On the Diophantine Equation

\((-1)^{(n-1)/2} \left( \frac{n-1}{2} \right)! \right)^2 + a^{n-1} = n^k\)

By

Fong Shun Chen, BSc. Mathematics
The Hong Kong University of Science & Technology

A Thesis Presented to
The Hong Kong University of Science & Technology
in Partial Fulfillment
of the Requirements for
the Degree of Master of Philosophy
in Mathematics

Hong Kong, July 1997

Copyright © by Fong Shun Chen 1997
Authorization

I hereby declare that I am the sole author of the thesis.

I authorize the Hong Kong University of Science and Technology to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I further authorize the Hong Kong University of Science and Technology to reproduce the thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.
On the Diophantine Equation

\((-1)^{(n-1)/2}\left(\left(\frac{n-1}{2}\right)!ight)^2 + a^{n-1} = n^k\)

By

Fong Shun Chen, BSc. Mathematics
The Hong Kong University of Science & Technology

Approved:

Prof. Kunrui Yu, Supervisor

Prof. Shiu Yuen Cheng, Head of Department

Department of Mathematics

July 1997
Acknowledgments

I am greatly indebted to my supervisor Professor Kunrui Yu, who led me to the field of the current work, directed the research throughout my M.Phil. study. His own research and perspective on related topics have had a great deal of influence on me. I would like to express my deep thank to him for his constant support and encouragement.

Also, I want to thank Dr. Jimmy C.H. Fung and Dr. Yik Man Chiang, for their help during my M.Phil. study. I also want to thank the Department of Mathematics for providing me the opportunity of studying here, and my classmates in HKUST for making my stay here so enjoyable.
Contents

Title page i
Authorization page ii
Signature page iii
Acknowledgments iv
Table of contents v
Abstract vi

1 Introduction 1

2 An elementary proof of Theorem 1.1 3

3 A second proof of Lemma 2.10 9
   3.1 Nonexistence of solutions with large $p$ 10
   3.2 Computer treatment 13

References 16
Abstract

We prove that the equation \((-1)^{(n-1)/2} \left( \frac{(n-1)!}{2} \right)^2 + a^{n-1} = n^k\) in positive integers \(n, a, k\) with \(n > 2\) and odd has only two solutions: \((n, a, k) = (3, 2, 1), (5, 1, 1)\).
1 Introduction

The famous Wilson's theorem states that \((p - 1)! + 1 \equiv 0 \pmod{p}\) for any prime \(p\). The theorem was first proved by Lagrange in 1771. In 1856, Liouville [4] proved that
\[
(p - 1)! + 1 = p^k
\]
in \(p, k \in \mathbb{Z}_{>0}\) with \(p > 2\) and prime has only two solutions: \((p, k) = (3, 1), (5, 2)\).

The more general diophantine equation
\[
(p - 1)! + a^{p-1} = p^k
\]
in \(p, a, k \in \mathbb{Z}_{>0}\) with \(p > 2\) and prime had been considered in the book of Erdős and Graham [2]. In 1991, Brindza and Erdős [1] noted that equation (1) has no solutions in \(p, a, k \in \mathbb{Z}_{>0}\) with \(p\) composite, and proved, based on deep results on linear forms in logarithms, i.e., Philippon and Waldschmidt [7] and Yu [8], that there exists an effectively computable absolute constant \(C\) such that all solutions of equation (1) satisfy \(\max\{p, a, k\} < C\).

In 1994, Yu and Liu [9] gave a complete resolution of equation (1). They proved that equation (1) has only three solutions: \((p, a, k) = (3, 1, 1), (3, 5, 3), (5, 1, 2)\). The key observation in [9] is that if \((p, a, k)\) is a solution to (1) with \(p \geq 5\) then \(k\) is even. From this fact, they obtained a small upper bound for \(p\) by applying Laurent, Mignotte and Nesterenko [3]. The remaining cases are verified by computation based on a criterion (see [9], Lemma 2).
It is easy to see from Wilson’s theorem that if \( p > 2 \) is a prime then
\[
(-1)^{(p-1)/2} \left( \left( \frac{p-1}{2} \right)! \right)^2 + 1 \equiv 0 \pmod{p}.
\]

In [4], Liouville claimed that the diophantine equation
\[
\left( \left( \frac{p-1}{2} \right)! \right)^2 + 1 = p^k
\]
in \( p, k \in \mathbb{Z}_{>0} \) with \( p > 2 \) and prime has only one solution \( (p, k) = (5, 1) \).

