ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 3, Summer 1996

A COMPLETE RESOLUTION OF A PROBLEM OF ERDŐS AND GRAHAM

KUNRUI YU AND DEHUA LIU

Dedicated to Professor Wolfgang M. Schmidt's 60th birthday

ABSTRACT. We prove that the equation $(p-1)! + a^{p-1} = p^k$ in p, a, $k \in \mathbf{Z}_{>0}$ with $p > 2$ and prime has only three solutions $(p, a, k) = (3, 1, 1), (3, 5, 3), (5, 1, 2)$.

1. Introduction. In the book of Erdős and Graham [**4**], it is asked: Is it true that the equation

$$(p-1)! + a^{p-1} = p^k \tag{1}$$

in $p, a, k \in \mathbf{Z}_{>0}$ with $p > 2$ and prime, has only a finite number of solutions? In 1856 Liouville [**6**] proved that (1) has only two solutions with $a = 1$:

$$(p, a, k) = (3, 1, 1), (5, 1, 2). \tag{2}$$

(See also Bachmann [**2**].) By Apéry [**1**], (1) has only two solutions with $p = 3$:

$$(p, a, k) = (3, 1, 1), (3, 5, 3). \tag{3}$$

Brindza and Erdős [**3**] noted that the equation $(n-1)! + a^{n-1} = n^k$ has no solution in $n, a, k \in \mathbf{Z}_{>0}$ with n composite. They proved in 1991 the following

Theorem 1 (Brindza and Erdős [**3**]). *There exists an effectively computable absolute constant C such that all solutions of equation* (1) *satisfy* $\max\{p, a, k\} < C$.

In the present paper we shall prove

Received by the editors on July 28, 1994, and in revised form on May 12, 1995.

Theorem 2. *Equation* (1) *has no solution other than the three given by* (2) *and* (3).

2. Preliminaries. We need the following lemmata.

Lemma 1. *Equation* (1) *has no solution* (p, a, k) *with* $p \geq 5$ *and* k *odd.*

Proof. Suppose equation (1) has a solution (p, a, k) with $p \geq 5$ and k odd. We proceed to deduce a contradiction from this assumption. Now (1) gives

$$p^k - a^{p-1} \equiv (p-1)! \equiv 0 \pmod{q}$$

for every odd prime $q < p$. Obviously, $(a, q) = 1$. Thus,

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

whence

$$\left(\frac{p}{q}\right) = 1 \quad \text{for every odd prime } q < p, \tag{4}$$

since p, k are odd, where (p/q) and (a/q) are Legendre symbols. (Damien Roy suggested this simple proof of (4). Our original proof is slightly more complicated.) We now deal with the following two cases separately.

(i) $p \equiv 1 \pmod 4$. Then

$$\left(\frac{q}{p}\right) = 1 \quad \text{for every odd prime } q < p \tag{5}$$

by (4) and the law of quadratic reciprocity, whence

$$\left(\frac{2l-1}{p}\right) = 1, \qquad l = 1, 2, \dots, (p-1)/2.$$

Further, $((p-1)/p) = (-1/p) = (-1)^{(1/2)(p-1)} = 1$. So there are at least $(1/2)(p-1) + 1$ quadratic residues: $1, 3, \dots, p-2, p-1 \pmod{p}$. This is absurd.

(ii) $p \equiv 3 \pmod 4$. Then

$$\left(\frac{q}{p}\right) = \begin{cases} +1 & \text{for every prime } q < p \\ & \text{with } q \equiv 1 \pmod 4, \\ -1 & \text{for every prime } q < p \\ & \text{with } q \equiv 3 \pmod 4, \end{cases} \tag{6}$$

by (4) and the law of quadratic reciprocity. Now $(p/3) = 1$ (by (4)) and $p \equiv 3 \pmod 4$ imply $p \equiv 7 \pmod{12}$. Further, $p = 7$ does not satisfy (4), since $(7/5) = -1$. So $p \geq 19$ and $p - 12$ has an odd number of prime divisors which are $\equiv 3 \pmod 4$. Hence, $((p-12)/p) = -1$ by (6). But (6) also yields

$$\left(\frac{p-12}{p}\right) = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)\cdot(-1) = 1,$$

contradicting $((p-12)/p) = -1$. The proof of Lemma 1 is thus complete. □

For any real θ write $\{\theta\}$ for its fractional part.

