain supercongruences, by which we mean congruences modulo higher than normal powers of p, for primes p in $\mathcal{B}$. For three classes of primes in $\mathcal{B}$, Lemma 9.1 provides an upper bound on the index m in order for a counterexample to Sondow's Conjecture to exist. Upon the examination of tables that we calculate, we finally confirm the truth of Sondow's Conjecture.

In Section 10, we show that certain p-adic functions, which naturally arise from the sequence of convergents to the continued fraction of e, satisfy some intriguing functional equations. In particular, we define p-adic functions that encode the divisibility and congruences satisfied by the denominators q_m and that satisfy functional equations. By a nice conjecture of Sondow and Schalm, for any odd prime p, there should be six such functions f_r, $1 \le r \le 6$. We extend the definitions of $f_r : \mathbb{Z} \to \mathbb{Z}$ to unique extensions (under a Lipschitz condition) by continuity to functions $f_r : \mathbb{Z}_p \to \mathbb{Z}_p$. We note some "trivial" zeros for the functions f_r, and close our paper with several open questions about these functions, such as the existence of "nontrivial" zeros of f_r.

2. Ramanujan's Claims

Ramanujan established three related results, which are amalgamated in Entries 2.1 and 2.2 below, and which we relate in a moderately more contemporary style. As customary, $[x]$ denotes the greatest integer in x.

Entry 2.1. *Let $\epsilon > 0$ be given. If a is any nonzero integer, then there exist infinitely many positive integers N such that*

$$Ne^{2/a} - [Ne^{2/a}] < \frac{(1+\epsilon)\log\log N}{|a|N\log N}. \tag{2.1}$$

Moreover, for all sufficiently large positive integers N,

$$Ne^{2/a} - [Ne^{2/a}] > \frac{(1-\epsilon)\log\log N}{|a|N\log N}. \tag{2.2}$$

Entry 2.1 might be compared with a theorem of P. Bundschuh established in 1971 [4]. If t is a nonzero integer, then there exists a positive constant c_1 and infinitely many rational numbers p/q such that

$$\left|e^{1/t} - \frac{p}{q}\right| < c_1\frac{\log\log q}{q^2\log q};$$

and there exists a positive constant c_2 such that for all rational numbers p/q,

$$\left|e^{1/t} - \frac{p}{q}\right| > c_2\frac{\log\log q}{q^2\log q}.$$

In his next theorem, Ramanujan considers two cases – a even and a odd. His result for a even is identical to that for Entry 2.1, except that he formulates his conclusion in terms of $1 + [Ne^{2/a}] - Ne^{2/a}$. We therefore state Ramanujan's claim only in the case that a is odd.

Entry 2.2. *If a is any odd integer and $\epsilon > 0$ is given, then there exist infinitely many positive integers N such that*

$$1 + [Ne^{2/a}] - Ne^{2/a} < \frac{(1+\epsilon)\log\log N}{4|a|N\log N}. \tag{2.3}$$

Furthermore, given $\epsilon > 0$, for all positive integers N sufficiently large,

$$1 + [Ne^{2/a}] - Ne^{2/a} > \frac{(1-\epsilon)\log\log N}{4|a|N\log N}. \tag{2.4}$$

It will be seen, from the proofs of these entries below, that the constants multiplying

$$\frac{\log\log N}{N\log N}$$

on the right-hand sides of (2.1), (2.2), (2.3), and (2.4) are optimal.

For comparison, we provide a precise statement of Davis's theorem [5, Theorem 2], which readers will immediately see is equivalent to Ramanujan's Entries 2.1 and 2.2. In his paper, Davis, in fact, only proves his theorem in the special case of e, indicating that the proof of the more general result follows along the same lines. Although both the proofs of Davis and Ramanujan employ continued fractions, they are quite different. Davis uses, for example, integrals, hypergeometric functions, and Tannery's theorem. On the other hand, Ramanujan utilizes only elementary properties of continued fractions.

Theorem 2.3. *Let $a = \pm 2/t$, where t is a positive integer, and set*

$$c = \begin{cases} 1/t, & \text{if } t \text{ is even}, \\ 1/(4t), & \text{if } t \text{ is odd}. \end{cases}$$

Then, for each $\epsilon > 0$, the inequality

$$\left|e^a - \frac{p}{q}\right| < (c+\epsilon)\frac{\log\log q}{q^2 \log q}$$

has an infinity of solutions in integers p, q. Furthermore, there exists a number q', depending only on ϵ and t, such that

$$\left|e^a - \frac{p}{q}\right| > (c-\epsilon)\frac{\log\log q}{q^2 \log q}$$

for all integers p, q, with $q \geq q'$.

3. Proofs of Ramanujan's Claims on Page 266

Proof. We begin with the continued fraction

$$\tanh x = \frac{x}{1} + \frac{x^2}{3} + \frac{x^2}{5} + \frac{x^2}{7} + \cdots, \qquad x \in \mathbb{C}, \tag{3.1}$$

first established by J. H. Lambert, and rediscovered by Ramanujan, who recorded it in his second notebook [11, Chapter 12, Section 18], [2, p. 133, Corollary 3]. Write

$$\tanh x = 1 - \frac{2}{e^{2x}+1}$$

in (3.1), solve for $2/(e^{2x}+1)$, take the reciprocal of both sides, and set $x = 1/a$, where a is any nonzero integer. Hence,

$$\frac{1}{2}\left(e^{2/a}+1\right) = \frac{1}{1} - \frac{1}{a} + \frac{1}{3a} + \frac{1}{5a} + \frac{1}{7a} + \cdots. \tag{3.2}$$

Now consider the nth approximant u_n/v_n of (3.2) [6, pp. 8–9], [2, p. 105, Entry 1], i.e., for $n \geq 3$,

$$\frac{1}{1} - \frac{1}{a} + \frac{1}{3a} + \frac{1}{5a} + \frac{1}{7a} + \cdots + \frac{1}{(2n-3)a} = \frac{u_n}{v_n}.$$

Then, provided that $|a| \geq 2$,

$$u_1 = 1, \quad v_1 = 1; \qquad u_2 = |a|, \quad v_2 = |a-1|. \tag{3.3}$$

Also, from standard recurrence relations [6, pp. 8–9],

$$u_{n+1} - u_{n-1} = (2n-1)|a|u_n; \qquad v_{n+1} - v_{n-1} = (2n-1)|a|v_n. \tag{3.4}$$

From the second equality in (3.4), we can deduce that

$$v_{n+1} \sim 2|a|nv_n \qquad \text{and} \qquad \log v_n \sim n\log n, \tag{3.5}$$

as $n \to \infty$.

Now, in general [2, p. 105, Entry 1], if we define $v_0 = 1$, then [17, p. 18]

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} + \cdots + \frac{a_n}{b_n} =: a_1\frac{u_n}{v_n} = \sum_{k=1}^{n} \frac{(-1)^{k+1}a_1a_2\cdots a_k}{v_kv_{k-1}}.$$

If we use the formula above in (3.2), we easily find that

$$\frac{1}{2}\left(e^{2/a}+1\right) = \frac{u_n}{v_n} + (-1)^n\left(\frac{1}{v_nv_{n+1}} - \frac{1}{v_{n+1}v_{n+2}} + \cdots\right). \tag{3.6}$$

It follows from (3.5) and (3.6) that, as n tends to ∞,

$$e^{2/a} + 1 - \frac{2u_n}{v_n} \sim \frac{(-1)^n}{|a|nv_n^2}. \tag{3.7}$$

We now subdivide our examination of (3.7) into two cases. First, suppose that a is even. Then, using the fact that v_1 and v_2 in (3.3) are odd, the recurrence relation for v_n in (3.4), and induction, we easily find that v_n is odd for all $n \geq 1$. Now choose $N = v_n$. By (3.5), we see that $n \sim \log N/\log\log N$, as $N \to \infty$. Hence, by (3.7), as $N \to \infty$,

$$N(e^{2/a} + 1) - 2u_n \sim \frac{(-1)^n \log\log N}{|a|N\log N}. \tag{3.8}$$

Second, suppose that a is odd. Ramanujan then claims that if n is odd, then v_n is odd, while if n is even, then v_n is even. However, these claims are incorrect. By (3.3), (3.4), and induction, we find, instead, that

$$v_{3m} \quad \text{and} \quad v_{3m+1} \quad \text{are odd ;} \qquad v_{3m+2} \quad \text{is even.}$$

Thus, choose $N = v_n$, when $n = 3m$ or $n = 3m+1$. In these cases, as in (3.8), we conclude that

$$N(e^{2/a} + 1) - 2u_n \sim \frac{(-1)^n \log\log N}{|a|N\log N}. \tag{3.9}$$

However, if $n = 3m + 2$, we can choose $N = \frac{1}{2}v_{3m+2}$. Hence, in this case,

$$N(e^{2/a} + 1) - u_n \sim \frac{(-1)^m \log\log N}{4|a|N\log N}. \tag{3.10}$$

Turning to Ramanujan's claims in Entries 2.1 and 2.2, from the asymptotic formulas (3.8) and (3.10), we see that all of Ramanujan's claims in these entries readily follow. This completes the proof. □

4. Convergents of the Continued Fraction of $e^{2/a}$ and Partial Sums of $e^{2/a}$

In this section, we use the method employed in [3], which generalizes that of Sondow and Schalm [15], in conjunction with the theorems by Ramanujan and Davis, to prove that only $O(\log M)$ of the first M convergents to the continued fraction of $e^{2/a}$ are partial sums of the corresponding Taylor series expansion. We show in [3] that only $O(\log n)$ of the first n partial sums of $e^{2/a}$ are also convergents to the continued fraction of $e^{2/a}$. We remark in this connection that, as proved in [3], there exist sequences of strictly positive integers a_k satisfying $1 \leq a_k \leq k$, for each positive integer k, such that a positive proportion of the convergents to the continued fraction of $\alpha := \sum_{k=1}^{\infty} a_k/k!$ coincide with partial sums $\sum_{k\leq n} a_k/k!$, even though only $O(\log n)$ of the first partial sums are convergents to the continued fraction of α.

Readers are warned that the notations for partial sums of power series and for convergents of continued fractions in Section 4 differ slightly from corresponding notations in Section 5 and all further sections, in which our attention is given to e, and not to $e^{2/a}$, the focus of this section.

Theorem 4.1. *Fix a nonzero integer a. In the first M convergents to the continued fraction of $e^{2/a}$, there are no more than $O(\log M)$ instances when the convergents match partial sums of $e^{2/a}$.*

Proof. Fix an integer $a \neq 0$. Let p_m/q_m denote the mth convergent to the (simple) continued fraction of $e^{2/a}$, and let $A_n/(|a|^n n!)$ denote the nth partial sum of the Taylor series

$$\frac{A_n}{|a|^n n!} = \sum_{k=0}^{n} \frac{2^k}{a^k k!}.$$

Fix a real number $\lambda > 1$. For each large positive integer M, we proceed to derive an upper bound for the number of integers m in the interval $[M, \lambda M]$ for which p_m/q_m is a partial sum of the Taylor series for $e^{2/a}$. For such an M, let

$$E = \left\{ m \in [M, \lambda M] : \frac{p_m}{q_m} = \frac{A_n}{|a|^n n!}, \quad \text{for some } n \in \mathbb{N} \right\}.$$

Let us remark that for fixed $a \neq 0$ and for M sufficiently large, for each m in the exceptional set E, there is a unique n such that

$$\frac{A_n}{|a|^n n!} = \frac{p_m}{q_m},$$

because the map $n \mapsto A_n/(|a|^n n!)$ is ultimately injective. Thus, for large M, we have a well defined map $\psi : E \mapsto \mathbb{N}$ given by

$$\frac{p_m}{q_m} = \frac{A_{\psi(m)}}{|a|^{\psi(m)} \psi(m)!} \tag{4.1}$$

for all $m \in E$. Although the map ψ is clearly injective, we do not know whether or not it is increasing. In principle, there might exist $m_1, m_2 \in E$, $m_1 < m_2$, such that

$$\frac{p_{m_1}}{q_{m_1}} = \frac{A_{n_1}}{|a|^{n_1} n_1!} \qquad \text{and} \qquad \frac{p_{m_2}}{q_{m_2}} = \frac{A_{n_2}}{|a|^{n_2} n_2!},$$

and although p_{m_1}/q_{m_1} is a rational number of smaller height than p_{m_2}/q_{m_2}, it still might be true that $n_1 > n_2$ (and consequently more cancellation in $A_{n_1}/(|a|^{n_1} n_1!)$ than in $A_{n_2}/(|a|^{n_2} n_2!)$).