Thus it is natural to study the more general diophantine equation
\[
(-1)^{(n-1)/2} \left( \left( \frac{n-1}{2} \right)! \right)^2 + a^{n-1} = n^k
\]
in \( n, a, k \in \mathbb{Z}_{>0} \) with \( n > 2 \) and odd. We shall prove the following:

**Theorem 1.1.** Equation (2) has only two solutions: \( (n, a, k) = (3, 2, 1), (5, 1, 1) \).

We succeeded in proving Theorem 1.1 first by following [9] closely, relying on the theory of linear forms in logarithms. (The essential part of this proof is now given in §3.) After that, the author discovered that the square on the left-hand side of (2) made our task easier than resolving (1), so that an elementary proof without appealing to the theory of linear forms in logarithms should be possible. We present the elementary proof in §2.
2 An elementary proof of Theorem 1.1

We need the following lemmas.

Lemma 2.1. Suppose \( n \in \mathbb{Z}_{>0} \) with \( n \) composite and odd, then

\[
\left(\frac{n-1}{2}\right)! \mid \left(\frac{n-1}{2}\right)!^2.
\]

Proof. \( n \) odd and composite implies that \( n \geq 9 \). Furthermore, there exist \( b, c \in \mathbb{Z}_{>0} \) and \( \min(b, c) \geq 3 \) such that \( n = bc \). Thus, \( \max(b, c) \leq n/3 \). Since \( n/3 < (n-1)/2 \) for \( n \geq 9 \), we have \( b \mid \left(\frac{n-1}{2}\right)! \) and \( c \mid \left(\frac{n-1}{2}\right)! \). From this we obtain (3).

Lemma 2.2. For \( n \in \mathbb{Z} \) and \( n \geq 9 \), we have

\[
\left(\frac{n-1}{2}\right)! > \frac{1}{4} n^{(n-1)/4}.
\]

Proof. By Stirling's formula there exists \( \theta \) with \( 0 < \theta < 1 \) such that

\[
\frac{n!}{\sqrt{2\pi n} \left(\frac{n}{e}\right)^n} e^{\theta/(12n)}.
\]

Replace \( n \) by \((n-1)/2\), we would have

\[
\left(\frac{n-1}{2}\right)! > \sqrt{\pi(n-1)} \left(\frac{n-1}{2e}\right)^{(n-1)/2}.
\]

For \( n \geq 32 \), we have \((n-1)/(2e))^2 > n \) and (4) follows at once. By direct computation using PARI GP 1.38, we can easily verify (4) for \( 9 \leq n < 32 \). This proves the Lemma.
Lemma 2.3. Equation (2) has no integer solutions with \( n \) composite and \( n \equiv 1 \pmod{4} \).

