Publ. Math. Debrecen
48 / 1-2 (1996), 145–149

On the diophantine equation $x^{p-1} + (p-1)! = p^n$

By MAOHUA LE (Zhanjiang, Guangdong)

Abstract. In this paper we prove that the equation $x^{p-1} + (p-1)! = p^n$, x, $n \in \mathbb{N}$, p an odd prime, has only the solutions $(x,p,n) = (1,3,1)$, $(1,5,2)$ and $(5,3,3)$. The above result completely solves a problem of ERDÖS and GRAHAM.

1. Introduction

Let $\mathbb{Z}, \mathbb{N}, \mathbb{Q}, \mathbb{P}$ be the sets of integers, positive integers, rational numbers and odd primes, respectively. ERDÖS and GRAHAM [5] asked if the equation

$$x^{p-1} + (p-1)! = p^n,\ x, n \in \mathbb{N},\ p \in \mathbb{P}, \tag{1}$$

has only finitely many solutions (x,p,n). In [1], BRINZDA and ERDÖS solved this problem. Simultaneously, they notice that by using the result of lower bounds for linear forms in two logarithms due to Mignotte and Waldschmidt, it is possible to obtain some sharper bounds for the solutions of (1). DONG [4] in his review on the paper of BRINDZA and ERDÖS [1] calculated that all solutions (x,p,n) of (1) satisfy $p \le 3.8 \cdot 10^{25}$ and $n \le 1.04 \cdot 10^{71}$. In this paper we prove the following result*:

Theorem. *The only solutions of the equation* (1) *are* $(x,p,n) = (1,3,1)$, $(1,5,2)$ *and* $(5,3,3)$.

Supported by the National Natural Science Foundation of China.
**Editorial remark*: The result of the present paper was presented also by KUNRUI YU at the Symposium on Diophantine Problems (Univ. of Colorado, Boulder, 2 June 26 – July 1, 1994). However according to our knowledge K. Yu's paper did not yet appear.
Mathematics Subject Classification: 11D61, 11J86.

2. Lemmas

Lemma 1. *The only solutions of the equation* (1) *with* $x = 1$ *are* $(x, p, n) = (1, 3, 1)$ *and* $(1, 5, 2)$.

Proof. This is an early result by J. Liouville (see [2]).

Lemma 2 ([8])**.** *The only solution of the equation*

$$X^2 + 2 = Y^Z, \quad X, Y, Z \in \mathbb{N}, \quad Z > 1, \tag{2}$$

is $(X, Y, Z) = (5, 3, 3)$.

Lemma 3 ([6])**.** *The equation*

$$X^p - Y^p = m!, \quad X, Y, m \in \mathbb{N}, \quad p \in \mathbb{P},$$

has no solutions (X, Y, m, p).

For any prime p and any $a/b \in \mathbb{Q} \setminus \{0\}$ with $\gcd(a, b) = 1$, we denote by $\mathrm{ord}_p\, a/b$ the order to which p divides $|a/b|$.

Lemma 4 ([3, Théorèm 2])**.** *Let* p *be a prime, and let* $a_1, \dots, a_n \in \mathbb{Z}$ *with* $a_i \equiv 1 \pmod p$ *for* $i = 1, \dots, n$. *If* $\Lambda = a_1^{b_1} \cdots a_n^{b_n} - 1 \neq 0$ *for some* $b_1, \dots, b_n \in \mathbb{Z}$, *then we have*

$$\mathrm{ord}_p \left(a_1^{b_1} \cdots a_n^{b_n} - 1\right) < \left(\frac{(2p-1)\log p}{2p-2}\right)^{n-2} 9^{n+4} n^{3n+5} (\log A_1) \cdots (\log A_n) Z_0 G_0,$$

where $A_i = \max(p, |a_i|)$ $(i = 1, \dots, n)$,

$$Z_0 = \begin{cases} 2(\log 2)(\log 8n), \\ 4(\log p)(\log 3np), \end{cases} \qquad G_0 = \begin{cases} \max\big((\log 2)(\log B),\ 6nZ_0\big), & \text{if } p = 2, \\ \max\big((\log p)(\log B),\ 5nZ_0\big), & \text{if } p > 2, \end{cases}$$

where $B = 7\max(|b_1|, \dots, |b_n|)/10(n+1)$.

3. Proof of the Theorem

By Lemma 1, it suffices to prove that the only solution of the equation (1) is $(x, p, n) = (5, 3, 3)$ with $x > 1$.