We now proceed to derive a lower bound for the least common multiple of the numbers q_m, $m \in E$. Denote this least common multiple by L. For any $m_1, m_2 \in E$ with $m_1 < m_2$, we use the familiar recurrence relations giving each q_m in terms of q_{m-1} and q_{m-2}, in order to write q_{m_2} as a linear combination of q_{m_1} and q_{m_1+1}. Thus,

$$q_{m_2} = A q_{m_1+1} + B q_{m_1},$$

for some positive integers A and B. Since q_{m_1} and q_{m_1+1} are relatively prime, it follows that

$$(q_{m_1}, q_{m_2}) = (q_{m_1}, A).$$

Therefore,

$$(q_{m_1}, q_{m_2}) \leq A = \frac{q_{m_2} - B q_{m_1}}{q_{m_1+1}} < \frac{q_{m_2}}{q_{m_1}}.$$

It follows that

$$L \geq \frac{\prod\limits_{m \in E} q_m}{\prod\limits_{\substack{m_1 < m_2 \\ m_1, m_2 \in E}} (q_{m_1}, q_{m_2})} \geq \frac{\prod\limits_{m \in E} q_m}{\prod\limits_{\substack{m_1 < m_2 \\ m_1, m_2 \in E}} \frac{q_{m_2}}{q_{m_1}}}.$$

More generally, for each nonempty subset S of E, the least common multiple L_S of numbers q_m with $m \in S$ is a divisor of L, and

$$L \geq L_S \geq \frac{\prod\limits_{m\in S} q_m}{\prod\limits_{\substack{m_1<m_2\\ m_1,m_2\in S}} \frac{q_{m_2}}{q_{m_1}}}. \tag{4.2}$$

Let us fix an $m_0 \in S$ and count the number of factors of q_{m_0} on the right side of (4.2). Notice that q_{m_0} appears once in the numerator $\prod_{m\in S} q_m$, it appears

$$\#\{m_1 \in S : \, m_1 < m_0\}$$

times in the numerator of

$$\mathsf{P} := \prod_{\substack{m_1<m_2\\ m_1,m_2\in S}} \frac{q_{m_2}}{q_{m_1}},$$

and it appears

$$\#\{m_2 \in S : \, m_2 > m_0\}$$

times in the denominator of P. It follows that

$$\begin{aligned}\frac{\prod\limits_{m\in S} q_m}{\prod\limits_{\substack{m_1<m_2\\ m_1,m_2\in S}} \frac{q_{m_2}}{q_{m_1}}} &= \prod_{m\in S} q_m^{1+\#\{m_2\in S:\, m_2>m\}-\#\{m_1\in S:\, m_1<m\}}\\ &= \prod_{m\in S} q_m^{\#\{S\}-2\#\{m_1\in S:\, m_1<m\}}. \end{aligned}\tag{4.3}$$

For each q_m on the far right side of (4.3) with a positive exponent, we now use the inequality $q_m \geq q_M$, and for each q_m with a negative exponent, we use the inequality $q_m \leq q_{[\lambda M]}$.

Note that

$$\sum_{\substack{m\in S\\ \#\{S\}>2\#\{m_1\in S:\, m_1<m\}}} (\#\{S\} - 2\#\{m_1 \in S : \, m_1 < m\}) = \begin{cases} k(k+1), & \text{if } \#\{S\} = 2k,\\ (k+1)^2, & \text{if } \#\{S\} = 2k+1. \end{cases} \tag{4.4}$$

Similarly,

$$-\sum_{\substack{m\in S\\ \#\{S\}<2\#\{m_1\in S:\, m_1<m\}}} (\#\{S\} - 2\#\{m_1 \in S : \, m_1 < m\}) = \begin{cases} k(k-1), & \text{if } \#\{S\} = 2k,\\ k^2, & \text{if } \#\{S\} = 2k+1. \end{cases} \tag{4.5}$$

Combining (4.2)–(4.5), we deduce that

$$L \geq \begin{cases} \dfrac{q_M^{k(k+1)}}{q_{[\lambda M]}^{k(k-1)}}, & \text{if } \#\{S\} = 2k,\\[2ex] \dfrac{q_M^{(k+1)^2}}{q_{[\lambda M]}^{k^2}}, & \text{if } \#\{S\} = 2k+1. \end{cases} \tag{4.6}$$

Since (4.6) holds for any nonempty subset S of E, we derive that

$$L \geq \max\left(\max_{1\leq k\leq [\frac{1}{2}\#\{E\}]} \frac{q_M^{k(k+1)}}{q_{[\lambda M]}^{k(k-1)}}, \max_{1\leq k\leq [\frac{1}{2}(\#\{E\}-1)]} \frac{q_M^{(k+1)^2}}{q_{[\lambda M]}^{k^2}} \right). \tag{4.7}$$

Next, by Ramanujan's result, Entry 2.1,

$$\left| e^{2/a} - \frac{p}{q} \right| \geq \frac{C_1 \log\log q}{q^2 \log q}, \tag{4.8}$$

for some constant $C_1 > 0$, depending only on a, and all rational numbers p/q (with q large). We apply (4.8) with

$$\frac{p}{q} = \frac{p_m}{q_m}, \qquad m \in [M, \lambda M],$$

in combination with the inequality

$$\left| e^{2/a} - \frac{p_m}{q_m} \right| < \frac{1}{q_m q_{m+1}}, \tag{4.9}$$

which is valid for all m. It follows that

$$\frac{q_{m+1}}{q_m} < \frac{\log q_m}{C_1 \log\log q_m}. \tag{4.10}$$

Multiplying the inequalities (4.10) for all $m \in [M, [\lambda M] - 1]$, we see that

$$\frac{q_{[\lambda M]}}{q_M} < \prod_{m=M}^{[\lambda M]-1} \frac{\log q_m}{C_1 \log\log q_m} < \left(\frac{\log q_{[\lambda M]}}{C_1 \log\log q_{[\lambda M]}} \right)^{(\lambda-1)M}. \tag{4.11}$$

Also, from Ramanujan's work,

$$m \leq \frac{C_2 \log q_m}{\log\log q_m} \tag{4.12}$$

for some constant $C_2 > 0$ depending only on a and valid for all m sufficiently large. We now apply (4.12) with $m = \lceil \lambda M \rceil$ and insert the result in the exponent on the right-hand side of (4.11) to deduce that

$$\begin{aligned} \frac{q_{[\lambda M]}}{q_M} &< \left(\frac{\log q_{[\lambda M]}}{C_1 \log\log q_{[\lambda M]}} \right)^{\frac{(\lambda-1)C_2 \log q_{\lceil \lambda M \rceil}}{\lambda \log\log q_{\lceil \lambda M \rceil}}} \\ &= q_{[\lambda M]}^{\frac{(\lambda-1)C_2}{\lambda}\left(1+O_{C_1}\left(\frac{\log\log\log q_{[\lambda M]}}{\log\log q_{[\lambda M]}}\right)\right)}, \end{aligned} \tag{4.13}$$

where we noted that

$$\log q_{\lceil \lambda M \rceil} = \log q_{[\lambda M]} + O(\log\log q_{[\lambda M]}),$$

by (4.10).

Next, we choose any constant $C_3 > C_2$, for example, $C_3 = 2C_2$. Then, for all M sufficiently large in terms of C_1, C_2, C_3, and λ, we deduce from (4.13) that

$$\frac{q_{[\lambda M]}}{q_M} \leq q_{[\lambda M]}^{(\lambda-1)C_3/\lambda}. \tag{4.14}$$

For the remainder of the proof, we require that $\lambda > 1$ is close enough to 1 so that

$$\frac{(\lambda-1)C_3}{\lambda} < 1. \tag{4.15}$$

Therefore, by (4.14),

$$q_{[\lambda M]} \le q_M^{\frac{1}{1-(\lambda-1)C_3/\lambda}} = q_M^{\frac{\lambda}{\lambda-(\lambda-1)C_3}}. \tag{4.16}$$

Using (4.16) in (4.7), we obtain

$$L \ge \max\left(\max_{1\le k\le [\frac{1}{2}\#\{E\}]} q_M^{k(k+1)-\frac{\lambda k(k-1)}{\lambda-(\lambda-1)C_3}}, \max_{1\le k\le [\frac{1}{2}(\#\{E\}-1)]} q_M^{(k+1)^2-\frac{\lambda k^2}{\lambda-(\lambda-1)C_3}} \right). \tag{4.17}$$

We now proceed to derive an upper bound for L. We first bound L in terms of the $\sup$ norm of ψ, where ψ is defined for each $m \in E$ prior to (4.1). Thus, q_m divides $|a|^{\psi(m)}\psi(m)!$. It follows that q_m divides $|a|^{\psi(m)}||\psi||!$, where

$$||\psi|| = \max\{\psi(x) : x \in E\}.$$

Since the inequality above holds for each q_m, with $m \in E$, their least common multiple L is also a divisor of $|a|^{||\psi||}||\psi||!$, and hence

$$L \le |a|^{||\psi||}||\psi||!. \tag{4.18}$$

Our next aim is therefore to obtain an upper bound for $||\psi||$. Let $m_0 \in E$ be such that $\psi(m_0) = ||\psi||$. By (4.8), (4.13), and (4.16),

$$\left| e^{2/a} - \frac{p_{m_0}}{q_{m_0}} \right| \ge \frac{C_1 \log\log q_{m_0}}{q_{m_0}^2 \log q_{m_0}} \ge \frac{C_1 \log\log q_{[\lambda M]}}{q_{[\lambda M]}^2 \log q_{[\lambda M]}} \ge \frac{1}{q_M^{\frac{2\lambda}{\lambda-(\lambda-1)C_3}}}. \tag{4.19}$$

On the other hand,

$$\begin{aligned} \left| e^{2/a} - \frac{p_{m_0}}{q_{m_0}} \right| &= \left| e^{2/a} - \frac{A_{\psi(m_0)}}{|a|^{\psi(m_0)}\psi(m_0)!} \right| = \left| \sum_{n>\psi(m_0)} \frac{2^n}{a^n n!} \right| \\ &= \frac{2^{\psi(m_0)+1}}{|a|^{\psi(m_0)+1}(\psi(m_0)+1)!} \left(1 + O_a\left(\frac{1}{\psi(m_0)} \right) \right) \le \frac{2^{||\psi||}}{|a|^{||\psi||}||\psi||!}. \end{aligned} \tag{4.20}$$

By (4.19) and (4.20), it follows that

$$|a|^{||\psi||}||\psi||! \le 2^{||\psi||} q_M^{\frac{2\lambda}{\lambda-(\lambda-1)C_3}}. \tag{4.21}$$

By Stirling's formula,

$$2^{||\psi||} = \left(|a|^{||\psi||}||\psi||! \right)^{O(1/\log||\psi||)}. \tag{4.22}$$

By (4.21) and (4.22), we find that

$$|a|^{||\psi||}||\psi||! \le q_M^{\frac{2\lambda}{\lambda-(\lambda-1)C_3}(1+O(1/\log||\psi||))} \le q_M^{\frac{2\lambda}{\lambda-(\lambda-1)C_4}}, \tag{4.23}$$

for any fixed C_4 such that $C_4 > C_3$, and for any sufficiently large M in terms of a, C_3, C_4, and λ.

Combining (4.17), (4.18), and (4.23), we finally conclude that

$$\frac{2\lambda}{\lambda-(\lambda-1)C_4} \geq \max\left(\max_{1\leq k\leq \left[\frac{1}{2}\#\{E\}\right]} k(k+1) - \frac{\lambda k(k-1)}{\lambda-(\lambda-1)C_3}, \right.$$
$$\left. \max_{1\leq k\leq \left[\frac{1}{2}(\#\{E\}-1)\right]} (k+1)^2 - \frac{\lambda k^2}{\lambda-(\lambda-1)C_3} \right). \tag{4.24}$$

Rather than compute explicitly the maximum on the right-hand side of (4.24) as a function of C_3, λ, and $\#\{E\}$, we remark that a *fixed* $k \geq 1$ can be used to finish the proof of the theorem. To be precise, if we keep k fixed and let $\lambda \to 1$, then the left side of (4.24) tends to 2, while the two quantities corresponding to k on the right-hand side of (4.24) tend to $k(k+1) - k(k-1) = 2k$ and $(k+1)^2 - k^2 = 2k+1$, respectively. We thus obtain a contradiction if $\#\{E\} > 2k$ and $1 < \lambda < \lambda_k$ for some suitable $\lambda_k > 1$ depending only on a and k. This in turn implies that $\#\{E\} \leq 2k$, for any interval of the form $[M, \lambda_k M]$, with M sufficiently large. Hence the total number of convergents p_m/q_m to the continued fraction of $e^{2/a}$ with $m \leq x$ is bounded by $\log x$ times a constant, which depends only on k and a.

For example, if we take $k = 1$ and fix a $\lambda_1 > 1$ for which

$$\frac{2\lambda_1}{\lambda_1-(\lambda_1-1)C_4} < 4 - \frac{\lambda_1}{\lambda_1-(\lambda_1-1)C_3}, \tag{4.25}$$

and which also satisfies (4.15), then there are at most two values of m in any interval of the form $[M, \lambda_1 M]$ with M sufficiently large, for which p_m/q_m is a partial sum of the Taylor series of $e^{2/a}$. In conclusion, we have established Theorem 4.1. □

5. Analysis of the Partial Denominators of the Continued Fraction of e

In [15], Sondow and Schalm, via a 2-adic approach, obtained various partial results towards Sondow's Conjecture. As we demonstrate below, replacing 2 by other, well-chosen prime numbers is advantageous. Let

$$\frac{A_n}{n!} = \sum_{\ell=0}^{n} \frac{1}{\ell!},$$

and let p_n/q_n denote the nth convergent to the (simple) continued fraction of e. The numbers A_n satisfy the recurrence formula

$$A_n = 1 + nA_{n-1}, \qquad n \geq 1, \qquad A_0 = 1. \tag{5.1}$$

Thus, $A_1 = 2$, $A_2 = 5$, $A_3 = 16$, $A_4 = 65$, $A_5 = 326$, $A_6 = 1957$, $A_7 = 13700$, $A_8 = 109601$, $A_9 = 986410$, $A_{10} = 9864101$, ... As shown in [15], any power of 2 divides infinitely many A_n. By contrast, there are prime numbers that do not divide any A_n. We denote by $\mathcal{A}$ the set of primes that do not divide any A_n. (For considerable information about the sequence A_n, see sequence A000522 in [13]. Furthermore, in connection with $\mathcal{A}$, readers may wish to consult sequence A072456 in [13].) For any prime number p, the sequence $A_n \pmod p$ is periodic with period p, since $A_p = 1 + pA_{p-1} \equiv A_0 \pmod p$, and if $A_{k+p} \equiv A_k \pmod p$, then $A_{k+1+p} \equiv A_{k+1} \pmod p$, by the recurrence (5.1). Thus, in order to check whether a given prime number p is in $\mathcal{A}$, it is sufficient to see if it divides any of

the numbers $A_0, A_1, \ldots, A_{p-1}$. For example, since none of the numbers $A_0, A_1, \ldots, A_{10}$ is divisible by 11, it follows that 11 is in $\mathcal{A}$. Similarly, none of the numbers $A_0, A_1, \ldots, A_6$ is a multiple of 7, so 7 belongs to $\mathcal{A}$. Since $A_2 \equiv 0 \pmod 5$ and $A_4 \equiv 0 \pmod{13}$, the primes 5 and 13 are not in $\mathcal{A}$.