**Proof.** Suppose there would exist such a solution \((n, a, k)\). Then we have \( n \geq 9 \) and
\[
\left( \left( \frac{n-1}{2} \right)! \right)^2 + a^{n-1} = n^k.
\]
Clearly the above yields
\[
n^k > \left( \left( \frac{n-1}{2} \right)! \right)^2
\]
and, on applying (4), we obtain \( k > (n-1)/3 \). Let \( p \) be an arbitrary prime divisor of \( n \). We proceed to show that \( p = 3 \). By (3), we have \( p \mid \left( \frac{n-1}{2} \right)! \), whence \( p \mid a \) by (5). For \( b \in \mathbb{Z} \setminus \{0\} \) denote by \( \text{ord}_p b \) the exponent to which \( p \) divides \( b \). Thus,
\[
\text{ord}_p \left( \left( \frac{n-1}{2} \right)! \right)^2 = \text{ord}_p (n^k - a^{n-1}) \\
\geq \min(k, n-1) > \frac{n-1}{3}.
\]
On the other hand, denoting by \([\theta]\) the integral part of a real number \( \theta \), we have
\[
\text{ord}_p \left( \left( \frac{n-1}{2} \right)! \right)^2 = 2 \sum_{i=1}^{\infty} \left[ \frac{n-1}{2p^i} \right] \\
\leq (n-1) \sum_{i=1}^{\infty} \frac{1}{p^i} = \frac{n-1}{p-1}.
\]
Thus we have \((n-1)/3 < (n-1)/(p-1)\). This leads to \( p < 4 \), whence \( p = 3 \) since \( n \) is odd. So \( n \) is power of 3 and \( 3 \mid a \). Since
\[
n^k > \left( \left( \frac{n-1}{2} \right)! \right)^2 > 3^{n-4},
\]
we have \( \text{ord}_3 (n^k) > n-4 \) and
\[
\text{ord}_3 (n^k - a^{n-1}) > n-4 > \frac{n-1}{2} \geq \text{ord}_3 \left( \left( \frac{n-1}{2} \right)! \right)^2.
\]
This contradicts (5), and Lemma 2.3 follows at once.
Lemma 2.4. Equation (2) has no integer solutions with \( n \) composite and \( n \equiv 3 \pmod{4} \).

Proof. Suppose there would exist such a solution \((n, a, k)\) to (2). Then \( n \geq 15 \),
\[
a^{n-1} - \left(\left(\frac{n-1}{2}\right)!ight)^2 = n^k
\]
and
\[
\left(a^{(n-1)/2} + \left(\frac{n-1}{2}\right)!\right)\left(a^{(n-1)/2} - \left(\frac{n-1}{2}\right)!ight) = n^k.
\]
Since \( a^{(n-1)/2} - \left(\frac{n-1}{2}\right)! \in \mathbb{Z}_{>0} \) and odd, \( a^{(n-1)/2} - \left(\frac{n-1}{2}\right)! = 1 \) and (7) would imply \( 2 \cdot \left(\frac{n-1}{2}\right)! + 1 = n^k \). Now let \( p \) be the smallest prime divisor of \( n \), so that \( 3 \leq p \leq n/3 \). Hence \( p \mid \left(\frac{n-1}{2}\right)! \), which means \( 2 \cdot \left(\frac{n-1}{2}\right)! + 1 = n^k \) is impossible. Thus, \( a^{(n-1)/2} - \left(\frac{n-1}{2}\right)! \geq 3 \). Applying (7) and (4), we obtain
\[
n^k \geq 3 \left(a^{(n-1)/2} + \left(\frac{n-1}{2}\right)!\right) > 6 \cdot \left(\frac{n-1}{2}\right)! > n^{(n-1)/4}.
\]
So \( k > (n - 1)/4 \). Next we prove that \( n \) is a power of 3. For otherwise there would exist a prime \( p \) such that \( p > 3 \) and \( p \mid n \). By (3), we have \( p \mid \left(\frac{n-1}{2}\right)! \) whence \( p \mid a \). Thus,
\[
\text{ord}_p(a^{n-1} - n^k) \geq \text{min}(k, n-1) = \frac{n-1}{4} \geq \frac{n-1}{p-1} \geq \text{ord}_p\left(\left(\frac{n-1}{2}\right)\right)^2,
\]
which contradicts (6). Hence \( n \) is a power of 3 and \( 3 \mid a \). (8) and \( n \geq 15 \) imply that \( n^k > 3^{(n-1)/2} \). So we have \( \text{ord}_3(n^k) > (n - 1)/2 \). Thus,
\[
\text{ord}_3(a^{n-1} - n^k) > \frac{n-1}{2} \geq \text{ord}_3\left(\left(\frac{n-1}{2}\right)!\right)^2.
\]
Again, we reach a contradiction to (6). This proves Lemma 2.4.

Lemma 2.5. For every integer \( n \geq 6 \), we have
\[
n! + 1 < \left(\frac{n}{2}\right)^n.
\]

Proof. (9) holds for \( n = 6 \) and can be verified by induction on \( n \), using \((1 + 1/n)^n > 2\) for \( n > 6 \).
Lemma 2.6. Equation (2) has only one solution with \( n \) prime and \( n \equiv 3 \pmod{4} \): \( (n, a, k) = (3, 2, 1) \).