Lemma 2. *If (p, a, k) is a solution to equation (1), which is distinct from the three solutions given by (2) and (3), then*

$$\begin{gathered} p \geq 5, \qquad a \geq p+2, \qquad 2|k, \\ p+1 \leq k < 2\frac{\log\Gamma(p)}{\log p} < 2p-6, \end{gathered} \tag{7}$$

and, in addition, if $p \equiv 1 \pmod 4$, then

$$k < 2\frac{\log\Gamma(p) - (p-1)\log 2 + \log(p-1)}{\log p}. \tag{8}$$

Furthermore, we have for $p \geq 11$,

$$\frac{-1.02\cdot(p-1)!}{p^k} < (p-1)\log a - k\log p < 0 \tag{9}$$

and

$$\{p^{k/(p-1)}\} < 1.02\cdot(p-2)!p^{-(p+1)(p-2)/(p-1)}. \tag{10}$$

Proof. By Liouville [**6**], Apéry [**1**] and Lemma 1, we have

$$a > 1, \qquad p \geq 5, \qquad 2|k.$$

By (1), the least prime divisor of a is greater than p, whence a is odd and $a \geq p + 2$. Now (1) implies $p^k > a^{p-1} > p^{p-1}$, so $k \geq p + 1$. Further, from

$$(p^{k/2} + a^{(p-1)/2})(p^{k/2} - a^{(p-1)/2}) = (p-1)! \tag{11}$$

and the fact that $p^{k/2} - a^{(p-1)/2}$ is a positive integer, we see that $p^{k/2} < (p-1)! < p^{p-3}$ (since $2 \cdot 3 \cdot 4 < p^2$). So (7) is proved.

Proof of (8). For $m \in \mathbf{Z}\backslash\{0\}$ denote by $\mathrm{ord}_2 m$ the exponent to which 2 divides m. Since $p \equiv 1 \pmod 4$, we have

$$\begin{aligned} p - 1 &= a_2 \cdot 2^2 + \cdots + a_{t-1} \cdot 2^{t-1} + 2^t, \\ &a_j \in \{0, 1\}, \quad 2 \leq j \leq t-1, \\ s(p-1) &:= a_2 + \cdots + a_{t-1} + 1 \leq t - 1 \leq \frac{\log(p-1)}{\log 2} - 1. \end{aligned}$$

Now $p^{k/2} \equiv a^{(p-1)/2} \equiv 1 \pmod 4$, whence $\mathrm{ord}_2(p^{k/2} + a^{(p-1)/2}) = 1$. By (11) we obtain

$$\begin{aligned} \mathrm{ord}_2(p^{k/2} - a^{(p-1)/2}) &= \mathrm{ord}_2(p-1)! - 1 \\ &= p - 1 - s(p-1) - 1 \\ &\geq p - 1 - \log(p-1)/\log 2, \end{aligned}$$

whence

$$p^{k/2} - a^{(p-1)/2} \geq \frac{2^{p-1}}{p-1}.$$

Again, by (11),

$$p^{k/2} < (p-1)! \frac{p-1}{2^{p-1}}.$$

Now (8) follows at once.

Proof of (9). Write $\lambda = (p-1)\log a - k\log p$. From (1), (7) and $p \geq 11$, we get

$$1 - e^{\lambda} = 1 - a^{p-1}p^{-k} = \frac{(p-1)!}{p^k} \leq \frac{10!}{11^{12}}.$$

This inequality and $\lambda < 0$ yield $-0.01 < \lambda < 0$. Now consider the function

$$f(x) = 1.02(1 - e^x) + x$$

on $(-0.01, 0)$, where $f'(x) = -1.02e^x + 1 < 0$. So $f(x) > f(0) = 0$ for $x \in (-0.01, 0)$. In particular, $f(\lambda) > 0$, that is,

$$\lambda > -1.02(1 - e^{\lambda}) = -1.02 \cdot \frac{(p-1)!}{p^k},$$

as required.