3	7	11	17	47	53	61	67	73	79
89	101	139	151	157	191	199	229	233	241
263	269	277	283	311	317	337	347	359	367
379	397	433	449	467	487	503	521	541	563
569	571	577	593	607	613	619	647	659	673
683	691	727	743	769	773	809	823	827	911
919	929	953	971	991	1013	1021	1039	1051	1061
1103	1109	1117	1181	1201	1213	1229	1231	1249	1259
1277	1283	1303	1361	1373	1409	1423	1427	1433	1459
1471	1493	1549	1553	1567	1571	1579	1583	1597	1607
1609	1613	1619	1627	1637	1657	1667	1669	1709	1747
1777	1783	1787	1811	1871	1873	1879	1889	1933	1949
1951	1973	1987	2017	2027	2029	2039	2053	2083	2087
2089	2111	2129	2131	2141	2143	2153	2243	2269	2273
2309	2333	2339	2347	2371	2377	2381	2399	2423	2459
2531	2551	2557	2593	2633	2647	2657	2683	2689	2699
2719	2729	2741	2753	2767	2789	2791	2797	2833	2887
2897	2917	2969	2999	3023	3067	3089	3181	3187	3191
3209	3217	3229	3251	3253	3259	3271	3299	3301	3361
3389	3469	3517	3533	3539	3541	3557	3559	3571	3583

TABLE 1. Table of primes in $\mathcal{A}$

Inspecting this table, we are led to make the following conjecture.

Conjecture 5.1. *If $A(x)$ denotes the number of primes in $\mathcal{A}$ that are $\leq x$, then*

$$\lim_{x\to\infty} \frac{A(x)}{\pi(x)} = \frac{1}{e}. \tag{5.2}$$

We shall attack Sondow's Conjecture by comparing the powers of a fixed prime number p in the sequence of partial sums $A_n/n!$ with those appearing in the sequence of convergents p_n/q_n. Given a prime p, let us denote by $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ the p-adic valuation, defined by $v_p(0) = \infty$ and $v_p(r) = m$ if $r = p^m \frac{a}{b}$, where $m, a, b \in \mathbb{Z}$, $(p, a) = (p, b) = 1$. Assume now that $p \in \mathcal{A}$. Then, for any n, $v_p(A_n) = 0$ and [8, p. 182, Theorem 4.2]

$$v_p\left(\frac{A_n}{n!}\right) = -v_p(n!) = -\sum_{\ell=1}^{\infty} \left\lfloor \frac{n}{p^\ell} \right\rfloor. \tag{5.3}$$

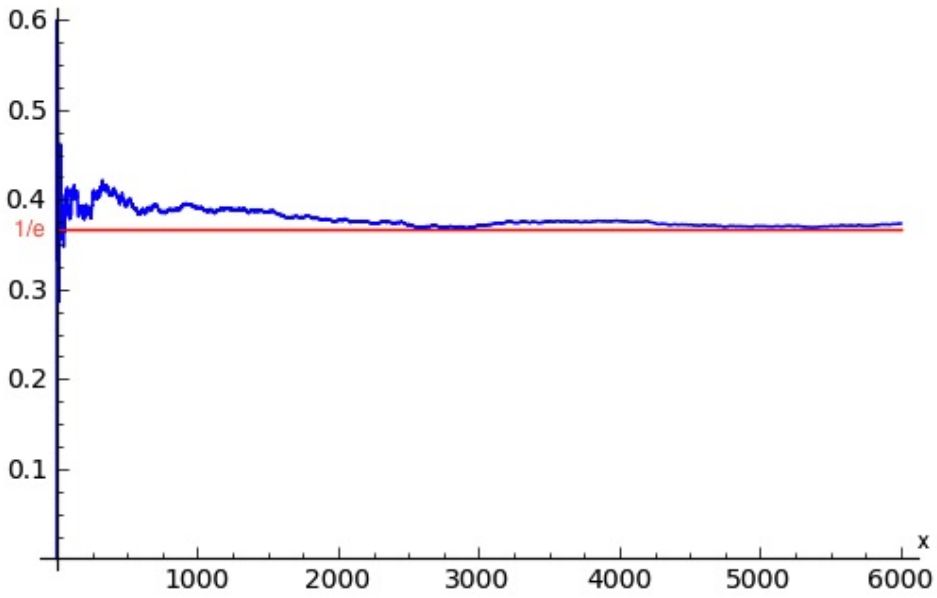

FIGURE 1. Graph of $A(x)/\pi(x)$

Suppose that, for some n, we have a counterexample to Sondow's Conjecture, i.e.,

$$\frac{A_n}{n!} = \frac{p_m}{q_m}$$

for some m. Then

$$\frac{1}{(n+1)!} < \left| e - \frac{A_n}{n!} \right| = \left| e - \frac{p_m}{q_m} \right| < \frac{1}{q_m q_{m+1}}. \tag{5.4}$$

The continued fraction of e is given by

$$\langle 2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, \dots \rangle, \tag{5.5}$$

and the corresponding recurrence relation for the denominators q_j is given by

$$q_j = h_j q_{j-1} + q_{j-2}, \qquad j \geq 2, \qquad q_0 = 0, \quad q_1 = 1, \tag{5.6}$$

where, for $j \geq 2$,

$$h_j = \begin{cases} \dfrac{2j}{3}, & \text{if } 3 \mid j, \\ 1, & \text{if } 3 \nmid j. \end{cases} \tag{5.7}$$

As a consequence of (5.6) and (5.7), we see that

$$q_m > \prod_{j=2}^{m} h_j = 2^{\lfloor m/3 \rfloor} \left(\left\lfloor \frac{m}{3} \right\rfloor \right)!, \qquad m \geq 2, \tag{5.8}$$

which, in combination with (5.4), implies that

$$(n+1)! > 2^{\lfloor m/3 \rfloor + \lfloor (m+1)/3 \rfloor} \left(\left\lfloor \frac{m}{3} \right\rfloor \right)! \left(\left\lfloor \frac{m+1}{3} \right\rfloor \right)!. \tag{5.9}$$

For any positive integers a, b, we easily see that

$$2^{a+b}a!b! > \binom{a+b}{a}a!b! = (a+b)!. \tag{5.10}$$

Applying (5.10) with

$$a = \left\lfloor \frac{m}{3} \right\rfloor \quad \text{and} \quad b = \left\lfloor \frac{m+1}{3} \right\rfloor$$

on the right side of (5.9), we find that

$$n \geq \left\lfloor \frac{m}{3} \right\rfloor + \left\lfloor \frac{m+1}{3} \right\rfloor. \tag{5.11}$$

The bound (5.11) is an improvement on

$$n \geq 1 + \left\lfloor \frac{m}{3} \right\rfloor,$$

which was used in [15]. Since p_m and q_m are relatively prime, $p_m/q_m = A_n/n!$, and $p \nmid A_n$, it follows that $p \nmid p_m$. Then, by (5.3) and (5.11),

$$\begin{aligned} v_p(q_m) &= -v_p\left(\frac{p_m}{q_m}\right) = -v_p\left(\frac{A_n}{n!}\right) = \sum_{\ell=1}^{\infty} \left\lfloor \frac{n}{p^\ell} \right\rfloor \\ &\geq \sum_{\ell=1}^{\infty} \left\lfloor \frac{\left\lfloor \frac{m}{3} \right\rfloor + \left\lfloor \frac{m+1}{3} \right\rfloor}{p^\ell} \right\rfloor := \mu, \end{aligned} \tag{5.12}$$

for any prime $p \in \mathcal{A}$ and any positive integer m for which the convergent p_m/q_m equals a partial sum $A_n/n!$. In [15], the authors considered only the prime 2, for which

$$\overline{\lim_{n\to\infty}}\, v_2(A_n) = \infty.$$

6. SYMMETRIES

We now proceed to study the distribution of the denominators q_m modulo powers of a fixed prime p, with the aim of finding a prime p in $\mathcal{A}$ for which the far right side of (5.12) is larger than $v_p(q_m)$ for m sufficiently large. We first define h_j for $j = 1, 0, -1, -2, \ldots$ in such a way so that (5.7) holds for all $j \in \mathbb{Z}$. Next, we define q_j recursively for $j = -1, -2, \ldots$ by letting

$$q_j = -h_{j+2}q_{j+1} + q_{j+2},$$

so that (5.6) holds for each integer j. The first few positive and negative values of q_m are given in the table below.

m	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
q_m	3	-4	-1	0	-1	-1	1	0	1	0	1	1	3	4	7	32	39	71	465

We notice that the numbers on the left part of the table are the same as those on the right, but not in the same order, and some of them are multiplied by -1. The relations that we have

m	-18	-17	-16	-15	-14	-13	-12	-11	-10	10	11	12	13	14
q_m	8544	-9545	-1001	465	-536	-71	32	-39	-7	536	1001	8544	9545	18089

observed are more elegantly stated as symmetries inside three subsequences corresponding to m given in residue classes modulo 3 as follows:

Case 1: $m \equiv 0 \pmod 3$

m	-18	-15	-12	-9	-6	-3	0	3	6	9	12
q_m	8544	465	32	3	0	1	0	3	32	465	8544

Here we have a symmetry with respect to $m = -3$ in the sense that

$$q_m = q_{-6-m}, \qquad \text{for all } m \in \mathbb{Z}, m \equiv 0 \pmod 3. \tag{6.1}$$

Case 2: $m \equiv 1 \pmod 3$

m	-17	-14	-11	-8	-5	-2	1	4	7	10	13
q_m	-9545	-536	-39	-4	-1	0	1	4	39	536	9545

In this case, the symmetry is with respect to -2, namely,

$$q_m = -q_{-4-m}, \qquad \text{for all } m \in \mathbb{Z}, m \equiv 1 \pmod 3. \tag{6.2}$$

Case 3: $m \equiv -1 \pmod 3$

m	-16	-13	-10	-7	-4	-1	2	5	8	11	14
q_m	-1001	-71	-7	-1	-1	1	1	7	71	1001	18089

In this case, the symmetry is with respect to -2.5. More precisely,

$$q_m = -q_{-5-m}, \qquad \text{for all } m \in \mathbb{Z}, m \equiv -1 \pmod 3. \tag{6.3}$$

In order to prove (6.1)–(6.3), it suffices to show that for any positive integer ℓ,

$$q_{3\ell} = q_{-3\ell-6}, \qquad q_{3\ell+1} = -q_{-3\ell-5}, \qquad q_{3\ell+2} = -q_{-3\ell-7}. \tag{6.4}$$

We prove (6.4) by induction on ℓ. The case $\ell = 1$ is easily verified from an inspection of the tables above. Suppose now that $\ell \geq 2$ and assume that (6.4) holds with ℓ replaced by $\ell - 1$, i.e.,

$$q_{3\ell-3} = q_{-3\ell-3}, \qquad q_{3\ell-2} = -q_{-3\ell-2}, \qquad q_{3\ell-1} = -q_{-3\ell-4}. \tag{6.5}$$

Using (6.5) and applying the recurrence formula (5.6) and (5.7) repeatedly, we find that

$$q_{3\ell} = 2\ell q_{3\ell-1} + q_{3\ell-2} = -2\ell q_{-3\ell-4} - q_{-3\ell-2}$$
$$= -(2\ell+1)q_{-3\ell-4} - q_{-3\ell-3} = q_{-3\ell-4} - q_{-3\ell-5} = q_{-3\ell-6}.$$

Thus, the first equality in (6.4) has been demonstrated. The remaining two equalities in (6.4) are established in the same manner. Thus, (6.1)–(6.3) are valid.

We now consider a sequence of matrices

$$E_j = \begin{pmatrix} h_j & 1 \\ 1 & 0 \end{pmatrix}, \qquad j \in \mathbb{Z}. \tag{6.6}$$

Given a positive integer L, by a block of length L, we mean a product of the form $E_{j+L}E_{j+L-1}\cdots E_{j+1}$, where j is any integer. For such a product, by (5.6) and (6.6),

$$\begin{pmatrix} q_{j+L} \\ q_{j+L-1} \end{pmatrix} = E_{j+L}E_{j+L-1}\cdots E_{j+1}\begin{pmatrix} q_j \\ q_{j-1} \end{pmatrix}. \tag{6.7}$$

In particular, the numbers q_m can be recovered as entries in such products. More precisely, for each $m \geq 1$,

$$E_{m+1}E_m\cdots E_2 = \begin{pmatrix} q_{m+1} & * \\ q_m & * \end{pmatrix}. \tag{6.8}$$

This leads us to study the p-adic valuation of entries of such products, and more specifically, in light of (5.12), we would like to know under what circumstances the product on the left-hand side of (6.8) belongs to the congruence subgroup

$$\Gamma(p^\mu) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc = 1, c \equiv 0 \,(\mathrm{mod}\, p^\mu) \right\},$$

where μ is defined on the right-hand side of (5.12).

It is worth mentioning that the right-hand side of (6.8) is actually

$$\begin{pmatrix} q_{m+1} & p_{m+1} \\ q_m & p_m \end{pmatrix}\begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

With this, one could prove results for (p_m) analogous to those for (q_m).

7. Basic Congruences for the Denominators q_m

To proceed, we fix an odd prime number p, and show that any block whose length is a multiple of $3(p-1)(p+1)p^{k+1}$ produces the identity matrix I modulo p^k.