Proof. Let \( (n, a, k) \) be such a solution. Then (2) implies (6) and (7). If \( a^{(n-1)/2} - \left( \frac{n-1}{2} \right)! \neq 1 \), then clearly both \( a^{(n-1)/2} - \left( \frac{n-1}{2} \right)! \) and \( a^{(n-1)/2} + \left( \frac{n-1}{2} \right)! \) are powers of \( n \). It follows that \( n \mid 2 \cdot \left( \frac{n-1}{2} \right)! \), which is absurd, since \( n \) is an odd prime. Hence,

\[
a^{(n-1)/2} = \left( \frac{n-1}{2} \right)! + 1.
\]

By using (9) and (10), we have \( a < (n - 1)/4 \) for odd \( n \geq 13 \), which contradicts the fact that the least prime divisor of \( a \) is greater than \( (n - 1)/2 \) (see (6)). Hence the only possibilities for \( n \) are \( n = 3, 7, 11 \). Now \( n = 3 \) and (10) imply \( a = 2 \); and (6) gives \( k = 1 \). Obviously (10) has no solutions with \( n = 7 \) or \( n = 11 \). This completes the proof of Lemma 2.6.

It remains to consider (2) with \( n \) prime and \( n \equiv 1 \pmod{4} \), which we may rewrite as

\[
\left( \left( \frac{p-1}{2} \right)! \right)^2 + a^{p-1} = p^k
\]

in \( p, a, k \in \mathbb{Z}_{>0} \) with \( p \) prime and \( p \equiv 1 \pmod{4} \).

Lemma 2.7. Suppose that \( (p, a, k) \) is a solution to (11) with \( p > 5 \). Then \( k \) is even.

Proof. Suppose \( k \) is odd, we shall deduce a contradiction. Now \( p \geq 13 \) and (11) gives

\[
p^k - a^{p-1} \equiv \left( \left( \frac{p-1}{2} \right)! \right)^2 \equiv 0 \pmod{q}
\]

for every prime \( q < (p-1)/2 \). The least prime divisor of \( a \) should be greater than \( (p - 1)/2 \) and hence \( (a, q) = 1 \). Thus,

\[
\left( \frac{p}{q} \right)^k = \left( \frac{a}{q} \right)^{p-1} = 1,
\]

whence

\[
\left( \frac{p}{q} \right) = 1 \quad \text{for every odd prime } q < (p - 1)/2,
\]
where \((\frac{\xi}{q})\) and \((\frac{\xi}{q})\) are Legendre symbols. Since \(p \equiv 1 \pmod{4}\), by the law of quadratic reciprocity, we have

\[
\left( \frac{q}{p} \right) = \left( \frac{q}{p} \right) \left( \frac{p}{q} \right) = (-1)^{(p-1)(q-1)/4} = 1
\]

for every odd prime \(q < (p - 1)/2\). The above yields

\[
\left( \frac{l}{p} \right) = 1
\]

for every positive odd integer \(l < (p - 1)/2\); more precisely, we have

\[
\left( \frac{2j - 1}{p} \right) = 1 \quad \text{for} \quad j = 1, \ldots, (p - 1)/4.
\]

On the other hand,

\[
\left( \frac{p - (2j - 1)}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{2j - 1}{p} \right) = (-1)^{(p-1)/2} = 1
\]

for \(j = 1, \ldots, (p - 1)/4\).

Note that the smallest even number among \(p - (2j - 1)\) for \(j = 1, \ldots, (p - 1)/4\) is \((p + 3)/2 \geq 8\), since \(p \geq 13\). Now \((\frac{2}{p}) = (\frac{2}{p})^2 = 1\). So altogether we have found at least \((p - 1)/2 + 1\) quadratic residues mod \(p\). This contradicts to the fact that there exist exactly \((p - 1)/2\) quadratic residues mod \(p\). Thus, \(k\) must be even.