Let (x, p, n) be a solution of (1) with $x > 1$. Write $p - 1 = q_0^{\alpha_0} q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, where $q_0 = 2$, $q_1, \dots, q_s$ are distinct odd primes and $\alpha_0, \alpha_1, \dots, \alpha_s \in \mathbb{N}$. If $s > 0$, then $x^{p-1} - 1 \equiv 0 \pmod{q_1^{\alpha_1+1}}$ and $(p-1)! \equiv 0 \pmod{q_1^{\alpha_1+1}}$, since $x^{p-1}-1\equiv 0 \pmod{p-1}$ and $(p-1)!\equiv 0 \pmod{(p-1)^2/2}$. Therefore, we see from (1) that $p^n-1\equiv 0 \pmod{q_1^{\alpha_1+1}}$. This implies that $n\equiv 0 \pmod{q_1}$. Let $X=p^{n/q_1}$ and $Y=x^{(p-1)/q_1}$. Then we have

$$X^{q_1}-Y^{q_1}=(p-1)!\ ,\quad X,Y\in\mathbb{N}. \tag{3}$$

By Lemma 3, (3) is impossible. So we have $s=0$, $p=2^{\alpha_0}+1$ and p is a Fermat's prime. Hence, $p=2^{2^m}+1$, where $m\in\mathbb{Z}$ with $m\geq 0$.

If $m=0$, then $p=3$ and $(X,Y,Z)=(x,3,n)$ is a solution of the equation (2) with $Z>1$. By Lemma 2, the only solution of the equation (1) with $x>1$ and $p=3$ is $(x,p,n)=(5,3,3)$.

If $m=1$, then $p=5$ and

$$x^4+24=5^n,\quad x,n\in\mathbb{N},\ x>1, \tag{4}$$

by (1). Since 3 is a quadratic nonresidue mod 5, we have $2\mid n$. Then from (4) we get $5^{n/2}+x^2=6$, $5^{n/2}-x^2=4$ and $(x,n)=(1,1)$. Therefore, (4) is impossible.

If $m\geq 2$, then $p\geq 17$ and

$$\mathrm{ord}_2(p-1)!=\sum_{i=1}^{\infty}\left[\frac{2^{2^m}}{2^i}\right]=2^{2^m-1}+\cdots+2+1=p-2. \tag{5}$$

Since $x^{p-1}-1\equiv 0 \pmod{2^{2^m+2}}$ and $p-2=2^{2^m}-1>2^m+2$, (1) implies that $p^n-1\equiv 0 \pmod{2^{2^m+2}}$ and $n\equiv 0 \pmod 4$. So we have

$$\begin{gathered} p^{n/2}+x^{(p-1)/2}=T_1,\quad p^{n/2}-x^{(p-1)/2}=T_2,\\ T_1T_2=(p-1)!,\quad T_1,T_2\in\mathbb{N}. \end{gathered} \tag{6}$$

Let

$$A(p)=\prod_{\substack{q\in\mathbb{P},\ q\equiv 1 \pmod 4,\\ q<p-1,\ q^\alpha\,\|\,(p-1)!}} q^\alpha,\qquad \overline{A}(p)=\frac{(p-1)!}{A(p)}. \tag{7}$$

Notice that $2\nmid px$, $\gcd(x,p)=1$ and $n/2\equiv (p-1)/2\equiv 0 \pmod 2$. We see from (6) and (7) that $\gcd(T_1/2,\ \overline{A}(p))=1$. Hence, we obtain $T_1\leq 2A(p)$ and

$$x<\big(A(p)\big)^{2/(p-1)}. \tag{8}$$

Since $\gcd(p,(p-1)!)=1$, every prime factor q of x satisfies $q\geq p+2$. On the other hand, by Stirling's theorem, we have

$$(p-1)!<\sqrt{2\pi(p-1)}\left(\frac{p-1}{e}\right)^{p-1}e^{1/12(p-1)}\ . \tag{9}$$

Since $A(p) < (p-1)!/2^{p-1}$ by (5), we get from (8) and (9) that

$$p+2 \le x < \big(A(p)\big)^{2/(p-1)} < \left(\frac{(p-1)!}{2^{p-1}}\right)^{2/(p-1)} \tag{10}$$

$$= \frac{1}{4}\big((p-1)!\big)^{2/(p-1)} < \frac{p^2}{4e^2}\left(1-\frac{1}{p}\right)^2 \big(2\pi(p-1)\big)^{1/(p-1)} e^{1/6(p-1)^2} < p^2.$$