Lemma 7.1. *Let p be an odd prime. For any positive integer k, any positive integer L that is a multiple of $3(p-1)(p+1)p^{k+1}$, and any integer j,*

$$E_{j+L}E_{j+L-1}\cdots E_{j+1} \equiv I \,(\mathrm{mod}\, p^k). \tag{7.1}$$

Proof. We prove the lemma by induction on k. For $k = 1$, let L be a multiple of $3(p-1)(p+1)p^2$ and let j be an integer. We send each E_{j+i}, $1 \leq i \leq L$, to $GL_2(\mathbb{F}_p)$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The group has order $(p-1)^2p(p+1)$, and the order of any of its elements is a divisor of $(p-1)(p+1)p$. Modulo p, the sequence $\{h_\ell\}$, $\ell \in \mathbb{Z}$, is periodic with period $3p$, and so the sequence $\{E_\ell\}$ is periodic with period $3p$. Therefore, $E_{j+L}E_{j+L-1}\cdots E_{j+1}$ can be subdivided into products of consecutive blocks of length $3p$ each, which have the same image, say A, in $GL_2(\mathbb{F}_p)$. Then $E_{j+L}E_{j+L-1}\cdots E_{j+1}$ is congruent to $A^{L/(3p)} = I$ in $GL_2(\mathbb{F}_p)$, which completes the proof for $k = 1$.

Assume now that (7.1) is valid for any particular $k \geq 1$, for all blocks of lengths that are multiples of $3(p-1)(p+1)p^{k+1}$. Let L be a multiple of $3(p-1)(p+1)p^{k+2}$, and let j be any integer. We subdivide $E_{j+L}E_{j+L-1}\cdots E_{j+1}$ into a product of p blocks, each of length L/p. Modulo p^{k+1}, the sequence $\{E_\ell\}$, $\ell \in \mathbb{Z}$, is periodic with period $3p^{k+1}$, which divides L/p. So the aforementioned p blocks of length L/p are congruent to each other modulo p^{k+1}. By the induction hypothesis, we may write the first one of them in the form

$$E_{j+L/p}E_{j+L/p-1}\cdots E_{j+1} = I + p^kX,$$

where the matrix X has integer entries. Then

$$E_{j+L}E_{j+L-1}\cdots E_{j+1} \equiv (I+p^kX)^p \equiv I \,(\mathrm{mod}\, p^{k+1}), \tag{7.2}$$

and this completes the proof of Lemma 7.1. □

By Lemma 7.1 and (6.7), it follows that

$$q_{j+L} \equiv q_j \,(\mathrm{mod}\, p^k), \tag{7.3}$$

for all $L \equiv 0 \,(\mathrm{mod}\, 3(p-1)(p+1)p^{k+1})$ and all integers j. Thus, the smallest period of the sequence $q_j \,(\mathrm{mod}\, p^k)$ is always a divisor of $3(p-1)(p+1)p^{k+1}$. Sondow and Schalm [14], [15] have conjectured that for every odd integer $M > 1$, the period of the sequence $q_j \,(\mathrm{mod}\, M)$ is equal to $6M$, and for every even integer $M > 0$, the period of $q_j \,(\mathrm{mod}\, M)$ divides $3M$. They also have numerically verified the conjecture for all $M \leq 1000$. This is an elegant conjecture, of wider interest than Sondow's Conjecture on instances when partial sums of the Taylor series of e coincide with convergents to the continued fraction of e, because the former conjecture shows that the convergents of e exhibit certain elegant and interesting arithmetical properties. It is easy to see, by the Chinese Remainder Theorem, that the conjecture holds for all $M > 1$ if and only if it holds for all prime powers. Also, from our next result, it follows that if the conjecture holds for a given odd prime number p, then it is also valid for all p^k, $k \geq 1$. Since in our application to Sondow's Conjecture, we eventually will work with concrete primes $p < 1000$, for which Sondow and Schalm's conjecture has already been checked, we may therefore assume in the sequel that $q_j \,(\mathrm{mod}\, p^k)$ is periodic with period $6p^k$, for each $k \geq 1$.

Proposition 7.2. *Let p be an odd prime. The following are equivalent.*

(1) $q_{j+6p} \equiv q_j \,(\mathrm{mod}\, p)$, *for all integers j.*
(2) $q_{j+6p^k} \equiv q_j \,(\mathrm{mod}\, p^k)$, *for all integers j and positive integers k.*
(3) $E_{j+6p}E_{j+6p-1}\cdots E_{j+1} \equiv I \,(\mathrm{mod}\, p)$, *for all integers j.*
(4) $E_{j+L}E_{j+L-1}\cdots E_{j+1} \equiv I \,(\mathrm{mod}\, p^k)$, *for all integers j, for all $k \geq 1$, and for all $L > 0$ such that $L \equiv 0 \,(\mathrm{mod}\, 6p^k)$.*
(5) $q_{3p-2} \equiv 0 \,(\mathrm{mod}\, p)$ *and* $q_{3p-1} \equiv \pm 1 \,(\mathrm{mod}\, p)$.

In what follows, we denote

$$\mathcal{B} = \text{the set of prime numbers that satisfy the conditions of Proposition 7.2.} \tag{7.4}$$

Proof of Proposition 7.2. We will end the proof by showing that (3) implies (4).

Employing (6.7) with $L = 6p^k$, we see that (4) implies (2), which in turn implies (1).

In order to show that (5) is a consequence of (1), we use the symmetry (6.2). Letting $m = 3p-2$ in (6.2), we deduce that $q_{3p-2} = -q_{-3p-2}$. On the other hand, taking $j = -3p-2$ in (1) yields $q_{3p-2} \equiv q_{-3p-2} \,(\mathrm{mod}\, p)$. Since p is odd, we deduce that $q_{3p-2} \equiv 0 \,(\mathrm{mod}\, p)$.

Next, setting $L = 3p$ and $j = -1$ in (6.7), and recalling that $q_{-2} = 0$ and $q_{-1} = 1$, we find that

$$\begin{pmatrix} q_{3p-1} \\ q_{3p-2} \end{pmatrix} = E_{3p-1}E_{3p-2}\cdots E_0 \begin{pmatrix} 1 \\ 0 \end{pmatrix}. \tag{7.5}$$

Hence,

$$E_{3p-1}E_{3p-2}\cdots E_0 = \begin{pmatrix} q_{3p-1} & * \\ q_{3p-2} & * \end{pmatrix}. \tag{7.6}$$

If we denote by A the image of $E_{3p-1}E_{3p-2}\cdots E_0$ in $GL_2(\mathbb{F}_p)$, and by y the image of q_{3p-1} in $\mathbb{F}_p$, then A has the form

$$A = \begin{pmatrix} y & * \\ 0 & * \end{pmatrix}.$$

Since the sequence $\{E_\ell\}$, $\ell \in \mathbb{Z}$, is periodic modulo p with period $3p$, it follows that $E_{6p-1}E_{6p-2}\cdots E_{3p}$ has the same image in $GL_2(\mathbb{F}_p)$ as $E_{3p-1}E_{3p-2}\cdots E_0$, namely A. Then $E_{6p-1}E_{6p-2}\cdots E_0$ projects to A^2, which has the form

$$A^2 = \begin{pmatrix} y^2 & * \\ 0 & * \end{pmatrix}.$$

On the other hand, by (6.7) with $L = 6p$ and $j = 0$, in similarity with (7.6),

$$E_{6p-1}E_{6p-2}\cdots E_0 = \begin{pmatrix} q_{6p-1} & * \\ q_{6p-2} & * \end{pmatrix}. \tag{7.7}$$

Reducing (7.7) modulo p, we see that the left-hand side projects to A^2, while the right-hand side projects to a matrix of the form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$ by the periodicity of (1) and the facts that $q_{-1} = 1$ and $q_{-2} = 0$. In conclusion, $y^2 = 1$ in $\mathbb{F}_p$, and (5) follows.

Next, we prove that (5) implies (3). Denote again by A the image of $E_{3p-1}E_{3p-2}\cdots E_0$ in $GL_2(\mathbb{F}_p)$. By (7.6) and the assumption (5), A has the form

$$A = \begin{pmatrix} \pm 1 & * \\ 0 & * \end{pmatrix}.$$

Since for each integer j, $\det E_j = -1$, it follows that $\det A = -1$. Thus, A has the form

$$A = \begin{pmatrix} 1 & * \\ 0 & -1 \end{pmatrix} \qquad \text{or} \qquad A = \begin{pmatrix} -1 & * \\ 0 & 1 \end{pmatrix}. \tag{7.8}$$

Observe that all possible matrices appearing in (7.8) satisfy the identity $A^2 = I$. It follows that

$$E_{6p-1}E_{6p-2}\cdots E_0 \equiv I \,(\mathrm{mod}\, p), \tag{7.9}$$

which implies that (3) holds for $j = -1$, and indeed for any j in the arithmetic progression $j = -1 + 3\ell$, for all integers ℓ. Finally, to prove (3) for every integer j, it suffices to verify it for $0 \le j < 6p - 1$. For such j, write

$$\begin{aligned} U &= E_{6p-1}E_{6p-2}\cdots E_{j+1}, \\ V &= E_{6p+j}E_{6p+j-1}\cdots E_{6p}, \\ W &= E_jE_{j-1}\cdots E_0, \end{aligned}$$

and notice that $V \equiv W \,(\mathrm{mod}\, p)$, and $UW = E_{6p-1}E_{6p-2}\cdots E_0 \equiv I \,(\mathrm{mod}\, p)$ by (7.9). Hence,

$$E_{6p+j}E_{6p+j-1}\cdots E_{j+1} = VU = V(UW)W^{-1} \equiv VW^{-1} \equiv I \,(\mathrm{mod}\, p). \tag{7.10}$$

This proves that (5) implies (3).

It remains to prove that (3) implies (4). One may be tempted to think that by the same argument that was used in the proof of Lemma 7.1, one can deduce that (3) implies (4). But, that argument does not work with only $6p^k$ as a period; it must be a multiple of $3p^{k+1}$. Let

us consider the following example provided by one of the referees. Let $p = 5, k = 1$ in the proof of Lemma 7.1 and define B_j and X_j by

$$B_j = \prod_{i=30j-29}^{30j} E_i = I + 5X_j, \qquad \text{for } j = 1, 2, 3, 4, 5.$$

For the argument from the proof of Lemma 7.1 to work in this case one would need all the X_j's to be congruent to each other modulo 5. That would imply that $\prod B_j \equiv I \pmod{5^2}$, which is what we need in part (4) of Proposition 7.2. But we find that

$$X_1 \equiv \begin{pmatrix} 4 & 1 \\ 0 & 1 \end{pmatrix} \pmod 5,\ X_2 \equiv \begin{pmatrix} 1 & 1 \\ 4 & 4 \end{pmatrix} \pmod 5,\ X_3 \equiv \begin{pmatrix} 3 & 1 \\ 3 & 2 \end{pmatrix} \pmod 5,$$

$$X_4 \equiv \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix} \pmod 5,\ X_5 \equiv \begin{pmatrix} 2 & 1 \\ 1 & 3 \end{pmatrix} \pmod 5.$$

We have

$$\prod B_j \equiv \prod (I + 5X_j) \equiv I + 5 \sum X_j \pmod{5^2}.$$

Surprisingly, one does have $\sum X_j \equiv 0 \pmod 5$ in the example above, so the conclusion $\prod B_j \equiv I \pmod{5^2}$ is still true. We would like to understand this phenomenon which is responsible for the extra factor of 5. The key observation here is that the matrices $X_1, \dots, X_5$ form an arithmetic progression modulo 5. More precisely, if we let $Y := \begin{pmatrix} 2 & 0 \\ 4 & 3 \end{pmatrix}$, then

$$Y \equiv X_{j+1} - X_j \pmod 5, \qquad \text{for } j = 1, 2, 3, 4.$$

Therefore

$$X_1 + \cdots + X_5 \equiv X_1 + (X_1 + Y) + \cdots + (X_1 + 4Y) \equiv 5X_1 + 10Y \equiv 0 \pmod 5.$$

We now present an alternative proof of the above key fact that the matrices $X_1, \dots, X_5$ form an arithmetic progression modulo 5. The proof below does not make use of the explicit computation of $X_1, \dots, X_5$, and it makes obvious the fact that the phenomenon holds more generally, and that (4) follows from (3), as claimed.

Let us note that if j is a multiple of 3, $E_{j+30} = E_j + \begin{pmatrix} 20 & 0 \\ 0 & 0 \end{pmatrix}$, and otherwise $E_{j+30} = E_j$. Therefore, if we denote, for the moment, $T = \begin{pmatrix} 20 & 0 \\ 0 & 0 \end{pmatrix}$, we have

$$B_2 = E_{60} \cdots E_{31} = (E_{30} + T)E_{29}E_{28}(E_{27} + T)E_{26} \cdots (E_3 + T)E_2E_1.$$

If we expand the product on the right-hand side above, we find one term that does not contain any T's, which is exactly B_1. Then there are some linear terms in T, and some terms which contain two or more factors of T. Those terms that contain at least two factors of T are congruent to zero modulo 25. It follows that

$$B_2 - B_1 \equiv \text{ sum of linear terms in } T \pmod{25}.$$

Next, $E_{j+60} = E_j$ for j not a multiple of 3 and $E_{j+60} = E_j + 2T$ if 3 divides j. Thus,

$$B_3 = E_{90} \cdots E_{61} = (E_{30} + 2T)E_{29}E_{28}(E_{27} + 2T)E_{26} \cdots (E_3 + 2T)E_2E_1.$$

As above, $B_3 - B_1$ is congruent to the sum of linear terms in T modulo 25. These linear terms are exactly the same as before, except T is replaced by $2T$ (and respectively by $3T$ or $4T$ if instead of $B_3 - B_1$ one considers $B_4 - B_1$ or $B_5 - B_1$). It follows that

$$B_3 - B_1 \equiv 2(B_2 - B_1) \,(\mathrm{mod}\, 25),$$

which shows that X_1, X_2, X_3 are in arithmetic progression modulo 5 (and similarly for X_4 and X_5). Clearly the same argument works in more generality. Instead of breaking a block of length 150 in 5 blocks of length 30 each, one breaks a block of length $6p^{k+1}$ into p blocks of length $6p^k$ each. Corresponding to these p blocks one has matrices B_j, X_j with $B_j = I + p^k X_j$ for $j = 1, \ldots, p$. As above, one finds that the X_j's form an arithmetic progression modulo p. If $Y \equiv X_{j+1} - X_j \,(\mathrm{mod}\, p)$, $j = 1, \ldots, p-1$, then

$$\sum_{j=1}^{p} X_j \equiv pX_1 + \frac{p(p-1)}{2} Y \equiv 0 \,(\mathrm{mod}\, p),$$

which in turn gives

$$B_p B_{p-1} \cdots B_1 \equiv I + p^k \sum_{j=1}^{p} X_j \equiv I \,(\mathrm{mod}\, p^{k+1}).$$

This proves that (3) implies (4), and completes the proof of Proposition 7.2.