**Lemma 2.8.** Equation (11) has only one solution with \(a = 1\): \((p, a, k) = (5, 1, 1)\).

**Proof.** For \(a = 1\), equation (11) becomes \(((\frac{p-1}{2})!)^2 + 1 = p^k\). Clearly for \(p = 5\), we have \(k = 1\). For \(p > 5\), Lemma 2.7 implies that \(k\) must be even. Thus, we have

\[
1 = \left( p^{k/2} - \left( \frac{p - 1}{2} \right)! \right) \left( p^{k/2} + \left( \frac{p - 1}{2} \right)! \right),
\]

where both factors on the right are positive integers, which is obviously absurd. Thus, Lemma 2.8 follows.
**Lemma 2.9.** Equation (11) has only one solution with \( p = 5 \): \( (p, a, k) = (5, 1, 1) \).

*Proof.* For \( p = 5 \), equation (11) becomes \( 4 + a^4 = 5^k \). It is shown by Nagell [6] that for the diophantine equation \( x^2 + 4 = y^n \) with \( n \geq 3 \), the solutions occur only when \( x = 2 \) and 11. Hence \( 4 + a^4 = 5^k \) has no solutions with \( k \geq 2 \); and this equation has only one solution with \( k = 1 \), \( a = 1 \).

**Lemma 2.10.** Equation (11) has no solutions with \( p > 5 \) and \( a > 1 \).

*Proof.* Suppose there would exist such a solution \( (p, a, k) \). We have from (11) that

\[
a^{p-1} = \left( \frac{p-1}{2} \right)! \left( \frac{p-1}{2} \right)! \left( \frac{p}{2} + \frac{p-1}{2} \right)!
\]

where both factors on the right are positive integers by Lemma 2.7. Suppose now \( a \) is prime. If \( p^{k/2} - \left( \frac{p-1}{2} \right)! > 1 \), then both \( p^{k/2} - \left( \frac{p-1}{2} \right)! \) and \( p^{k/2} + \left( \frac{p-1}{2} \right)! \) must be powers of \( a \). It follows that \( a \mid 2p^{k/2} \), which is impossible. Hence we obtain \( p^{k/2} - \left( \frac{p-1}{2} \right)! = 1 \) and \( 2 \cdot \left( \frac{p-1}{2} \right)! + 1 = a^{p-1} \). Applying Lemma 2.5, we get \( a^{p-1} < 2((p-1)/4)^{(p-1)/2} \). But this contradicts the fact that \( a \) is greater than \( (p-1)/2 \). Assume alternatively \( a \) is composite, then \( a \geq (p+1)^2/4 \).

Note that (11) gives

\[
\left( \left( \frac{p-1}{2} \right)! \right)^2 = (p^{k/2} - a^{(p-1)/2})(p^{k/2} + a^{(p-1)/2}) \\
\geq p^{k/2} + a^{(p-1)/2} > a^{(p-1)/2}.
\]

So

\[
\left( \frac{p-1}{2} \right)^{p-1} > \left( \left( \frac{p-1}{2} \right)! \right)^2 > a^{(p-1)/2} \geq \left( \frac{p+1}{2} \right)^{p-1},
\]

which is absurd again. The proof of Lemma 2.10 is thus complete.

*Completion of the proof of Theorem 1.1.* From Lemmas 2.8, 2.9, 2.10, we see that equation (2) has only one solution with \( n \) prime and \( n \equiv 1 \pmod{4} \): \( (n, a, k) = (5, 1, 1) \). On combining this fact with Lemmas 2.3, 2.4, 2.6, we obtain Theorem 1.1.
3 A second proof of Lemma 2.10

The method of linear forms in logarithms is very powerful, which enables us to give a second proof of Lemma 2.10, without the *ad hoc* observation on whether \( a \) is prime or composite, as we did in the proof of Lemma 2.10 given in §2. Obviously, this is of considerable theoretical interest.