Therefore, by (1), (9) and (10), we have

$$\begin{aligned} p-1 \le n &= \frac{\log\big(x^{p-1}+(p-1)!\big)}{\log p} \\ &= \frac{1}{\log p}\Bigg((p-1)\log x + \frac{2(p-1)!}{2x^{p-1}+(p-1)!} \\ &\qquad \times \sum_{j=0}^{\infty}\frac{1}{2j+1}\left(\frac{(p-1)!}{2x^{p-1}+(p-1)!}\right)^{2j}\Bigg) \\ &< \frac{1}{\log p}\left((p-1)\log x + \frac{4(p-1)!}{2p^{p-1}+(p-1)!}\right) \\ &< \frac{p\log x}{\log p} < 2p. \end{aligned} \tag{11}$$

By Lemma 4, if $p > 2^{100}$, then from (10) and (11) we get

$$\begin{aligned} &\operatorname{ord}_2\left(p^n - x^{p-1}\right) = \operatorname{ord}_2\left(p^n x^{-(p-1)} - 1\right) \\ &< 2^{14}3^{12}(\log 2)^2(\log p)(\log x)\left(\log\frac{7n}{30}\right) < 8\cdot 10^9(\log p)^3. \end{aligned} \tag{12}$$

Since $\operatorname{ord}_2\left(p^n - x^{p-1}\right) = \operatorname{ord}_2(p-1)!$ by (1), the combination of (5) and (12) yields

$$p-2 < 8\cdot 10^9(\log p)^3,$$

whence we conclude $p < 2^{52}$, a contradiction. Therefore, $p < 2^{100}$ and $m < 7$. By [7], it suffices to consider the cases $p \in \{17, 257, 65537\}$.

Since $A(17) = 5^3\cdot 13$ and $A(257) = 5^{62}\cdot 13^{20}\cdot 17^{15}\cdot 29^8\cdot 37^6\cdot 41^6\cdot 53^4\cdot 61^4 \cdot 73^3\cdot 89^2\cdot 97^2\cdot 101^2\cdot 109^2\cdot 113^2\cdot 137\cdot 149\cdot 157\cdot 173\cdot 181\cdot 193\cdot 197\cdot 229\cdot 233\cdot 241\cdot 249$, we have $\big(A(17)\big)^{1/8} < 3$ and $\big(A(257)\big)^{1/128} < 25$. Hence, by (8) and (10), equation (1) has no solution (x, p, n) if $p \in \{17, 257\}$.

If $p=65537$, then we have $p\equiv 2 \pmod{257}$ and $2^n\equiv p^n\equiv x^{p-1} \equiv 1 \pmod{257}$. Since $2^8\equiv -1 \pmod{257}$, we get $n\equiv 0 \pmod{16}$. Therefore, by (9) and (10), we obtain

$$(p-1)^{59640}>(p-1)!=p^n-x^{p-1}=\left(p^{n/16}\right)^{16}-\left(x^{(p-1)/16}\right)^{16}$$
$$=\left(p^{n/16}-x^{(p-1)/16}\right)\left(p^{15n/16}+p^{14n/16}x^{(p-1)/16}+\cdots+x^{15(p-1)/16}\right)$$
$$>16x^{15(p-1)/16}\geq 16(p+2)^{61440},$$

a contradiction. Thus, the only solution of equation (1) with $x>1$ is $(x,p,n)=(5,3,3)$. The proof is complete.

Acknowledgements. The author would like thank the referee for his valuable suggestions.

References

[1] B. Brindza and P. Erdös, On some diophantine problems involving powers and factorials, *J. Austral. Math. Soc. Ser. A* **51** (1991), 1–7.
[2] L. E. Dickson, History of the Theory of Numbers, Vol. 2, *Chelsea Pub. Co., New York*, 1952.
[3] P.-P Dong, Minorations de combinaisons linéaires de logarithmes p-adiques de nombres algébriques, *C. R. Acad. Sci. Paris Sér. I Math.* **315** (1992), 503–506.
[4] P.-P. Dong, Mathematical Review, 92i: 11036.
[5] P. Erdös and R. L. Graham, Old and New Problems and Results in Combinatorial Number Theory, *Geneva*, 1980.
[6] P. Erdös and R. Obláth, Über diophantische Gleichungen der Form $n!=x^p\pm y^p$ and $n!\pm m!=x^p$, *Acta Litt. Sci. Szeged* **8** (1937), 241–255.
[7] J. C. Hallyburton and J. Brillhart, Two new factors of Fermat numbers, *Math. Comp.* **29** (1975), 109–112.
[8] T. Nagell, Verallgemeinerung eines Fermatschen Satzes, *Arch. Math.* **5** (1954), 153–159.

LE MAOHUA
DEPARTMENT OF MATHEMATICS
ZHANJIANG TEACHERS COLLEGE
P.O. BOX 524048
ZHANJIANG, GUANGDONG
P. R. CHINA

(Received December 6, 1994; revised May 16, 1995)