Remark. The same referee has offered an alternative, shorter proof that (1) implies (5) above, as follows. The coefficients in the recurrence for q are periodic modulo p with period $3p$, and the recurrence is homogeneous, so if there exists c such that $q_{3p-2} \equiv cq_{-2} \,(\mathrm{mod}\, p)$ and $q_{3p-1} \equiv cq_{-1} \,(\mathrm{mod}\, p)$, then for all j, $q_{3p+j} \equiv cq_j \,(\mathrm{mod}\, p)$, and furthermore

$$q_{6p+j} \equiv cq_{3p+j} \equiv c^2 q_j \,(\mathrm{mod}\, p). \tag{7.11}$$

Defining $c = q_{3p-1}$ satisfies our requirements since $q_{3p-2} \equiv q_{-2} \equiv 0 \,(\mathrm{mod}\, p)$ (as shown in the proof above) and $q_{-1} = 1$. From (1) and (7.11) we see that $c^2 \equiv 1 \,(\mathrm{mod}\, p)$ and thus $c \equiv \pm 1 \,(\mathrm{mod}\, p)$ as required.

As a bonus, this argument shows that (5) implies (1) as well.

As observed by the authors numerically, and rediscovered by the referee, it appears that one always has $q_{3p-1} \equiv -1 \,(\mathrm{mod}\, p)$. We do not know how to prove this, and offer it as an open problem to the reader. □

8. SUPERCONGRUENCES

In the proof that (3) implies (4) in Proposition 7.2, we saw an instance where a given congruence holds modulo a higher power of p than expected. In the present section, we pursue this line of reasoning in a more systematic way. Our key result in this direction is Lemma 8.2 below. As before, we provide an unconditional version of the lemma, which shows that q_j satisfies attractive supercongruences modulo powers of any odd prime p, and a conditional version, valid for primes in $\mathcal{B}$, which is used to attack Sondow's Conjecture. We

first need some preparation. For any $p \in \mathcal{B}$, any integer j, and any $\ell \in \{j+1, \dots, j+6p^k\}$, with $\ell \equiv 0 \pmod 3$, denote

$$M_{p,k,j,\ell} = E_{j+6p^k} \cdots E_{\ell+1} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} E_{\ell-1} \cdots E_{j+1}. \tag{8.1}$$

Lemma 8.1. *In the notation above, for any prime $p \in \mathcal{B}$, any $k \geq 1$, and any integer j,*

$$\sum_{\substack{j+1 \leq \ell \leq j+6p^k \\ \ell \equiv 0 \pmod 3}} M_{p,k,j,\ell} \equiv 0 \pmod{p^{k-1}}. \tag{8.2}$$

Proof. We proceed by induction on k. There is nothing to prove when $k = 1$. Let $k \geq 2$ and assume that (8.2) holds for $k-1$. The principal idea is that although $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ does not commute with the matrices E_i, we are able to obtain congruences involving suitable pairs $M_{p,k,j,\ell}$, $M_{p,k,j,\ell'}$ by applying (4) of Proposition 7.2 to the product of those E_i, $\ell \leq i \leq \ell'$. To be precise, let $j+1 \leq \ell < \ell' \leq j+6p^k$, where $\ell \equiv 0 \pmod 3$ and $\ell \equiv \ell' \pmod{6p^{k-1}}$. Then, by (8.1),

$$M_{p,k,j,\ell} - M_{p,k,j,\ell'} = U \left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} V - W \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \right) T, \tag{8.3}$$

where

$$U = E_{j+6p^k} \cdots E_{\ell'+1}, \qquad T = E_{\ell-1} \cdots E_{j+1}, \tag{8.4}$$

and

$$V = E_{\ell'-1} \cdots E_{\ell}, \qquad W = E_{\ell'} \cdots E_{\ell+1}. \tag{8.5}$$

Each block in (8.5) has length $\ell' - \ell$, which is a multiple of $6p^{k-1}$, and so by (4) of Proposition 7.2,

$$V \equiv I \pmod{p^{k-1}} \qquad \text{and} \qquad W \equiv I \pmod{p^{k-1}}. \tag{8.6}$$

Combining (8.3) with (8.6), we deduce that

$$M_{p,k,j,\ell} \equiv M_{p,k,j,\ell'} \pmod{p^{k-1}}, \qquad \text{for all } \ell' \equiv \ell \pmod{6p^{k-1}}. \tag{8.7}$$

For each ℓ with $j+1 \leq \ell \leq j+6p^{k-1}$ and $j \equiv 0 \pmod 3$, there are exactly p numbers ℓ' with $j+1 \leq \ell' \leq j+6p^k$ and $\ell' \equiv \ell \pmod{6p^{k-1}}$. Hence, by (8.7), (8.1), and (4) of Proposition 7.2,

$$\begin{aligned} \sum_{\substack{j+1 \leq \ell \leq j+6p^k \\ \ell \equiv 0 \pmod 3}} M_{p,k,j,\ell} &\equiv p \sum_{\substack{j+1 \leq \ell \leq j+6p^{k-1} \\ \ell \equiv 0 \pmod 3}} M_{p,k,j,\ell} \pmod{p^{k-1}} \\ &\equiv p \sum_{\substack{j+1 \leq \ell \leq j+6p^{k-1} \\ \ell \equiv 0 \pmod 3}} M_{p,k-1,j,\ell} E_{j+1+6p^{k-1}} \cdots E_{j+6p^k} \pmod{p^{k-1}} \\ &\equiv p \sum_{\substack{j+1 \leq \ell \leq j+6p^{k-1} \\ \ell \equiv 0 \pmod 3}} M_{p,k-1,j,\ell} I \pmod{p^{k-1}}. \end{aligned} \tag{8.8}$$

Using the induction hypothesis, we have shown that the right-hand side of (8.8) is congruent to 0 modulo p^{k-1}, and so this completes the proof of the lemma. □

Lemma 8.2. (i) *Let p denote an odd prime number and let k be an integer larger than or equal to 2. Then any two adjacent blocks of length $3(p-1)(p+1)p^{k+1}$ are congruent modulo p^{2k-1}, i.e.,*

$$E_{j+6(p-1)(p+1)p^{k+1}}\cdots E_{j+3(p-1)(p+1)p^{k+1}+1}\equiv E_{j+3(p-1)(p+1)p^{k+1}}\cdots E_{j+1}\,(\mathrm{mod}\,p^{2k-1}), \tag{8.9}$$

for all integers j.
(ii) *Let $p\in\mathcal{B}$. Then for any integers j and $k\geq 2$,*

$$E_{j+12p^k}\cdots E_{j+6p^k+1}\equiv E_{j+6p^k}\cdots E_{j+1}\,(\mathrm{mod}\,p^{2k-1}). \tag{8.10}$$

Proof. We prove only (ii), which is used in the sequel; the proof of (i) is similar. Fix $p\in\mathcal{B}$ and integers j and $k\geq 1$. By (4) of Proposition 7.2, both sides of (8.10) are congruent to I modulo p^k. We need to prove a stronger congruence by increasing this exponent k by $k-1$. For each $\ell\in\{j+1,\dots,j+6p^k\}$, define X_ℓ by $E_{\ell+6p^k}=E_\ell+X_\ell$. Thus, by (5.7),

$$X_\ell=\begin{cases}\begin{pmatrix}4p^k & 0\\ 0 & 0\end{pmatrix}, & \text{if } 3\mid\ell,\\ \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}, & \text{if } 3\nmid\ell.\end{cases} \tag{8.11}$$

The left side of (8.10) equals

$$(E_{j+6p^k}+X_{j+6p^k})\cdots(E_{j+1}+X_{j+1}),$$

which we expand as a sum of 2^{6p^k} terms, each being a product of $6p^k$ factors of the form E_ℓ or X_ℓ. The term that does not contain an X_j coincides with the product on the right side of (8.10). Notice also that each term that contains two or more X_ℓ's is congruent to zero modulo p^{2k}. Therefore the difference modulo p^{2k} of the two sides of (8.10) can be written as a sum of terms, each containing exactly one X_ℓ. Also, those X_ℓ with $3\nmid\ell$ are zero and can be omitted. In conclusion,

$$E_{j+12p^k}\cdots E_{j+6p^k+1}-E_{j+6p^k}\cdots E_{j+1}\equiv\sum_{\ell=j+1}^{j+6p^k}B_\ell\,(\mathrm{mod}\,p^{2k}), \tag{8.12}$$

where for each $\ell\in\{j+1,\dots,j+6p^k\}$ with $3\mid\ell$, we have denoted

$$\begin{aligned}B_\ell&=E_{j+6p^k}\cdots E_{\ell+1}X_\ell E_{\ell-1}\cdots E_{j+1}\\ &=4p^kE_{j+6p^k}\cdots E_{\ell+1}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}E_{\ell-1}\cdots E_{j+1}=4p^kM_{p,k,j,\ell}.\end{aligned} \tag{8.13}$$

Using now Lemma 8.1 in conjunction with (8.12) and (8.13), we conclude the proof of the congruence (8.10). □

Let us remark that by applying Lemma 8.1 repeatedly, (8.9) and (8.10), we can obtain the generalizations

$$E_{j+3d(p-1)(p+1)p^{k+1}}\cdots E_{j+3(d-1)(p-1)(p+1)p^{k+1}+1}\equiv E_{j+3(p-1)(p+1)p^{k+1}}\cdots E_{j+1}\,(\mathrm{mod}\,p^{2k-1}), \tag{8.14}$$

for all odd primes p and all integers j, $k \geq 1$, and $d \geq 1$, and, respectively,

$$E_{j+6dp^k} \cdots E_{j+6(d-1)p^k+1} \equiv E_{j+6p^k} \cdots E_{j+1} \pmod{p^{2k-1}}, \tag{8.15}$$

for all primes p that are in $\mathcal{B}$ and all integers j, $k \geq 1$, and $d \geq 1$.

As a consequence of the foregoing relations and the existence of the three zeros $q_{-6} = q_{-2} = q_0 = 0$, we find that the denominators q_m of the continued fraction of e satisfy the following supercongruences.

Proposition 8.3. *For any prime number p that belongs to $\mathcal{B}$, any positive integer k, and any integer ℓ,*

(1) $q_{6p^k\ell} \equiv \ell q_{6p^k} \pmod{p^{2k-1}}$,
(2) $q_{-2+6p^k\ell} \equiv \ell q_{-2+6p^k} \pmod{p^{2k-1}}$,
(3) $q_{-6+6p^k\ell} \equiv \ell q_{-6+6p^k} \pmod{p^{2k-1}}$.

Proof. We prove only (3). By (2) of Proposition 7.2 and the fact that $q_{-6} = 0$, it follows that both sides of (3) are divisible by p^k, and, as functions of ℓ, both are periodic modulo p^{2k-1} with period p^{k-1}. So, we may restrict ourselves to the case when $\ell \in \{1, 2, \ldots, p^{k-1}\}$.

By (6.7), with $j = -5$ and $L = 6p^k$ and, respectively, $L = 6p^k\ell$,

$$\begin{pmatrix} q_{6p^k-5} \\ q_{6p^k-6} \end{pmatrix} = E_{6p^k-5} \cdots E_{-4} \begin{pmatrix} q_{-5} \\ q_{-6} \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} q_{6p^k\ell-5} \\ q_{6p^k\ell-6} \end{pmatrix} = E_{6p^k\ell-5} \cdots E_{-4} \begin{pmatrix} q_{-5} \\ q_{-6} \end{pmatrix}. \tag{8.16}$$

Here, $q_{-5} = -1$ and $q_{-6} = 0$. Hence, the two blocks from (8.16) have the forms

$$E_{6p^k-5} \cdots E_{-4} = \begin{pmatrix} -q_{6p^k-5} & * \\ -q_{6p^k-6} & * \end{pmatrix} \quad \text{and} \quad E_{6p^k\ell-5} \cdots E_{-4} = \begin{pmatrix} -q_{6p^k\ell-5} & * \\ -q_{6p^k\ell-6} & * \end{pmatrix}. \tag{8.17}$$

The product $E_{6p^k\ell-5} \cdots E_{-4}$ can be subdivided into a product of ℓ blocks of the form

$$E_{6p^kd-5} \cdots E_{6p^k(d-1)-4}, \qquad d \in \{1, 2, \ldots, \ell\}.$$

By (8.15), with $j = -5$,

$$E_{6p^kd-5} \cdots E_{6p^k(d-1)-4} \equiv E_{6p^k-5} \cdots E_{-4} \pmod{p^{2k-1}}.$$

Therefore,

$$\left(E_{6p^k-5} \cdots E_{-4}\right)^\ell \equiv E_{6p^k\ell-5} \cdots E_{-4} \equiv \begin{pmatrix} -q_{6p^k\ell-5} & * \\ -q_{6p^k\ell-6} & * \end{pmatrix} \pmod{p^{2k-1}}. \tag{8.18}$$

On the other hand, combining the first equality in (8.17) with (4) of Proposition 7.2 for $j = -5$ and $L = 6p^k$, we may write $E_{6p^k-5} \cdots E_{-4}$ in the form

$$E_{6p^k-5} \cdots E_{-4} = I + X, \quad \text{with } X = \begin{pmatrix} * & * \\ -q_{6p^k-6} & * \end{pmatrix}, \quad X \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \pmod{p^k}. \tag{8.19}$$

Then,

$$\left(E_{6p^k-5} \cdots E_{-4}\right)^\ell = (I + X)^\ell \equiv I + \ell X \equiv \begin{pmatrix} * & * \\ -\ell q_{6p^k-6} & * \end{pmatrix} \pmod{p^{2k}}. \tag{8.20}$$

Comparing (8.18) and (8.20), we see that (3) follows. The congruences (1) and (2) can be similarly proved. □

9. Further Special Primes

The three zeros of the sequence $\{q_\ell\}$, $\ell \in \mathbb{Z}$, located, as we have previously seen, at $\ell = 0$, $\ell = -2$, and $\ell = -6$, together with Lemma 7.1 and Proposition 7.2 show that for m running over certain sequences, $v_p(q_m)$ grows at least as fast as the p-adic valuation of the distance from m to $0, -2$, or -6. We now proceed to define three sets of prime numbers p for which $v_p(q_m)$ does not grow much faster than what the obstructions above force them to grow. To be precise, let $s \geq 0$ be an integer, and let p be a prime. We denote by $\mathcal{B}_{-1,s}$ those primes p in $\mathcal{B}$ such that

$$v_p(q_m) \leq s, \qquad \text{for all integers } m \text{ with } m \equiv -1 \,(\mathrm{mod}\, 3). \tag{9.1}$$

We denote by $\mathcal{B}_{1,s}$ those primes p in $\mathcal{B}$ such that

$$v_p(q_m) \leq s + v_p(2+m), \qquad \text{for all integers } m \text{ with } m \equiv 1 \,(\mathrm{mod}\, 3). \tag{9.2}$$

We denote by $\mathcal{B}_{0,s}$ those primes p belonging to $\mathcal{B}$ and satisfying the condition

$$v_p(q_m) \leq s + \max\{v_p(m), v_p(6+m)\}, \qquad \text{for all integers } m \text{ with } m \equiv 0 \,(\mathrm{mod}\, 3). \tag{9.3}$$

Let us denote

$$\mathcal{B}_{-1} = \bigcup_{s \geq 0} \mathcal{B}_{-1,s},$$
$$\mathcal{B}_{1} = \bigcup_{s \geq 0} \mathcal{B}_{1,s},$$
$$\mathcal{B}_{0} = \bigcup_{s \geq 0} \mathcal{B}_{0,s}.$$

The importance of the sets $\mathcal{B}_{-1}$, $\mathcal{B}_{-1}$, and $\mathcal{B}_0$ in connection with Sondow's Conjecture is seen in the following lemma.

Lemma 9.1. *Let s_1, s_2, and s_3 denote nonnegative integers and let p_1, p_2, and p_3 denote not necessarily distinct primes in $\mathcal{A}$ (in the sense of Section 5), such that $p_1 \in \mathcal{B}_{-1,s_1}$, $p_2 \in \mathcal{B}_{1,s_2}$, and $p_3 \in \mathcal{B}_{0,s_3}$. Then there exists an effectively computable constant C, depending only on s_1, s_2, s_3, p_1, p_2, and p_3, such that any possible counterexample*

$$\frac{A_n}{n!} = \frac{p_m}{q_m}$$

to Sondow's Conjecture has $m \leq C$.

In other words, if we find an explicit *good* prime in $\mathcal{A}$ in each of the three cases, then Sondow's Conjecture has only finitely many counterexamples, which can be found numerically.

Proof. Let s_1, s_2, s_3, p_1, p_2, and p_3 be as in the statement of the lemma. Let m be any positive integer satisfying

$$m \geq \max\left\{\frac{3}{2}p_1(s_1+1), \frac{3}{2}p_2\left(s_2 + 1 + \frac{\log(2+m)}{\log p_2}\right), \frac{3}{2}p_3\left(s_3 + 1 + \frac{\log(6+m)}{\log p_3}\right)\right\}. \tag{9.4}$$

We claim that no such m gives rise to a counterexample to Sondow's Conjecture.

Indeed, suppose that m satisfies (9.4) and that

$$\frac{p_m}{q_m} = \frac{A_n}{n!}$$

for some nonnegative integer n. Then (5.12) holds for any prime $p \in \mathcal{A}$, and in particular, it holds for p_1, p_2, and p_3. Assume now that $m \equiv 0 \pmod 3$. We then use (5.12) in combination with (9.4) to derive that

$$v_{p_3}(q_m) \geq \sum_{\ell=1}^{\infty} \left\lfloor \frac{\left\lfloor \frac{m}{3} \right\rfloor + \left\lfloor \frac{m+1}{3} \right\rfloor}{p_3^{\ell}} \right\rfloor \geq \left\lfloor \frac{2m}{3p_3} \right\rfloor > s_3 + \frac{\log(6+m)}{\log p_3}. \tag{9.5}$$

On the other hand, $v_{p_3}(m)$ and $v_{p_3}(6+m)$ are both bounded by $\log(6+m)/\log p_3$, and so (9.3) implies that

$$v_{p_3}(q_m) \leq s_3 + \frac{\log(6+m)}{\log p_3}, \tag{9.6}$$

which contradicts (9.5). The cases $m \equiv 1 \pmod 3$ and $m \equiv -1 \pmod 3$ can be examined along the same lines, and this completes the proof of the lemma. □

Given a prime p and an integer $s \geq 0$, we conclude that a finite amount of computation is sufficient in order to check if $p \in \mathcal{B}_{-1,s}$ or if it is not. More precisely, since by Lemma 7.1, $\{q_m\}$ forms a periodic sequence modulo p^{s+1} with period dividing $3(p-1)(p+1)p^{s+2}$, it follows that $p \in \mathcal{B}_{-1,s}$ if and only if

$$v_p(q_m) \leq s, \qquad \text{for all } m \equiv -1 \pmod 3, \quad 1 \leq m \leq 3(p-1)(p+1)p^{s+2}. \tag{9.7}$$

Moreover, using also the symmetry (6.3), we see that $p \in \mathcal{B}_{-1,s}$ if and only if

$$v_p(q_{3\ell-1}) \leq s, \qquad \text{for } 1 \leq \ell \leq p^{s+1}. \tag{9.8}$$

Table 2 below provides a list of primes p that are good in Case $-1 \pmod 3$, and for each p it displays the smallest nonnegative integer s for which $p \in \mathcal{B}_{-1,s}$. An empty entry indicates that we we did not find any such s. Not all known minimal values of s are equal to zero; for example, when $p = 79$, the minimal value of s is 1.

Next, we consider the Case $1 \pmod 3$. Here we employ the supercongruences from Section 8 in order to show that if given a prime $p \in \mathcal{B}$ and an integer $s \geq 0$, a finite amount of computation is sufficient to establish whether or not $p \in \mathcal{B}_{1,s}$. To proceed, let us fix a prime p that belongs to $\mathcal{B}$. Let us first remark that if $p > 3$, then

$$v_p(q_m) \geq v_p(2+m), \qquad \text{for all } m \in \mathbb{Z}, m \equiv 1 \pmod 3. \tag{9.9}$$

This is clear for even m, because in this case $2+m$ is a multiple of 6, and so $2+m = 6p^k d$ with $k = v_p(m+2)$ and $d \in \mathbb{Z}$, and by (2) of Proposition 7.2,

$$q_m \equiv q_{m-6p^k d} \equiv q_{-2} \equiv 0 \pmod{p^k}. \tag{9.10}$$

If m is odd, then we write $2+m = 3p^k d$ with $k = v_p(2+m)$ and $d \in \mathbb{Z}$, and use (2) of Proposition 7.2 in conjunction with the symmetry (6.2) to deduce that

$$q_m \equiv q_{m-6p^k d} \equiv q_{-4-m} \equiv -q_m \pmod{p^k}, \tag{9.11}$$

which again implies that $q_m \equiv 0 \pmod{p^k}$. In the case that $p = 3$, the same reasoning leads to a slightly weaker version of (9.9), namely,

$$v_3(q_m) \geq v_3(2+m) - 1. \tag{9.12}$$

Given a prime p that is in $\mathcal{B}$ and nonnegative integers s and k, we say that $p \in \mathcal{B}_{1,s}$ at level k, provided that

$$v_p(q_m) \leq s + k, \qquad \text{for all } m \in \mathbb{Z}, \text{with } m \equiv 1 \pmod 3 \text{ and } v_p(2+m) = k. \tag{9.13}$$

Thus, $p \in \mathcal{B}_{1,s}$ if and only if $p \in \mathcal{B}_{1,s}$ at all levels $k \geq 0$. If p, s, and k are each fixed, it is sufficient to check a finite set of data in order to determine whether $p \in \mathcal{B}_{1,s}$ at level k. As with (9.8), $p \in \mathcal{B}_{1,s}$ at level k if and only if

$$v_p(q_{3\ell+1}) \leq s + k, \qquad \text{for all } 1 \leq \ell \leq p^{k+s+1} \text{ with } v_p(3\ell+3) = k. \tag{9.14}$$

We now show that it is sufficient to check (9.14) for finitely many k in order to conclude that it holds for all k.

Lemma 9.2. *Let $s \geq 0$, and let p be a prime that is in $\mathcal{B}_{1,s}$ at levels $k = 0, 1, \ldots, s+3$. Then $p \in \mathcal{B}_{1,s}$ at all levels $k \geq 0$, i.e., $p \in \mathcal{B}_{1,s}$.*

Proof. Let s and p be as in the statement of the lemma. We prove that $p \in \mathcal{B}_{1,s}$ at all levels k. We proceed by induction on k, with the cases $k = 0, 1, \ldots, s+3$ satisfied by hypothesis. Let $k \geq s+4$ and assume that $p \in \mathcal{B}_{1,s}$ at level $k-1$. Let m be an arbitrary integer such that $m \equiv 1 \pmod 3$ and $v_p(2+m) = k$.

Assume first that m is even. Then the number $\ell = \frac{1}{6}(m+2)p^{-k+1}$ is an integer. Also, ℓ is divisible by p, but not by p^2, and $m = -2 + 6p^{k-1}\ell$. Applying (2) of Proposition 8.3 with k replaced by $k-1$, we find that

$$q_m \equiv \ell q_{-2+6p^{k-1}} \pmod{p^{2k-3}}. \tag{9.15}$$

By the induction hypothesis, $p \in \mathcal{B}_{1,s}$ at level $k-1$, and so $v_p(q_{-2+6p^{k-1}}) \leq s+k-1$. Thus, the integer $\ell q_{-2+6p^{k-1}}$ is not divisible by p^{s+k+1}. Since $k \geq s+4$, the two sides of (9.15) will also be congruent modulo p^{s+k+1}. It follows that q_m is not divisible by p^{s+k+1}, as desired.

Assume now that m is odd. In this case we modify the argument above and that of (2) of Proposition 8.3 as follows. We need to show that q_m is not divisible by p^{k+s+1}. Suppose that q_m is divisible by p^{k+s+1}. By the symmetry in (6.2), q_{-4-m} is also divisible by p^{k+s+1}. Without loss of generality, we may therefore restrict our attention to the case $m > 0$ in the sequel. The usual block upon which we focus, namely, the one connecting q_{-2} with q_m, is not convenient to us, because its length, although divisible by $3p^k$, is not divisible by $6p^k$. Therefore, we employ a block of twice its length, which connects q_{-4-m} with q_m. We can then conveniently subdivide this block into a product of congruent blocks of length $6p^{k-1}$ each. None of them begins or ends at the center q_{-2}, but the middle block, the one that contains the center, has an extra symmetry (with respect to the center), which we exploit as follows to finish the proof. By (6.7), with $j = -3-m$ and $L = 2m+4$,

$$\begin{pmatrix} q_{m+1} \\ q_m \end{pmatrix} = E_{m+1}E_m \cdots E_{-2-m} \begin{pmatrix} q_{-3-m} \\ q_{-4-m} \end{pmatrix}. \tag{9.16}$$

Since, as shown above, $q_m \equiv 0 \pmod{p^{k+s+1}}$, we have $q_{-4-m} \equiv 0 \pmod{p^{k+s+1}}$. Furthermore, since q_{-3-m} is relatively prime to q_{-4-m}, then $p \nmid q_{-3-m}$. It follows from (9.16) that

$$E_{m+1}E_m \cdots E_{-2-m} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{p^{k+s+1}}. \tag{9.17}$$

We now subdivide the block on the left-hand side of (9.17) into a product of ℓ consecutive blocks of length $6p^{k-1}$ each, where $\ell = \frac{1}{3}(m+2)p^{-k+1}$. As before, ℓ is a multiple of p but not a multiple of p^2. We know from (8.15), with $j = -3-m$, $d = 1, 2, \ldots, \ell$, and k replaced by $k-1$, that all of these blocks are congruent to each other modulo p^{2k-3}. Here the middle block is given by

$$E_{3p^{k-1}-1}E_{3p^{k-1}-2} \cdots E_{-3p^{k-1}}.$$

Therefore,

$$\left(E_{3p^{k-1}-1}E_{3p^{k-1}-2} \cdots E_{-3p^{k-1}}\right)^{\ell} \equiv E_{m+1}E_m \cdots E_{-2-m} \pmod{p^{2k-3}}. \tag{9.18}$$

As before, $2k-3 \geq k+s+1$, and so by (9.17) and (9.18),

$$\left(E_{3p^{k-1}-1}E_{3p^{k-1}-2} \cdots E_{-3p^{k-1}}\right)^{\ell} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{p^{k+s+1}}. \tag{9.19}$$

By (4) of Proposition 7.2, with $j = -3p^{k-1} - 1$ and $L = 6p^{k-1}$, we may write

$$E_{3p^{k-1}-1}E_{3p^{k-1}-2} \cdots E_{-3p^{k-1}} = \begin{pmatrix} 1+p^{k-1}x & p^{k-1}y \\ p^{k-1}z & 1+p^{k-1}t \end{pmatrix}, \tag{9.20}$$

for certain integers x, y, z, t.

Firstly, by (9.20) and the binomial theorem,

$$\left(E_{3p^{k-1}-1}E_{3p^{k-1}-2} \cdots E_{-3p^{k-1}}\right)^{\ell} \equiv I + \ell p^{k-1} \begin{pmatrix} x & y \\ z & t \end{pmatrix} \pmod{p^{2k-2}}, \tag{9.21}$$

which, in conjunction with (9.19), yields

$$\ell p^{k-1} z \equiv 0 \pmod{p^{k+s+1}} \qquad \text{and} \qquad p^{k-1}z \equiv 0 \pmod{p^{k+s}}. \tag{9.22}$$

Secondly, by (6.7), with $j = -3p^{k-1} - 1$ and $L = 6p^{k-1}$, in combination with (9.20) and the symmetry $q_{-2+3p^{k-1}} = -q_{-2-3p^{k-1}}$, it follows that

$$\begin{pmatrix} q_{-1+3p^{k-1}} \\ q_{-2+3p^{k-1}} \end{pmatrix} = \begin{pmatrix} 1+p^{k-1}x & p^{k-1}y \\ p^{k-1}z & 1+p^{k-1}t \end{pmatrix} \begin{pmatrix} q_{-1-3p^{k-1}} \\ -q_{-2+3p^{k-1}} \end{pmatrix}. \tag{9.23}$$

As a consequence of (9.22) and (9.23),

$$q_{-2+3p^{k-1}} \equiv -(1+p^{k-1}t)q_{-2+3p^{k-1}} \pmod{p^{k+s}}. \tag{9.24}$$

By (9.9) and the definition of m, $q_{-2+3p^{k-1}}$ is a multiple of p^{k-1}, and so $p^{k-1}tq_{-2+3p^{k-1}} \equiv 0 \pmod{p^{2k-2}}$. By (9.24) and the fact that $k \geq s+4$, we conclude that

$$q_{-2+3p^{k-1}} \equiv 0 \pmod{p^{k+s}}.$$

This contradicts the induction hypothesis that $p \in \mathcal{B}_{1,s}$ at level $k-1$, and completes the proof of Lemma 9.2. $\square$

By Lemma 9.2 and (9.14), it follows that a prime $p > 3$ that belongs to $\mathcal{B}$ also belongs to $\mathcal{B}_{1,s}$ if and only if

$$v_p(q_{3\ell+1}) \le s + v_p(3\ell+3), \qquad \text{for } 1 \le \ell \le p^{2s+4}. \tag{9.25}$$

Lastly, we consider the Case $0 \pmod 3$, and here we say that a prime $p \in \mathcal{B}_{0,s}$ at level k provided that

$$v_p(q_m) \le s + k \ \text{ for all } m \in \mathbb{Z} \text{ with } m \equiv 0 \pmod 3 \text{ and } \max\{v_p(m), v_p(6+m)\} = k. \tag{9.26}$$

We follow the procedure from Case $1 \pmod 3$ and emphasize below only those aspects of the proof that are different from those in Case $0 \pmod 3$. In the following, we restrict ourselves to primes $p > 3$.

First, by the periodicity from Proposition 7.2 and the symmetry (6.1), a prime $p \in \mathcal{B}$ is in $\mathcal{B}_{0,s}$ at level k if and only if

$$v_p(q_{3\ell}) \le s + k, \quad \text{for all } 1 \le \ell \le p^{k+s+1} \ \text{ with } \ \max\{v_p(\ell), v_p(\ell+2)\} = k. \tag{9.27}$$

Next, the analogue of (9.9) also holds in this case, namely,

$$v_p(q_m) \ge \max\{v_p(m), v_p(6+m)\}, \ \text{for all } m \in \mathbb{Z} \text{ with } \ m \equiv 0 \pmod 3. \tag{9.28}$$

This is clear in the case that m is even by the same reasoning that gave (9.10). The argument, however, breaks down for m odd, because of the lack of a minus sign in the symmetry (6.1). In particular, in this case, the analogue of (9.11) will have the far right side identical to the far left side, which prevents us from extracting any information from it. We can nonetheless elicit information directly from (9.9). Take any $m \equiv 0 \pmod 3$, and let $k := \max\{v_p(m), v_p(6+m)\}$. We need to show that $v_p(q_m) \ge k$. We may assume that $k \ge 1$. Then, since $p \ne 3$, exactly one of $m, 6+m$ is a multiple of p. We distinguish two cases.

Case (I): $m \equiv 0 \pmod{p^k}$. By (9.9), with m replaced by $m-2$, which is congruent to 1 modulo 3, we know that $v_p(q_{m-2}) \ge v_p(m)$, and so $q_{m-2} \equiv 0 \pmod{p^k}$. Since $m \equiv 0 \pmod{p^k}$, by (5.7), $h_m = 2m/3$, and so $h_m \equiv 0 \pmod{p^k}$. Hence, from the recurrence (5.6), $q_m = h_m q_{m-1} + q_{m-2}$, we can conclude that $q_m \equiv 0 \pmod{p^k}$, as claimed.

Case (II): $m + 6 \equiv 0 \pmod{p^k}$. By (9.9), with m replaced by $m+4$, $v_p(q_{m+4}) \ge v_p(m+6)$, and so $q_{m+4} \equiv 0 \pmod{p^k}$. By (5.7),

$$h_{m+4} = 1, \qquad h_{m+3} = \frac{2(m+3)}{3}, \qquad h_{m+2} = 1.$$

Hence, the recurrence (5.6), $q_m = h_m q_{m-1} + q_{m-2}$, gives

$$q_{m+4} = q_{m+3} + q_{m+2}, \qquad \text{and so} \qquad q_{m+3} \equiv -q_{m+2} \pmod{p^k}. \tag{9.29}$$

Also, by the aforementioned recurrence,

$$q_{m+3} = \frac{2(m+3)}{3} q_{m+2} + q_{m+1}.$$

Since $m \equiv -6 \pmod{p^k}$, $2(m+3)/3 \equiv -2 \pmod{p^k}$, and so

$$q_{m+3} \equiv -2q_{m+2} + q_{m+1} \pmod{p^k}. \tag{9.30}$$

Hence, by (9.29) and (9.30),

$$q_{m+2} \equiv q_{m+1} \pmod{p^k}. \tag{9.31}$$

But, $h_{m+2} = 1$, and so $q_{m+2} = q_{m+1} + q_m$. From (9.31), it follows that $q_m \equiv 0 \pmod{p^k}$, which completes the proof of (9.28).

We now prove an analogue of Lemma 9.2.

Lemma 9.3. *Let $s \geq 0$ and let $p > 3$ be a prime that is in $\mathcal{B}_{0,s}$ at levels $0, 1, \ldots, s+3$. Then $p \in \mathcal{B}_{0,s}$.*

Proof. As before, we proceed by induction on k. Let $k \geq s+4$ and assume that $p \in \mathcal{B}_{0,s}$ at level $k-1$. Let m denote the smallest positive integer for which $m \equiv 0 \pmod 3$, $\max\{v_p(m), v_p(6+m)\} = k$, and $v_p(q_m) \geq k+s+1$. To make a choice, say $v_p(6+m) = k$. The proof is similar in the case when $v_p(m) = k$. If m is even, let $\ell = \frac{1}{6}(6+m)p^{-k+1}$. Thus, $m = -6 + 6\ell p^{k-1}$ and ℓ is divisible by p, but not by p^2. Applying (3) of Proposition 8.3, we obtain an analogue of (9.15), namely,

$$q_m \equiv \ell q_{-6+6p^{k-1}} \pmod{p^{2k-3}}. \tag{9.32}$$

Using the induction hypothesis and (2) of Proposition 7.2, we see that $|\ell| q_{-6+6p^{k-1}}$ is not divisible by p^{s+k+1}, and since $2k-3 \geq s+k+1$, it follows from (9.32) that q_m is not divisible by p^{s+k+1}, which contradicts our assumptions on m.

Let us now assume that m is odd. As was the case with (9.28), a new idea is needed, because the argument for odd m from the proof of Lemma 9.2 collapses. We proceed as follows. First, note that $m+6 < 3p^{k+s+1}$. Indeed, by (2) of Proposition 7.2, with k replaced by $k+s+1$,

$$q_{m-6p^{k+s+1}} \equiv q_m \equiv 0 \pmod{p^{k+s+1}}.$$

Also, by the previous congruence and our assumptions on v_p, we find that $v_p(m+6-6p^{k+s+1}) = k$. So, if $m+6-6p^{k+s+1}$ were positive, then it would satisfy the definition of m, contradicting the minimality of m. Thus, $m+6 < 6p^{k+s+1}$, and since $m+6$ is divisible by $3p^k$ but not by $3p^{k+1}$, the largest possible value of $m+6$ is $6p^{k+s+1} - 3p^k$. If now $m+6 \geq 3p^{k+s+1}$, then, similarly to that above, we must have $m+6 \geq 3p^{k+s+1} + 6p^k$. Thus,

$$m \in [3p^{k+s+1} + 6p^k - 6, 6p^{k+s+1} - 3p^k - 6].$$

Then, if we use the symmetry (6.1) to replace m by $-6-m$ followed by adding $6p^{k+s+1}$, we see that $-6-m+6p^{k+s+1}$ is positive, satisfies the conditions from the definition of m, and is smaller than m. Therefore our assumption that $m+6 \geq 3p^{k+s+1}$ is erroneous, and we conclude that $m+6 < 3p^{k+s+1}$, and therefore also that $m+6 \leq 3p^{k+s+1} - 6p^k$.

We now focus on the block that connects q_m to $q_{-6+3p^{k+s+1}}$. Applying (9.28) with m replaced by $-6+3p^{k+s+1}$ and recalling that $q_{-6} = 0$, we know that

$$q_{-6+3p^{k+s+1}} \equiv 0 \pmod{p^{k+s+1}}. \tag{9.33}$$

Consider the block

$$B := E_{-5+3p^{k+s+1}} \cdots E_{m+2}.$$

Then, by (6.7), with $j = m+1$ and $L = -6+3p^{k+s+1} - m$,

$$\begin{pmatrix} q_{-5+3p^{k+s+1}} \\ q_{-6+3p^{k+s+1}} \end{pmatrix} = B \begin{pmatrix} q_{m+1} \\ q_m \end{pmatrix}. \tag{9.34}$$

If we reduce the equality (9.34) modulo p^{k+s+1}, both $q_{-6+3p^{k+s+1}}$ and q_m vanish, by (9.33) and the assumption on m, while the residue class of q_{m+1} is invertible. This forces the image of B to be upper triangular, i.e.,

$$B \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{p^{k+s+1}}. \tag{9.35}$$

We now take advantage of the fact that the length of the block B, which equals $3p^{k+s+1} - (m+6)$, is a multiple of $6p^k$. We subdivide B into a product of consecutive blocks of length $6p^{k-1}$ each, and denote by A the last one. Thus,

$$A = E_{-5+3p^{k+s+1}} \cdots E_{-4+3p^{k+s+1}-6p^{k-1}}.$$

By (8.15), each of these blocks is congruent to A modulo p^{2k-3}. Hence,

$$B \equiv A^\ell \pmod{p^{2k-3}}, \qquad \text{where} \qquad \ell = \frac{3p^{k+s+1} - (m+6)}{6p^{k-1}}. \tag{9.36}$$

We claim that A is upper triangular modulo p^{k+s}. Indeed, using (4) of Proposition 7.2, we write A in the form

$$A = I + X, \qquad X \equiv \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \pmod{p^{k-1}}.$$

Then, since $2k-3 \geq k+s+1$ and $A^\ell \equiv I + \ell X \pmod{p^{2k-2}}$, by (9.35) and (9.36), it follows that

$$I + \ell X \equiv A^\ell \equiv B \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{p^{k+s+1}}. \tag{9.37}$$

Since $m+6$ is divisible by p^k but not by p^{k+1}, ℓ is divisible by p but not by p^2. Employing this observation in (9.37), we deduce that

$$X \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{p^{k+s}},$$

and therefore A is upper triangular modulo p^{k+s}, as desired. It follows that A^{-1} is also upper triangular modulo p^{k+s}. But, by (6.7),

$$\begin{pmatrix} q_{-5+3p^{k+s+1}} \\ q_{-6+3p^{k+s+1}} \end{pmatrix} = A \begin{pmatrix} q_{-5+3p^{k+s+1}-6p^{k-1}} \\ q_{-6+3p^{k+s+1}-6p^{k-1}} \end{pmatrix} \text{ and } \begin{pmatrix} q_{-5+3p^{k+s+1}-6p^{k-1}} \\ q_{-6+3p^{k+s+1}-6p^{k-1}} \end{pmatrix} = A^{-1} \begin{pmatrix} q_{-5+3p^{k+s+1}} \\ q_{-6+3p^{k+s+1}} \end{pmatrix}. \tag{9.38}$$

Reducing the second equality in (9.38) modulo p^{k+s}, we see that $q_{-6+3p^{k+s+1}}$ is sent to zero. Since A^{-1} is upper triangular,

$$q_{-6+3p^{k+s+1}-6p^{k-1}} \equiv 0 \pmod{p^{k+s}}.$$

This generates a contradiction, since the number $m^* := -6 + 3p^{k+s+1} - 6p^{k-1}$ satisfies the conditions $m^* \equiv 0 \pmod 3$ and $\max\{v_p(m^*), v_p(6+m^*)\} = k-1$. So, by the induction hypothesis, q_{m^*} cannot be divisible by p^{k+s}. This completes the proof of the lemma. □

As a consequence of the results above, we have a criterion for a prime $p \in \mathcal{B}_{0,s}$ similar to that established in Case $1 \pmod 3$: A prime $p \in \mathcal{B}_{0,s}$ if and only if

$$v_p(q_{3\ell}) \leq s + \max\{v_p(3\ell), v_p(3\ell+6)\}, \quad \text{for } 1 \leq \ell \leq p^{2s+4}. \tag{9.39}$$