**Lemma 3.1.** If \((p, a, k)\) is a solution to equation (11) with \( p > 5 \) and \( a > 1 \), then

\[
(12) \quad a \geq \frac{p+1}{2}, \quad k \equiv 2 \pmod{4}
\]

and

\[
(13) \quad (p - 1) \frac{\log \frac{p+1}{2}}{\log p} < k < 4 + 2\left(\frac{2 \log \left(\frac{p-1}{2}\right)! - p \log 2}{\log p}\right).
\]

**Proof.** From (11), we see that the least prime divisor of \( a \) must be greater than \((p - 1)/2\) and so \( a \geq (p + 1)/2 \). Suppose \( k \equiv 0 \pmod{4} \), then equation (11) can be written as

\[
\left(\left(\frac{p-1}{2}\right)!\right)^2 + \left(a^{(p-1)/4}\right)^4 = (p^{k/4})^4.
\]

By Mordell [5], the equation \( x^4 - y^4 = z^2 \) has no solutions with \( y > 0 \) and \( z > 0 \). We conclude that \( k \) is not congruent to \( 0 \pmod{4} \) and (12) follows from Lemma 2.7. By (11) and (12), we have

\[
p^k > a^{p-1} \geq \left(\frac{p+1}{2}\right)^{p-1},
\]

whence

\[
k > (p - 1) \frac{\log \frac{p+1}{2}}{\log p}.
\]

Since \( p \equiv 1 \pmod{4} \), we have

\[
p - 1 = a_2 2^2 + \cdots + a_{t-1} 2^{t-1} + 2^t,
\]
where \( a_j \in \{0, 1\} \) for \( 2 \leq j \leq t - 1 \), and
\[
a_2 + \cdots + a_{t-1} + 1 \leq t - 1 \leq \frac{\log(p - 1)}{\log 2} - 1,
\]
whence
\[
\text{ord}_2 \left( \left( \frac{p - 1}{2} \right)! \right) = \frac{p - 1}{2} - \left( a_2 + \cdots + a_{t-1} + 1 \right) \\
\geq \frac{p - 1}{2} - \frac{\log(p - 1)}{\log 2} + 1.
\]

From (11) and Lemma 2.7, we have
\[
\left( \frac{p^{k/2} + a^{(p-1)/2}}{2} \right) \left( \frac{p^{k/2} - a^{(p-1)/2}}{2} \right) = \left( \frac{p - 1}{2} \right)!^2.
\]
Note that \( p^{k/2} \equiv a^{(p-1)/2} \equiv 1 \pmod 4 \), since \( p \equiv 1 \pmod 4 \) and \( a \) is odd, whence \( p^{k/2} + a^{(p-1)/2} \equiv 2 \pmod 4 \). Thus,
\[
\text{ord}_2 (p^{k/2} + a^{(p-1)/2}) = 1.
\]

By (14), we obtain
\[
\text{ord}_2 (p^{k/2} - a^{(p-1)/2}) = 2 \text{ord}_2 \left( \frac{p - 1}{2} \right)! - 1 \\
\geq p - 2 \frac{\log(p - 1)}{\log 2}.
\]
The above inequality and (14) yield
\[
\left( \left( \frac{p - 1}{2} \right)! \right)^2 \geq \frac{2^p}{(p - 1)^2} \left( \frac{p^{k/2} + a^{(p-1)/2}}{2} \right) > \frac{2^p p^{k/2}}{(p - 1)^2}.
\]
Hence
\[
k < 4 + 2 \left( \frac{2 \log \left( \frac{p - 1}{2}! \right) - p \log 2}{\log p} \right).
\]
This completes the proof of Lemma 3.1.

### 3.1 Nonexistence of solutions with large \( p \)

The nonexistence of solutions to (11) with large \( p \) will follow from a deep result on linear forms in two logarithms, due to Laurent, Mignotte and Nesterenko [3].
In the sequel, denote by $h(\alpha)$ the logarithmic absolute height of an algebraic number $\alpha$, and $\log y$ signifies the natural logarithm for all $y \in \mathbb{R}_{>0}$. Note that, by definition, we have $h(m) = \log m$ for $m \in \mathbb{Z}_{>0}$.