Proof of (10). Write $d = p^{k/(p-1)}$ and $c = d \cdot \exp(-1.02 \cdot (p-2)!/p^k)$. By (9) and (1),

$$c < a < d. \tag{12}$$

Note that $d \notin \mathbf{Z}$, since

$$1 < \frac{p+1}{p-1} \leq \frac{k}{p-1} < \frac{2p-6}{p-1} < 2$$

by (7). Now (12), the fact that $a \in \mathbf{Z}$ and (7) imply

$$\begin{aligned}\{d\} < d - c &= d\left(1 - \exp\left(-1.02 \cdot \frac{(p-2)!}{p^k}\right)\right) \\ &< 1.02 \cdot p^{k/(p-1)} \cdot \frac{(p-2)!}{p^k} \\ &= 1.02 \cdot (p-2)! p^{-k(p-2)/(p-1)} \\ &\leq 1.02 \cdot (p-2)! p^{-(p+1)(p-2)/(p-1)}.\end{aligned}$$

This proves (10). The proof of Lemma 2 is complete. □

In the sequel, $h(\alpha)$ denotes the logarithmic absolute height of an algebraic number α and $\log y$ signifies the natural logarithm for all $y \in \mathbf{R}_{>0}$. Note that, by definition, we have $h(m) = \log m$ for $m \in \mathbf{Z}_{>0}$.

Lemma 3. *Let $\alpha_1, \alpha_2 > 1$ be multiplicatively independent real algebraic numbers. Set*

$$\begin{aligned}
&\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1, \\
&\qquad \text{where } b_1, b_2 \text{ are positive integers}, \\
&D = [\mathbf{Q}(\alpha_1, \alpha_2) : \mathbf{Q}], \\
&b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1},
\end{aligned}$$

where A_1 and A_2 denote real numbers greater than 1 such that

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

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 [**5**] with numerical values given by $(h_2, \rho, C_2) = (10, 4.9, 32.31)$ in Section 8, Tableau 2 of [**5**]. □

3. Proof of Theorem 2. Suppose that (1) has a solution (p, a, k) other than those given by (2) and (3). We proceed to prove that

$$p \leq 823309. \tag{13}$$

On noting that a and p are multiplicatively independent, we may apply Lemma 3 to

$$\Lambda = \frac{1}{2} k \log p - \frac{1}{2}(p-1) \log a$$

with $\alpha_1 = a$, $\alpha_2 = p$, $b_1 = (p-1)/2$, $b_2 = k/2$. Now $D = 1$ and we can choose

$$\begin{aligned} \log A_1 &= \frac{k}{p-1}\log p > \max\{h(a), \log a, 1\}, \\ \log A_2 &= \log p = \max\{h(p), \log p, 1\}, \\ b' &= \frac{b_1}{D\log A_2} + \frac{b_2}{D\log A_1} = \frac{p-1}{\log p}. \end{aligned}$$

In order to prove (13) we may assume that $p > 2\cdot 10^5$, whence $\log b' + 0.71 > 10$. So by Lemma 3 and (9), we obtain

$$\begin{aligned} -32.31&\left(\log\left(\frac{p-1}{\log p}\right) + 0.71\right)^2 \frac{k}{p-1}(\log p)^2 \\ &\le \log|\Lambda| \\ &< \log 0.51 + \log(p-1)! - k\log p. \end{aligned}$$

That is,

$$\begin{aligned} \frac{k\log p}{p-1}&\left\{p - 1 - 32.31\left(\log\left(\frac{p-1}{\log p}\right) + 0.71\right)^2 \log p\right\} \\ &\qquad - \log\Gamma(p) - \log 0.51 < 0. \end{aligned} \tag{14}$$

Now on noting (7) and

$$p - 1 - 32.31\left(\log\left(\frac{p-1}{\log p}\right) + 0.71\right)^2 \log p > 0 \quad \text{for } p > 2\cdot 10^5,$$

we see that (14) holds for $k = p+1$. Observe that the lefthand side of (14) with $k = p+1$ is an increasing function of p for $p > 2\cdot 10^5$. To see this, replacing p by x in the indicated function of p, we obtain a function

$$\begin{aligned} f(x) = (x+1)\log x - 32.31&\left(1 + \frac{2}{x-1}\right) \\ &\cdot\{\log x\cdot(\log(x-1) - \log\log x + 0.71)\}^2 \\ &- \log\Gamma(x) - \log 0.51. \end{aligned} \tag{15}$$