Inspecting Table 2 below, we see that 3 is in $\mathcal{B}_{0,s}$, 7 is in $\mathcal{B}_{1,s}$, and 7 or 11 is in $\mathcal{B}_{-1,s}$. Therefore Lemma 9.1 gives a concrete level C for the possible counterexamples to Sondow's Conjecture. After checking all the convergents up to that bound, we can conclude the following:

Theorem 9.4. *Sondow's Conjecture is true.*

p	$\mathcal{B}(-1,s)$	$\mathcal{B}(0,s)$	$\mathcal{B}(1,s)$	in $\mathcal{A}$?
3	0	0	0	Y
5	0	0	0	N
7	–	0	0	Y
11	–	0	0	Y
13	–	0	–	N
17	0	0	0	Y
19	0	0	0	N
23	0	0	–	N
29	0	0	0	N
31	–	–	0	N
37	0	–	0	N
41	–	0	–	N
43	0	0	–	N
47	0	0	–	Y

TABLE 2. The Minimal Value of s for primes in $\mathcal{B}(-1,s)$, $\mathcal{B}(0,s)$, $\mathcal{B}(1,s)$

10. FUNCTIONAL EQUATIONS ARISING FROM THE SEQUENCE OF CONVERGENTS TO e

In this section we show that certain p-adic functions, which naturally arise from the sequence of convergents to the continued fraction of e, satisfy simple functional equations. In what follows, we fix a prime number p belonging to $\mathcal{B}$. The discussion below would also apply to a general prime p if we subdivide the integers $\mathbb{Z}$ into arithmetic progressions with modulus $3(p-1)(p+1)p$ instead of arithmetic progressions with modulus 6, as we do in the following passages. For simplicity, and also because, as checked by Sondow and Schalm [15], the primes up to 1000 belong to $\mathcal{B}$, we restrict ourselves, as mentioned above, to primes p in $\mathcal{B}$. Fix such a prime p, let $\mathbb{Q}_p$ denote the field of p-adic numbers, and let $\mathbb{Z}_p$ denote the ring of integers in $\mathbb{Q}_p$. Let $|\cdot|_p$ denote the p-adic absolute value on $\mathbb{Q}_p$, normalized by $|p|_p = 1/p$. For each $r \in \mathbb{Z}$, define a function $f_r : \mathbb{Z} \to \mathbb{Z}$ by

$$f_r(\ell) = q_{6\ell - r}, \qquad \text{for all } \ell \in \mathbb{Z}. \tag{10.1}$$

These functions are continuous with respect to the p-adic absolute value. They, in fact, are 1-*Lipschitzian*, i.e.,

$$|f_r(\ell_2) - f_r(\ell_1)|_p \le |\ell_2 - \ell_1|_p, \tag{10.2}$$

for any integers r, ℓ_1, and ℓ_2. Indeed, write $\ell_2 - \ell_1 = p^k \mu$, for some integer μ with $(\mu, p) = 1$. By (2) of Proposition 7.2, the sequence $\{q_j\}$, $j \in \mathbb{Z}$, is periodic modulo p^k with period $6p^k$. Hence,

$$f_r(\ell_2) - f_r(\ell_1) = q_{6\ell_1 - r + 6p^k \mu} - q_{6\ell_1 - r} \equiv 0 \,(\mathrm{mod}\, p^k),$$

and (10.2) follows. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, it follows from (10.2) that each f_r has a unique extension to a continuous function $f_r : \mathbb{Z}_p \to \mathbb{Z}_p$, which is 1-$Lipschitzian$, i.e.,

$$|f_r(x) - f_r(y)|_p \le |x - y|_p, \tag{10.3}$$

for all $x, y \in \mathbb{Z}_p$. If follows from Mahler's work [7] that each f_r has a representation of the form

$$f_r(x) = a_{r,0} + a_{r,1} x + a_{r,2} \frac{x(x-1)}{2} + \cdots + a_{r,k} \binom{x}{k} + \cdots, \tag{10.4}$$

where the coefficients $a_{r,k}$, which in the present case are integers, are given by

$$\begin{aligned} a_{r,0} &= f_r(0) = q_{-r}, \qquad a_{r,1} = f_r(1) - f_r(0) = q_{-r-6} - q_{-r}, \\ a_{r,2} &= f_r(2) - 2f_r(1) + f_r(0) = q_{-r+12} - 2q_{-r+6} + q_{-r}, \ldots. \end{aligned} \tag{10.5}$$

Furthermore, the series on the right-hand side of (10.4) converges uniformly for $x \in \mathbb{Z}_p$. The functions f_r encode divisibility and congruence properties of the denominators of the convergents to e, and, as such, deserve further investigation.

In the remainder of this section, we record a few basic properties of these functions, which follow from our results in previous sections. First, we note that all the information on divisibility and congruence properties of the denominators q_m modulo powers of p encoded in the functions f_r is already captured in $f_1, f_2, \ldots, f_6$, since all the other f_r's are simple shifts of these. More precisely, by (10.1), $f_r(\ell) = q_{6\ell - r} = f_{r+6}(\ell + 1)$, for all integers r and ℓ. Therefore, by continuity,

$$f_r(x) = f_{r+6}(x+1), \qquad \text{for all } r \in \mathbb{Z} \text{ and } x \in \mathbb{Z}_p. \tag{10.6}$$

We also have relations between any three consecutive functions f_r emanating from the recurrence relation (5.6). Applying (5.6) and (5.7) with $j = 6\ell - r$, we see that

$$f_r(\ell) = q_{6\ell - r} = h_{6\ell - r} q_{6\ell - r - 1} + q_{6\ell - r - 2} = h_{6\ell - r} f_{r+1}(\ell) + f_{r+2}(\ell),$$

where $h_{6\ell - r} = \frac{2}{3}(6\ell - r)$ if $r \equiv 0 \,(\mathrm{mod}\, 3)$ and $h_{6\ell - r} = 1$ otherwise. By continuity, we find that

$$f_r(x) = \begin{cases} \left(4x - \frac{2}{3} r\right) f_{r+1}(x) + f_{r+2}(x), & \text{if } r \equiv 0 \,(\mathrm{mod}\, 3), \\ f_{r+1}(x) + f_{r+2}(x), & \text{otherwise}, \end{cases} \tag{10.7}$$

for all $r \in \mathbb{Z}$ and $x \in \mathbb{Z}_p$. The relations among $f_1, f_2, \ldots, f_6$ provided by (10.6) and (10.7) are then given by

$$\begin{cases} f_1(x) &= f_2(x) + f_3(x), \\ f_2(x) &= f_3(x) + f_4(x), \\ f_3(x) &= (4x-2) f_4(x) + f_5(x), \\ f_4(x) &= f_5(x) + f_6(x), \\ f_5(x) &= f_6(x) + f_1(x-1), \\ f_6(x) &= (4x-4) f_1(x-1) + f_2(x-1), \end{cases} \tag{10.8}$$

for all $x \in \mathbb{Z}_p$.

Lastly, from the symmetries (6.1)–(6.3) and the continuity of f_r, we find that $f_1, f_2, \dots, f_6$ satisfy the functional equations

$$\begin{cases} f_1(x) &= -f_4(-x), \\ f_2(x) &= -f_2(-x), \\ f_3(x) &= f_3(-x), \\ f_5(x) &= -f_5(1-x), \\ f_6(x) &= f_6(1-x), \end{cases} \tag{10.9}$$

for all $x \in \mathbb{Z}_p$.

We collect the results above in the following theorem.

Theorem 10.1. *Let p be a prime belonging to the set $\mathcal{B}$.*

(i) *For each $r \in \mathbb{Z}$, the function $f_r : \mathbb{Z} \to \mathbb{Z}$ defined by* (10.1) *has a unique extension by continuity to a function $f_r : \mathbb{Z}_p \to \mathbb{Z}_p$, which satisfies* (10.3).

(ii) *The functions $f_r : \mathbb{Z}_p \to \mathbb{Z}_p$, $r \in \mathbb{Z}$, are related to each other by the equalities* (10.6) *and* (10.7). *In particular, the functions $f_1, f_2, \dots, f_6$ are related by* (10.8).

(iii) *The functions $f_r : \mathbb{Z}_p \to \mathbb{Z}_p$, $r = 1, 2, \dots, 6$, satisfy the functional equations* (10.9).

It would be interesting to study further properties of the functions f_r, and then possibly to apply these findings to deduce new divisibility and congruence properties of the convergents to the continued fraction of e. A natural question arising from Theorem 10.1 is whether any of these functions are differentiable. In this connection, we remark that differentiability of $f_r(x)$ at $x = 0$ is equivalent, by a theorem of Mahler [7], to

$$\lim_{n\to\infty} \frac{a_{r,n}}{n} = 0$$

in $\mathbb{Q}_p$, a condition that can be reinterpreted via (10.5) in terms of congruence properties of certain linear combinations of the denominators q_m. A further natural question is whether the functions f_r are restrictions to $\mathbb{Z}_p$ of certain $p-$adic rigid analytic functions defined on some appropriate domains in $\mathbb{C}_p$ (the completion of the algebraic closure of $\mathbb{Q}_p$ with respect to the $p-$adic absolute value). Another question arising naturally from Theorem 10.1 concerns the zeros of the these functions in $\mathbb{Z}_p$. We already know that some of these functions have "trivial" zeros. For example, since $q_{-2} = q_{-6} = q_0 = 0$, we know that $f_2(0) = 0$ and that $f_6(0) = f_6(1) = 0$. Also, the functional equation of f_5 in (10.9) shows that f_5 has a trivial zero at $x = \frac{1}{2}$, which for odd p belongs to $\mathbb{Z}_p$. Next, for any positive integer k,

$$f_3\left(\frac{p^k-1}{2}\right) = q_{3p^k-6} \qquad \text{and} \qquad f_3\left(\frac{p^k+1}{2}\right) = q_{3p^k},$$

and both q_{3p^k-6} and q_{3p^k} are divisible by p^k, by (9.28). Letting $k \to \infty$ and using the continuity of f_3, we conclude that

$$f_3\left(-\frac{1}{2}\right) = f_3\left(\frac{1}{2}\right) = 0.$$

Note that these two zeros of f_3, which we also consider to be "trivial" zeros, do not follow directly from the functional equation of f_3, and this explains why in order to prove (9.28),

we needed to find a new approach, which did not use the symmetry (6.1). Do any of the functions f_r have any "nontrivial" zeros?

Acknowledgments

The authors are grateful to M.Tip Phaovibul for computing all of our tables and to Mike Bennett for informing them of [5]. The authors owe an enormous thanks to the referees for an exceptionally careful reading of their manuscript and for numerous very useful comments and suggestions.

REFERENCES

[1] A. A. Krisnaswami Aiyangar, *Partial solution to Question* 784, J. Indian Math. Soc. **18** (1929–30), 214–217.
[2] B. C. Berndt, *Ramanujan's Notebooks*, Part II, Springer-Verlag, New York, 1989.
[3] B. C. Berndt, S. Kim, and A. Zaharescu, *Dirichlet L-functions, elliptic curves, hypergeometric functions, and rational approximation with partial sums of power series*, Math. Res. Letters, to appear.
[4] P. Bundschuh, *Irrationalitätsmasze für* e^a, $a \neq 0$ *rational oder Liouville-Zahl*, Math. Ann. **192** (1971), 229–242.
[5] C. S. Davis, *Rational approximation to* e, J. Austral. Math. Soc. **25** (1978), 497–502.
[6] L. Lorentzen and H. Waadeland, *Continued Fractions with Applications*, North Holland, Amsterdam, 1992.
[7] K. Mahler, *An interpolation series for continuous functions of a* p*-adic variable*, J. Reine Angew. Math. **199** (1958), 23-34.
[8] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, fifth ed., Wiley, New York, 1991.
[9] S. Ramanujan, *Question* 784, J. Indian Math. Soc. **8** (1916), 159.
[10] S. Ramanujan, *Collected Papers*, Cambridge University Press, Cambridge, 1927; reprinted by Chelsea, New York, 1962; reprinted by the American Mathematical Society, Providence, RI, 2000.
[11] S. Ramanujan, *Notebooks* (2 volumes), Tata Institute of Fundamental Research, Bombay, 1957.
[12] S. Ramanujan, *The Lost Notebook and Other Unpublished Papers*, Narosa, New Delhi, 1988.
[13] N. J. A. Sloane, *On-line Encylopedia of Integer Sequences*, http://oeis.org/.
[14] J. Sondow, *A geometric proof that* e *is irrational and a new measure of its irrationality*, Amer. Math. Monthly **113** (2006), 637–641.
[15] J. Sondow and K. Schalm, *Which partial sums of the Taylor series for* e *are convergents to* e*?* (*and a link to the primes* 2, 5 13, 37, 463). Part II. in *Gems in Experimental Mathematics*, T. Amdeberhan, L.A. Medina, V.H. Moll, eds., Contemp. Math., vol. 517, American Mathematical Society, Providence, RI, 2010, pp. 349-363.
[16] T. Vijayraghavan and G. N. Watson, *Solution to Question* 784, J. Indian Math. Soc. **19** (1931), 12–23.
[17] H. S. Wall, *Analytic Theory of Continued Fractions*, Van Nostrand, New York, 1948; reprinted by Chelsea, New York, 1967; reprinted by the American Mathematical Society, Providence, RI, 2000.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS, 1409 WEST GREEN STREET, URBANA, IL 61801, USA
E-mail address: berndt@illinois.edu

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, 231 WEST 18TH AVENUE, COLUMBUS, OH 43210, USA
E-mail address: kim.1674@math.ohio-state.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS, 1409 WEST GREEN STREET, URBANA, IL 61801, USA, AND INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY, P.O. BOX 1-764, BUCHAREST RO-70700, ROMANIA
E-mail address: zaharesc@illinois.edu