**Lemma 3.2.** Let $\alpha_1, \alpha_2 > 1$ be multiplicatively independent real algebraic numbers and $b_1, b_2$ be positive integers. Set

\[
\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1, \\
D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}], \\
b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1},
\]

where $A_1$ and $A_2$ denote real numbers $> 1$ such that

\[
\log A_i \geq \max \left\{ h(\alpha_i), \frac{\log \alpha_i}{D}, \frac{1}{D} \right\} \quad (i = 1, 2).
\]

Then

\[
\log |\Lambda| \geq -32.31 D^4 \left( \max \left\{ \log b' + 0.71, \frac{10}{D}, \frac{1}{2} \right\} \right)^2 \log A_1 \log A_2.
\]

**Proof.** This is Corollary 2 of Theorem 2 of [3] with numerical values given by $(h_2, \rho, C_2) = (10, 4.9, 32.31)$ in Section 8, Tableau 2 of [3].

**Lemma 3.3.** If $(p, a, k)$ is a solution to equation (11) with $p > 5$ and $a > 1$, then

\[
-1.000005 \frac{((p-1)/2)!^2}{p^k} < (p - 1) \log a - k \log p < 0
\]

and

\[
13 \leq p \leq 763349.
\]

**Proof.** From (11) we have

\[
\frac{((p-1)/2)!^2}{p^k} = 1 - a^{p-1}p^{-k} = 1 - e^\lambda,
\]

where

\[
\lambda = (p - 1) \log a - k \log p < 0.
\]
On combining this with (13), we get $k \geq 10$ and $1 - e^{\lambda} \leq 720^2/13^{10}$. This implies that $\lambda > -4 \times 10^{-6}$. Consider the function

$$f(x) = 1.000005(1 - e^x) + x \quad \text{for} \quad x \in (-0.000004, 0).$$

Note that on the above interval

$$f'(x) = 1 - 1.000005e^x < 0.$$

Thus, we have $f(x) > f(0) = 0$ for $x \in (-0.000004, 0)$ and this yields

$$-1.000005(1 - e^{\lambda}) < \lambda < 0.$$

This and (17) imply (15). Now we proceed to prove (16). First we note that $a$ and $p$ are multiplicatively independent. For otherwise there would exist $b_1, b_2 \in \mathbb{Z}$ not all zero such that $p^{b_1}a^{b_2} = 1$. This yields $b_1b_2 < 0$ and $p | a$ which leads to a contradiction to (11). Hence we may apply Lemma 3.2 to \(\Lambda = (k/2) \log p - ((p - 1)/2) \log a\) with \(\alpha_1 = a, \alpha_2 = p, b_1 = (p - 1)/2, b_2 = k/2\). Then $D = 1$ and we can choose

$$\log A_1 = \frac{k}{p - 1} \log p > \max \{h(a), \log a, 1\},$$

$$\log A_2 = \log p = \max \{h(p), \log p, 1\},$$

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1} = \frac{p - 1}{\log p}.$$ We may assume that $p > 500000$, whence $\log b' + 0.71 > 10$. Lemma 3.2 and (15) imply that

$$-32.31 \left( \log \left( \frac{p - 1}{\log p} \right) + 0.71 \right)^2 \cdot \frac{k}{p - 1} (\log p)^2 \leq \log |\Lambda| < \log \left( 1.000005 \left( \frac{(p - 1)/2)!}{2^{p^k}} \right) \right).$$

This yields

$$\frac{k \log p}{p - 1} \left( p - 1 - 32.31 \log p \left( \log \left( \frac{p - 1}{\log p} \right) + 0.71 \right)^2 \right)$$

$$-2 \log \left( \frac{p - 1}{2} \right)! - \log \frac{1.000005}{2} < 0.$$ On noting that for $p > 500000$,

$$p - 1 - 32.31 \log p \left( \log \left( \frac{p - 1}{\log p} \right) + 0.71 \right)^2 > 0,$$
we see that (18) still holds with $k$ replaced by its lower bound (see (13))

$$(p - 1) \frac{\log \frac{p+1}{2}}{\log p}.$$ 

That is,

$$(19) \log \frac{p+1}{2} \left( p - 1 - 32.31 \log p \left( \log \left( \frac{p-1}{\log p} \right) + 0.71 \right)^2 \right)$$

