J. Austral. Math. Soc. (Series A) **51** (1991), 1-7

ON SOME DIOPHANTINE PROBLEMS INVOLVING POWERS AND FACTORIALS

B. BRINDZA and P. ERDŐS

(Received 20 June 1989)

Communicated by J. H. Loxton

To the memory of Kurt Mahler

Abstract

In this paper the power values of the sum of factorials and a special diophantine problem related to the Ramanujan-Nagell equation are studied. The proofs are based on deep analytic results and Baker's method.

1980 *Mathematics subject classification* (*Amer. Math. Soc.*) (1985 *Revision*): 11 D 61.

1. Power values of the sum of factorials

Erdös visited Mahler a few days before his death in February 1988 and discussed with Mahler the paper, his last, on which Mahler had been working. Mahler had investigated the following question.

Let $k > 1$ be an integer and consider those numbers of the form $\sum_{i=1}^{\infty} \varepsilon_i k^i$ where $\varepsilon_i \in \{0, 1\}$ such that

$$(1) \qquad \sum_{i=1}^{\infty} \varepsilon_i k^i = x^2, \qquad x \in \mathbb{Z}$$

has infinitely many solutions (for $k = 2$ this is of course trivial). Mahler conjectured that for $k \geq 5$ the equation (1) has only a finite number of solutions. A nontrivial solution, for $k = 4$, is $1 + 7 + 7^2 + 7^3 = 20^2$.

The first author is a National Research Fellow, funded by the Australian Research Committee.

On seeing Mahler's question it seems natural to ask whether it is true that

(2) $$\sum_{i=1}^{\infty} \varepsilon_i i! = x^z, \qquad \varepsilon_i \in \{0, 1\}, \qquad \sum_{i=1}^{\infty} \varepsilon_i < \infty$$

has only finitely many solutions in $\varepsilon_1, \dots, x, z \in \mathbb{Z}$ with $z > 1$. But in this generality the question is hopeless. However, it is an old conjecture that

$$1 + n! = x^2$$

has only the solutions $n = 4, 5, 7$. We prove

THEOREM 1. *For every positive integer r there is an $n_0 = n_0(r)$ such that none of the integers*

$$\sum_{i=1}^{r} n_i!, \qquad n_0 < n_1 < \cdots < n_r$$

are powerful; that is, each has a prime factor which divides $\sum_{i=1}^{\infty} n_i!$ to the first power.

Unfortunately, there seems to be no way to give an explicit value for $n_0(r)$.

PROOF OF THEOREM 1. Denote by $p_1 < \cdots < p_l$ the primes in the interval $(\frac{1}{2}n_1, n_1)$. Observe that

$$\frac{1}{n_1!} \sum_{i=1}^{r} n_i! = 0 \bmod \left[\prod_{j=1}^{l} p_j\right];$$

otherwise one of the p_j's would divide $\sum_{i=1}^{r} n_i!$ to the first power only. From the known elementary inequality $\prod_{j=1}^{l} p_j > 2^{1/2n_1}$ we obtain

$$\frac{1}{n_1!} \sum_{i=1}^{r} n_i! > 2^{1/2n_1}$$

which easily implies

(3) $$n_r > n_1 \left(1 + \frac{c_1}{\log n_1}\right)$$

where the constant c_1 depends only on r.

Now we must use a strong theorem on prime numbers for which there is no effective proof (though such a proof could be constructed in principle).

There is an absolute constant c_2 so that for large n and $d > n^{3/4}$

(4) $$\pi(n+d) - \pi(n) > \frac{c_2 d}{\log n}$$

(See, for example, [2, page 167].)

Applying this result we immediately have

$$n_2 < 2p_1 < n_1 + 2n_1^{3/4}. \tag{5}$$

If $r = 2$ then from (3) and (5)

$$n_1 + \frac{c_1 n_1}{\log n_1} < n_2 < n_1 + 2n_1^{3/4}$$

which is a contradiction for n_0 large enough.

In the sequel we may assume that $r \geq 3$. Let $2 < s \leq r$ be the smallest index for which

$$n_s > n_1 + 2n_1^{3/4} \quad \text{and} \quad n_s - n_{s-1} > (n_{s-1} - n_1)(\log n_1)^4.$$

Such an s does exist by (3). Moreover, by (3) and the minimality of s we can assume that $n_{s-1} < n_1 + n_1^{9/10}$.

Let $q_1, \dots, q_t$ denote the primes between $n_{s-1}/2$ and $\min(1/2n_s, n_1)$. By (4), $t > (n_{s-1} - n_1)(\log n_{s-1})$ (since $\log n_1$ and $\log n_{s-1}$ differ by $\log 2$ at most).

Now we show that

$$\frac{1}{n_1!} \sum_{i=1}^{s-1} n! < \prod_{j=1}^{t} q_j.$$

Indeed,

$$\frac{1}{n_1!} \sum_{i=1}^{s-1} n! < r n_{s-1}^{n_{s-1} - n_1} < n_{s-1}^{(n_{s-1} - n_1)\log n_1} < \left[\frac{n_{s-1}}{2}\right]^t < \prod_{j=1}^{t} q_j.$$

Hence there is a prime q_j which does not divide $(1/n_1!)\sum_{i=1}^{s-1} n!$.

On the other hand $n_1 < n_{s-1} < 2q_j < n_s$ and $q_j < n_1$, and therefore q_j divides $\sum_{i=1}^{r} n_i!$ to the first power only, which completes the proof.

2. The Ramanujan-Nagell equation and a related problem

In the book of Erdös and Graham "Old and new problems and results in combinatorial number theory" it is asked "Is it true that the equation

$$(p-1)! + a^{p-1} = p^k \tag{6}$$

in positive integers a, k, p, with $p > 2$ and prime, has only a finite number of solutions?" More than 150 years ago Liouville proved that

$$(p-1)! + 1 = p^k$$

https://doi.org/10.1017/S1446788700033255 Published online by Cambridge University Press

has only two solutions: $p = 3$ and $p = 5$. For $a > 1$, a non-trivial solution is given by $2! + 5^2 = 3^3$. It is interesting that if p is not a prime then (6) has no solution, that is, the equation

$$(n-1)! + a^{n-1} = n^k$$

has no solution in positive integers n, a, k with $n > 2$ and not a prime. Indeed, if n is a composite number then $n|(n-1)!$ and $n^k > (n-1)!$ implies $k > n - n/\log n$. Let P be the largest prime factor of n. Then $(n-1)!$ cannot be divisible by such a high power of P except, possibly, if $P = 2$. In this case, n is a power of 2 and a is even. Hence $2^{n-1}|a^{n-1}$, $2^{n-1}|n^k$ but 2^{n-1} does not divide $(n-1)!$.

Returning to the equation (6), we prove

THEOREM 2. *There exists an effectively computable absolute constant C such that all solutions of the equation* (6) *satisfy*

$$\max\{p, a, k\} < C.$$

This equation is a little eccentric but the proof of Theorem 2 is rather interesting. We shall show that for every solution

$$\exp\left(C_1 \frac{p}{\log p}\right) < k < C_2 p^3 \tag{7}$$

where C_1 and C_2 are effectively computable absolute constants. Both the lower and upper bounds in (7) are proved by *Baker's method* and, surprisingly, the lower bound is much larger in p than the upper one. The second part of (7) is a simple consequence of the following more general result on the Ramanujan-Nagell equation.

THEOREM 3. *Let D be a nonzero rational integer. Then all the solutions of the equation*

$$x^2 + D = p^k \tag{8}$$

in positive integers x, p, k with $k, p > 1$ satisfy

$$\frac{k}{\log k} < C_3(p \log p + \log |D|)p \log p$$

where C_3 is an effectively computable absolute constant.

This upper bound for k is near to the best possible in D.

The proofs of Theorems 2 and 3 are based on the following deep results on linear forms in logarithms.

Let $\alpha_1, \ldots, \alpha_n$ be nonzero algebraic numbers and let $A_1, \ldots, A_n$ be positive real numbers satisfying

$$A_j \geq \max\{H(\alpha_j), e\}, \qquad 1 \leq j \leq n$$

where $H(\cdot)$ is the usual absolute height function.

LEMMA 1 (Philippon and Waldschmidt [4]). *Let $b_1, \ldots, b_n$ be rational integers such that*

$$\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1.$$

Let B be a real number satisfying

$$B \geq \max_{1 \leq i \leq n} |b_i| \quad \text{and} \quad B \geq e.$$

Then $|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| > \exp(C_4 \log A_1 \cdots \log A_n \log B)$ where C_4 is an effectively computable constant depending only on n and on the degree of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ over $\mathbb{Q}$.

The following lemma is a special simple case of Yu's result for linear forms in the p-adic case.

LEMMA 2 (Yu [5]). *Let a_1, a_2 be odd integers with $|a_1||a_2| > 1$ and let b_1, b_2 be rational integers such that $a_1^{b_1} a_2^{b_2} \neq 1$. Further, let $q > 2$ be a prime for which*

$$[Q(a_1^{1/q}, a_2^{1/q}) : \mathbb{Q}] = q^2.$$

Then

$$\operatorname{ord}_2(a_1^{b_1} a_2^{b_2} - 1) < C_5 q^6 \log|a_1| \log|a_2| \log\log|a_1| \log B$$

where $B = \max\{2, |b_1|, |b_2|\}$ and C_5 is an effectively computable absolute constant.

PROOF OF THEOREM 2. From (6) we immediately have $a > p$, $k \geq p$ and

$$1/2(p-1) \leq \operatorname{ord}_2(p-1)! = \operatorname{ord}_2(p^k a^{-p} - 1). \tag{9}$$

Preparatory to an application of Lemma 2, we prove the existence of a prime $q > 2$ for which

$$q < 2 \log\log a \quad \text{and} \quad [\mathbb{Q}(p^{1/q}, a^{1/q}) : \mathbb{Q}] = q^2.$$

Indeed, there is a prime $2 < q < 2 \log\log a$ such that a is not a qth power, otherwise

$$a \geq 3^A \text{ with } A = \prod_{P < 2 \log\log a} P \qquad (P \text{ prime})$$

https://doi.org/10.1017/S1446788700033255 Published online by Cambridge University Press

which is a contradiction. If $a^{1/q}$ does not generate an extension of $\mathbb{Q}(p^{1/q})$ of degree q then, by Kummer theory, $a = p^r b^q$ where $0 \le r < q$, $r \in \mathbb{Z}$ and $b \in \mathbb{Q}$. This is not possible since a is not a qth power and $(a, p) = 1$. Thus we may apply Lemma 2 with an appropriate q, obtaining

$$\text{(10)} \qquad \operatorname{ord}_2(p^k a^{-p} - 1) < c_6 \log p \log a \log k (\log\log a)^7$$

with $c_6 = 2^6 c_5$. In the sequel $c_7, \dots, c_{18}$ will denote effectively computable positive absolute constants. Comparing (10) with (9) we have

$$\tfrac{1}{2}(p-1)^2 < c_6(\log p)(\log a^{p-1})(\log k)(\log\log a)^7 < c_7 k(\log k)^8(\log p)^2$$

and that yields $p^{3/2} < c_8 k$. Combining this inequality with (6) we have

$$|a^{p-1}p^{-k} - 1| = \frac{(p-1)!}{p^k} < \exp -c_9 k \log p < \exp -c_{10} p \log a.$$

However, from Lemma 1

$$|a^{p-1}p^{-k} - 1| > \exp -c_{11} \log a \log p \log k.$$

The last two inequalities imply $\exp c_{12}\frac{p}{\log p} < k$.

To prove the second part of (7) we set $x = a^{(p-1)/2}$ and $D = (p-1)!$. Then

$$x^2 + D = p^k$$

and Theorem 3 gives $k > c_{13} p^3$ which completes the proof of Theorem 2.

Proof of Theorem 3. We factorize equation (8) in the field $\mathbb{Q}(\sqrt{p})$:

$$((\sqrt{p})^k - x)((\sqrt{p})^k + x) = D.$$

Let ε be the fundamental unit for $\mathbb{Q}(\sqrt{p})$ with

$$1 < |\varepsilon| < \exp c_{14} p \log p.$$

The norm of the factors $(\sqrt{p})^k \pm x$ is D or $-D$. Hence the factors can be written in the form

$$\text{(11)} \qquad (\sqrt{p})^k + x = d_1 \varepsilon^t, \qquad (\sqrt{p})^k - x = d_2 \varepsilon^{-t} \qquad (t \in \mathbb{Z})$$

where d_1 and d_2 are conjugate to one another (over $\mathbb{Q}$) and where we may assume that

$$\text{(12)} \qquad |\log|d_i|| < c_{15} p \log p + \log|D|, \qquad i = 1, 2$$

(see for example [1, Lemma 3]). Let $\{1, \omega\}$ be an integral basis for $\mathbb{Q}(\sqrt{p})$ with $\omega \in \{\sqrt{p}, (1+\sqrt{p})/2\}$ and $\varepsilon = u + v\omega$. Then

$$|\varepsilon| > \tfrac{1}{2}\left(|\varepsilon| + \frac{1}{|\varepsilon|}\right) \ge |v\omega| \ge |\omega| \ge \tfrac{1}{2}(1+\sqrt{p}) \ge \tfrac{1}{2}(1+\sqrt{2}) > 1$$

https://doi.org/10.1017/S1446788700033255 Published online by Cambridge University Press

and from (11) and (12)

$$|t| < c_{16}|t|\log|\varepsilon| \le c_{16}(\log((\sqrt{p})^k + x) + |\log|d_1||) < c_{17}k\log p,$$

under the assumption that $k > \max\{p, \log|D|\}$, for otherwise, Theorem 3 is proved. Obviously,

$$d_1\varepsilon^t + d_2\varepsilon^{-t} = 2(\sqrt{p})^k.$$

Hence

$$\Lambda = |2(\sqrt{p})^k d_1^{-1}\varepsilon^{-t} - 1| < \frac{|(\sqrt{p})^k - x|}{|(\sqrt{p})^k + x|} < \frac{1}{(\sqrt{p})^k}.$$

But from Lemma 1,

$$\Lambda > \exp -c_{18}(\log p)(p\log p)(p\log p + \log|D|)\log k,$$

which proves Theorem 3.

REMARK. A p-adic version of a recent result of Mignotte and Waldschmidt [3] would lead to a sharper bound for k.

References

[1] K. Győry, 'Solutions of linear diophantine equations', Algebraic Integers of Bounded Norm, *Ann. Univ. Scien. Budapest* **22–23** (1980), 225–233.

[2] Y. Motohashi, *Lectures on sieve methods and prime number theory*, Springer, Berlin, 1989.

[3] M. Mignotte and M. Waldschmidt, 'Linear forms in two logarithms and Schneider's Method (II)', to appear.

[4] P. Philippon and M. Waldschmidt, 'Lower bounds for linear forms in logarithms', *New Advances in Transcendence Theory*, ed. A. Baker, Cambridge Univ. Press, 1988, pp. 280–313.

[5] K. Yu, 'Linear forms in logarithms in the p-adic case', *New Advances in Transcendence Theory*, ed. A. Baker, Cambridge Univ. Press, Cambridge, 1988, pp. 411–434.

Mathematical Institute
Kossuth Lajos University
4010 Debrecen
Hungary