By Whittaker and Watson [**7**, p. 241], we have for $x > 2\cdot 10^5$,

$$
\begin{aligned}
\frac{d}{dx}\log\Gamma(x) &= -\gamma - \frac{1}{x} + x\sum_{n=1}^{\infty}\frac{1}{n(x+n)} \\
&\le -\gamma - \frac{1}{x} + x\sum_{n=1}^{\infty}\frac{1}{n([x]+n)} \\
&< -\gamma - \frac{1}{x} + [x]\sum_{n=1}^{\infty}\frac{1}{n([x]+n)} \\
&\quad + \sum_{n=1}^{\infty}\frac{1}{n(n+2\cdot 10^5)} \\
&< -\gamma - \frac{1}{x} + \left(1 + \frac{1}{2} + \cdots + \frac{1}{[x]}\right) \\
&\quad + 0.0001 \\
&< \log x - \frac{1}{x} + 0.0001,
\end{aligned}
\tag{16}
$$

where γ is Euler's constant:

$$
\begin{aligned}
\gamma &= \lim_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right) \\
&> 1 + \frac{1}{2} + \cdots + \frac{1}{[x]} - \log[x].
\end{aligned}
$$

By (15) and (16) we have, for $x > 2\cdot 10^5$,

$$
\begin{aligned}
f'(x) &> 1 - 0.0001 - 64.62\left(1 + \frac{2}{x-1}\right)\log x(\log(x-1) - \log\log x + 0.71) \\
&\quad \cdot \{x^{-1}(\log(x-1) - \log\log x + 0.71) \\
&\qquad + \log x\cdot((x-1)^{-1} - (x\log x)^{-1})\} \\
&> 0.1.
\end{aligned}
\tag{17}
$$

Now by (14) with $k = p+1$, (15), (17), the fact that p is a prime, and the aid of PARI GP 1.38, we obtain (13).

We used PARI GP 1.38 on several Sun Sparc 10 workstations and found out:

(i) For $p \in \{5, 7\}$ we have $p + 1 \geq 2p - 6$. Thus, by Lemma 2, equation (1) has no solution (p, a, k) with $p \in \{5, 7\}$, which is distinct from those given by (2) and (3).

(ii) For every pair (p, k) with $11 \leq p < 100$ and k satisfying (7), we have

$$\{p^{k/(p-1)}\} > 1.02 \cdot (p-2)! p^{-(p+1)(p-2)/(p-1)}.$$

We conclude, by Lemma 2, that equation (1) has no solution (p, a, k) with $11 \leq p < 100$.

(iii) For every pair (p, k) with $100 < p \leq 823309$, k satisfying (7), when $p \equiv 3 \pmod 4$; k satisfying (7) and (8), when $p \equiv 1 \pmod 4$, we have

$$\{p^{k/(p-1)}\} > 10^{-42} > 1.02 \cdot (p-2)! p^{-(p+1)(p-2)/(p-1)}.$$

Thus, by Lemma 2, equation (1) has no solution (p, a, k) with $100 < p \leq 823309$. This completes the proof of Theorem 2. □

Acknowledgments. We are indebted to Prof. M. Mignotte for sending us the paper Laurent, Mignotte and Nesterenko [**5**] via e-mail. The present paper was reported on at the Symposium on Diophantine Problems in Honor of Wolfgang Schmidt's 60th birthday, Boulder; and the writing up of the paper was completed during the authors' visit to Boulder in July 1994. We are grateful to Prof. Wolfgang Schmidt for his hospitality. We also thank Prof. A. Schinzel for supplying the reference [**2**].

REFERENCES

1. R. Apéry, *Sur une équation diophantienne*, C.R. Acad. Sci. Paris **251** (1960), 1451–1452.

2. P. Bachmann, *Niedere Zahlentheorie*, Erster Teil, Druck und Verlag von B.G. Teubner, Leipzig, 1902.

3. B. Brindza and P. Erdős, *On some diophantine problems involving powers and factorials*, J. Austral. Math. Soc., Ser. A, **51** (1991), 1–7.

4. P. Erdős and R.L. Graham, *Old and new problems and results in combinatorial number theory*, Monographie No. 28 de L'Enseignement Mathématique, Genève, 1980.

5. M. Laurent, M. Mignotte and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory, to appear.

6. M.J. Liouville, *Sur l'équation* $1 \cdot 2 \cdot 3 \cdots (p-1) + 1 = p^m$, J. Math. Pures Appl., Ser. 2, **1** (1856), 351–352.

7. E.T. Whittaker and G.N. Watson, *A course of modern analysis*, 4th edition, Cambridge University Press, 1958.

Department of Mathematics, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong.