[18] R. M. Kaufman, *Bounds for linear forms in the logarithms of algebraic numbers with p-adic metric*, Vestnik Moskov. Univ. Ser. I, 26 (1971), 3–10.
[19] J. H. Loxton, M. Mignotte, A. J. van der Poorten and M. Waldschmidt, *A lower bound for linear forms in the logarithms of algebraic numbers*, C. R. Math. Acad. Sci. Canada = Math. Report Acad. Sci. Canada 11 (1987), 119–124.
[20] K. Mahler, *Ein Beweis der Transzendenz der P-adischen Exponentialfunktion*, J. Reine Angew. Math. 169 (1932), 61–66.
[21] — *Über transzendente P-adische Zahlen*, Compositio Math. 2 (1935), 259–275.
[22] — *On some inequalities for polynomials in several variables*, J. London Math. Soc. 37 (1962), 341–344.
[23] — *On a class of entire functions*, Acta Math. Acad. Sci. Hungar. 18 (1967), 83–96.
[24] M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Schneider's method*, Math. Annalen 231 (1978), 241–267.
[25] A. J. van der Poorten, *Hermite interpolation and p-adic exponential polynomials*, J. Austral. Math. Soc. 22 (1976), 12–26.
[26] — *Linear forms in logarithms in the p-adic case*, in: *Transcendence theory: advances and applications*, edited by A. Baker and D. W. Masser, Academic Press, London 1977, 29–57 pp.
[27] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.
[28] A. Schinzel, *On two theorems of Gelfond and some of their applications*, Acta Arith. 13 (1967), 177–236.
[29] L. G. Schnirelman, *On functions in normed algebraically closed fields*, Izv. Akad. Nauk SSSR, Ser. Mat. 5/6, 23 (1938), 487–496.
[30] V. G. Sprindžuk, *Concerning Baker's theorem on linear forms in logarithms*, Dokl. Akad. Nauk BSSR, 11 (1967), 767–769.
[31] — *Estimates of linear forms with p-adic logarithms of algebraic numbers*, Vesci Akad. Nauk BSSR, Ser. Fiz-Mat. (1968), no. 4, 5–14.
[32] R. Tijdeman, *On the equation of Catalan*, Acta Arith. 29 (1976), 197–209.
[33] M. Waldschmidt, *A lower bound for linear forms in logarithms*, ibid. 37 (1980), 257–283.
[34] E. T. Whittaker and G. N. Watson, *A course of modern analysis*, Reprint of 4th ed., Cambridge Univ. Press, 1969.
[35] G. Wüstholz, *A new approach to Baker's theorem on linear forms in logarithms* I, II, Lecture Notes in Math. 1290 (1987), 189–202, 203–211, III, in: *New advances in transcendence theory, the Proceedings of the Durham Symposium on Transcendental Number Theory, July 1986*, edited by A. Baker, Cambridge Univ. Press, Cambridge 1988, pp. 399–410.
[36] K. R. Yu, *Linear forms in logarithms in the p-adic case*, in: *New advances in transcendence theory, the Proceedings of the Durham Symposium on Transcendental Number Theory, July 1986*, edited by A. Baker, Cambridge Univ. Press, Cambridge 1988, pp. 411–434.
[37] — *Linear forms in the p-adic logarithms*, Max-Planck-Institut für Mathematik, Bonn, MPI/87-20.

MAX-PLANCK-INSTITUT FÜR MATHEMATIK
Gottfried-Claren-Str. 26
D-5300 Bonn 3, Federal Republic of Germany
INSTITUTE OF MATHEMATICS
ACADEMIA SINICA
Beijing 100080, China

Received on 4.6.1987
and in revised form on 12.2.1988 (1728)

ACTA ARITHMETICA
LIII (1989)

Integers with identical digits

by

T. N. SHOREY (Bombay)

In memory of Professor V. G. Sprindžuk

1. For an integer $\nu > 1$, we denote by $\omega(\nu)$ the number of distinct prime factors of ν and we write $\omega(1) = 0$. Let $N > 2$ be an integer. Let $S(N)$ be the set of all integers x with $1 < x < N-1$ such that N has all the digits equal to one in its x-adic expansion. We write $s(N)$ for the number of distinct elements of $S(N)$. Goormaghtigh in 1917 observed that $s(31) = s(8191) = 2$;

$$31 = \frac{2^5-1}{2-1} = \frac{5^3-1}{5-1}, \quad 8191 = \frac{2^{13}-1}{2-1} = \frac{90^3-1}{90-1}.$$

It has been conjectured that

$$(1) \qquad s(N) \leqslant 1, \quad N \neq 31 \quad \text{and} \quad N \neq 8191.$$

A weaker conjecture states that $s(N) \leqslant 1$ whenever N is a prime number different from 31 and 8191. See Dickson [3], p. 703 and Guy [4], p. 45. For $x \in S(N)$, we have

$$(2) \qquad N = \frac{x^\mu - 1}{x-1}$$

and

$$(3) \qquad N-1 = x\frac{x^{\mu-1}-1}{x-1}$$

for some integer $\mu \geqslant 3$. We write

$$(4) \qquad \mu = l(N; x) \geqslant 3.$$

We prove

THEOREM 1. *Let $N > 2$, $N \neq 31$ and $N \neq 8191$ be an integer satisfying $\omega(N-1) \leqslant 5$. There is at most one $y \in S(N)$ such that $l(N; y)$ is an odd integer.*

If N is a prime number, we see from (2) and (4) that $l(N;y)$ is an odd prime number for every $y \in S(N)$. Thus, Theorem 1 confirms (1) for all primes N with $\omega(N-1) \leq 5$. It is known (see [5]) that the number of primes $N \leq Z$ such that $\omega(N-1) \leq 5$ is at least constant times $Z(\log Z)^{-2}$. It is easy to see that $s(N) < \omega(N-1)$ whenever N is prime. In general, we prove

THEOREM 2. *Let $N > 2$ be an integer. Then*

$$s(N) \leq \max(2\omega(N-1)-3, 0), \quad \omega(N-1) \leq 4$$

and

$$s(N) \leq 2\omega(N-1)-4, \quad \omega(N-1) \geq 5.$$

The proofs of our results are elementary. For earlier results, we refer to [7], [2], [1], [10], [11] and [6]. In Section 2, we state notation. The Sections 3 and 4 contain lemmas for the proof of Theorem 1 and the proof of Theorem 1 is completed in Section 5. Finally, Section 6 consists of a proof of Theorem 2.

2. Let $v \geq 1$ be an integer. We refer to Section 1 for the definition of $\omega(v)$. For $v > 1$, we denote by $\omega'(v)$ the number of distinct prime divisors > 2 of v and we put $\omega'(1) = 0$. Furthermore, for $v > 1$, we write $P(v)$ and $\bar{P}(v)$ for the greatest prime divisor and the greatest prime power divisor, respectively, of v and we denote by $\mathrm{Supp}(v)$ the set of prime divisors of v. For an integer $x > 1$, we put

$$\delta(x) = \begin{cases} 1, & x \equiv 0 \pmod 2, \\ 1/2, & x \equiv 1 \pmod 2. \end{cases} \tag{5}$$

For integers $x > 1$ and $v \geq 1$, we write

$$\eta(v;x) = \begin{cases} 1, & (x+1, v) = 1, \\ v, & (x+1, v) > 1 \end{cases} \tag{6}$$

and

$$\eta'(v;x) = \begin{cases} 1, & x+1 \neq v, \\ v, & x+1 = v. \end{cases} \tag{7}$$

For integers $x > 1$ and $v > 1$, we denote

$$A(v;x) = \frac{x^v+1}{x+1}, \quad B(v;x) = \frac{x^v-1}{x-1}, \tag{8}$$

$$A(v;x) < B(v;x) < (1-x^{-1})^{-2} A(v;x), \tag{9}$$

$$A(v;x) < B(v;x) < 3A(v;x). \tag{10}$$

The letter N denotes an integer > 2. For the definitions of $S(N)$ and $l(N;x)$ with $x \in S(N)$, we refer to Section 1. For $x_1 \in S(N)$ and $x_2 \in S(N)$, we observe that

$$l(N;x_1) \neq l(N;x_2), \quad x_1 \neq x_2, \tag{11}$$

and, by (3),

$$\mathrm{ord}_p(x_1) = \mathrm{ord}_p(x_2), \quad p \mid (x_1, x_2) \quad \text{and} \quad p \text{ prime}. \tag{12}$$

The letters y, y_1 and y_2 will denote elements of $S(N)$ such that $l(N;y)$, $l(N;y_1)$ and $l(N;y_2)$ are odd integers. We write

$$n = l(N;y), \quad n_1 = l(N;y_1), \quad n_2 = l(N;y_2), \tag{13}$$

$$m = (n-1)/2, \quad m_1 = (n_1-1)/2, \quad m_2 = (n_2-1)/2. \tag{14}$$

Thus m, m_1 and m_2 are positive integers. By (3) with $x = y$ and $\mu = n$,

$$N-1 = y(y^m+1)B(m;y), \tag{15}$$

$$N-1 = y(y+1)A(m;y)B(m;y). \tag{16}$$

By (2) with $x = y_1, \mu = n_1$ and $x = y_2, \mu = n_2$,

$$N = B(n_1;y_1) = B(n_2;y_2). \tag{17}$$

By (16) with $y = y_1$, $m = m_1$ and $y = y_2$, $m = m_2$,

$$N-1 = y_1(y_1+1)A(m_1;y_1)B(m_1;y_1) = y_2(y_2+1)A(m_2;y_2)B(m_2;y_2). \tag{18}$$

By (17) and (14),

$$y_1^{2m_1} < (1-y_2^{-1})^{-1} y_2^{2m_2}, \quad y_2^{2m_2} < (1-y_1^{-1})^{-1} y_1^{2m_1} \tag{19}$$

which implies that

$$y_1^{2m_1} < 2y_2^{2m_2}, \quad y_2^{2m_2} < 2y_1^{2m_1}. \tag{20}$$

By the left-hand side of (17) and (18), we shall always understand the expressions $B(n_1;y_1)$ and $y_1(y_1+1)A(m_1;y_1)B(m_1;y_1)$, respectively. The latter is equal to $y_1(y_1+1)(y_1^2+1)(y_1^4+1)(y_1^8+1)$, $y_1(y_1+1)(y_1^2+1)(y_1^4+1)$, $y_1(y_1+1)(y_1^2+1)$ and $y_1(y_1+1)$ according as $n_1 = 17$, $n_1 = 9$, $n_1 = 5$ and $n_1 = 3$, respectively and, whenever $n_1 \in \{3, 5, 9, 17\}$, the left-hand side of (18) is replaced by the corresponding expressions without further reference. A similar remark applies to the right-hand side of (18).

3. We shall apply several times the following result on Catalan's equation.

LEMMA 1. *Let $\theta \in \{-1, 1\}$. Suppose that $x > 1$, $\mu > 1$ and $v > 1$ are integers satisfying $x^\mu - 2^v = \theta$. Then $\theta = 1$, $x = v = 3$ and $\mu = 2$.*

The proof of Lemma 1 is clear.

As an immediate consequence of Lemma 1, we have

Corollary 1. *Let $x > 1$ be an integer satisfying $\omega(x(x+1)) = 2$. If x is odd, then x is a prime number and $x+1$ is a power of 2. If $x \neq 8$ is even, then $x+1$ is a prime number and x is a power of 2.*

Let m, n, $\eta(m; y)$, $\eta'(m; y)$, A and B be given by (13), (14), (6), (7) and (8). We prove

Lemma 2. *Let $N > 2$ be an integer. Suppose that $y \in S(N)$ such that $l(N; y) \geqslant 7$ is an odd integer. Then*

(a) *Either $N = 127$ or*

$$\omega(N-1) \geqslant \omega(y(y+1))+2. \tag{21}$$

(b) *Suppose that $m \neq 4$ and $\omega(N-1) = \omega(y(y+1))+2$. Then m is a prime number and*

$$\omega\left(\frac{A(m; y)}{\eta(m; y)}\right) = \omega(B(m; y)) = 1.$$

Proof. We observe that $m \geqslant 3$. For an integer v, we derive from Lemma 1 that

$$\omega'(y^v+1) > 0, \quad v \geqslant 2, \tag{22}$$

$$\omega'(B(v; y)) > 0, \quad v \geqslant 3. \tag{23}$$

By (15), we have

$$\omega(N-1)-1 = \omega'(N-1) = \omega'(y)+\omega'(y^m+1)+\omega'(B(m; y)). \tag{24}$$