$$-2 \log \left( \frac{p-1}{2} \right)! - \log \frac{1.000005}{2} < 0.$$ 

Observe that the left-hand side of the above inequality is an increasing function of $p$ for $p > 500000$. To see this, we denote by $f(x)$ the function obtained from the left-hand side of (19) by replacing $p$ with $x$; and writing

$$g(x) = (x - 1) \log \frac{x+1}{2} - 32.31(\log x \cdot (\log (x - 1) - \log \log x + 0.71))^2$$

$$-2 \log \Gamma \left( \frac{x+1}{2} \right) - \log \frac{1.000005}{2}.$$ 

Evidently for $x > 500000$, by (16) of [9], we have

$$f'(x) > g'(x) \geq 1 - 0.0001 - 64.62 \log x \cdot (\log x + 0.71) \cdot$$

$$((\log x + 0.71)/x + (\log x)/(x - 1))$$

$$> 0.3.$$ 

Now using (19) and the above observation, with the aid of PARI GP 1.38 on a Sun Sparc 20 Workstation, we obtain (16). This completes the proof of Lemma 3.3.

3.2 Computer treatment

Now equation (11) with $13 \leq p \leq 763349$ and $a > 1$ remains to be investigated. This will be carried out by computer based on the following criterion. For any real $\theta$, write $\{\theta\}$ for its fractional part.
Lemma 3.4. If \((p, a, k)\) is a solution to equation (11) for \(p > 5\) and \(a > 1\), then

\[
\{p^{k/(p-1)}\} < 1.000005 \frac{\left(\frac{p-1}{2}\right)!^2}{(p-1)(\frac{p+1}{2})^{p-2}}.
\]

Proof. Let

\[
d = p^{k/(p-1)}
\]

and

\[
c = d \exp \left(-1.000005 \frac{\left(\frac{p-1}{2}\right)!^2}{p^k(p-1)}\right).
\]

Then \(a^{p-1} < p^k\) yields \(a < d\). Note that (15) implies

\[
c < d \exp \left(\frac{(p-1) \log a - k \log p}{p-1}\right) = a.
\]

Now \(a \in \mathbb{Z}\) and \(a < d\) yield \(a \leq [d]\). Hence we have

\[
\{d\} = d - [d] \leq d - a < d - c
\]

and so

\[
\{d\} < d \left(1 - \exp \left(-1.000005 \frac{\left(\frac{p-1}{2}\right)!^2}{p^k(p-1)}\right)\right).
\]

\[
< d \cdot 1.000005 \frac{\left(\frac{p-1}{2}\right)!^2}{p^k(p-1)}
\]

\[
= 1.000005 \cdot \frac{\left(\frac{p-1}{2}\right)!^2}{p-1} p^{-k(p-2)/(p-1)}.
\]

Thus (20) follows by combining the above inequality with (13).

Lemma 3.4 enables us to carry out calculation on computer and effectively check the range of \(p\) satisfying (16). We use PARI GP 1.38 on a Sun Sparc 20 Workstation. (Technically, we use \((\frac{p-1}{2})! = \exp \log \Gamma'(\frac{p+1}{2})\). Thus we find out that for every pair \((p, k)\) with \(13 \leq p < 53\) and \(k\) satisfying (12) and (13),

\[
\{p^{k/(p-1)}\} > 1.000005 \frac{\left(\frac{p-1}{2}\right)!^2}{(p-1)(\frac{p+1}{2})^{p-2}}.
\]
For every pair \((p, k)\) with \(53 \leq p \leq 763349\) and \(k\) satisfying (12) and (13), we also have

\[
\left\{\frac{p^k}{(p-1)}\right\} > 10^{-25} > 1.000005 \frac{\left(\frac{p-1}{2}\right)^2}{(p-1)\left(\frac{p+1}{2}\right)^{p-2}}.
\]

Thus, we conclude, by Lemma 3.4, that equation (11) has no solutions \((p, a, k)\) with \(p\) satisfying (16) and \(a > 1\). This fact and Lemma 3.3 imply Lemma 2.10.
References