(a) It is easy to see that

$$\omega'(y^m+1) \geqslant \omega'(y+1)+1, \quad m \text{ odd and } N \neq 127, \tag{25}$$

$$\omega'(B(m; y)) \geqslant \omega'(y+1)+1, \quad m \text{ even}. \tag{26}$$

Now, we combine (24), (25), (26), (22) and (23) to obtain (21) whenever $N \neq 127$.

(b) Suppose that $m \neq 4$ and $\omega(N-1) = \omega(y(y+1))+2$ which, together with (24), implies that

$$\omega'(y^m+1)+\omega'(B(m; y)) = \omega'(y+1)+2. \tag{27}$$

Let m be even. Then, we see from (27), (26) and (22) that $\omega'(y^m+1) = 1$ which implies that $m \geqslant 8$ is a power of 2. Then $\omega'(B(m; y)) \geqslant \omega'(y+1)+2$ which, by (27), gives $\omega'(y^m+1) = 0$ contradicting (22). Thus, we conclude that m is an odd integer. Then, since $N \neq 127$, we combine (27), (25) and (23) to derive that $\omega(B(m; y)) = \omega'(B(m; y)) = 1$ which implies that m is a prime number. Further, we see from (27) that $\omega(y^m+1) = \omega(y+1)+1$ and hence, $\omega(A(m; y)/\eta(m; y)) = 1$. ∎

Lemma 3. *Let $N > 2$ be an integer satisfying $\omega(N-1) = 5$. Let $y \in S(N)$ such that $l(N; y) \geqslant 7$ is an odd integer and $\omega(y(y+1)) = 2$. Then*

(a) *Suppose that m is different from 4, 6, 8 and 9. Then m is a prime number. Furthermore*

$$\omega\left(\frac{A(m; y)}{\eta'(m; y)}\right) = 1 \quad \text{or} \quad \omega(B(m; y)) = 1. \tag{28}$$

(b) *If $m = 6$ or $m = 9$, then $y = 2$.*

Proof. Observe that $m \geqslant 3$ and $N \neq 127$.

(a) First, we consider the case that y is odd. By (24) with $\omega(N-1) = 5$,

$$\omega'(y^m+1)+\omega'(B(m; y)) = 3$$

which, together with (22) and (23), implies that either

$$\omega'(y^m+1) = 1, \quad \omega'(B(m; y)) = 2 \tag{29}$$

or

$$\omega'(y^m+1) = 2, \quad \omega'(B(m; y)) = 1. \tag{30}$$

Now, we argue, as in Lemma 2 (b), to obtain the assertion of the lemma if either (29) or (30) is valid.

Thus, we may suppose that y is even. Then y is a power of 2 and, by (24) with $\omega(N-1) = 5$, we have

$$\omega(y^m+1)+\omega(B(m; y)) = 4. \tag{31}$$

We may assume that $\omega(B(m; y)) \geqslant 2$. Further, since $N \neq 127$, we see that $\omega(y^m+1) = 1$ implies that m is a power of 2 and therefore, since $m \neq 4$ and $m \neq 8$, we see that $\omega(B(m; y)) \geqslant 4$. Consequently, we derive from (31) that

$$\omega(y^m+1) = 2, \tag{32}$$

$$\omega(B(m; y)) = 2. \tag{33}$$

First, we show that m is prime. If $y \neq 2$ and $y \neq 8$, we see from Corollary 1 that $y = z^2$ for some integer $z > 1$ and then,

$$\omega(B(m; y)) = \omega(A(m; z))+\omega(B(m; z)).$$

Therefore, by (33), $\omega(B(m; z)) = 1$ which implies that m is prime. Thus, we may suppose that either $y = 2$ or $y = 8$. If m is even, we see from (33) that $\omega(2^{m/2}+1) = 1$ if $y = 2$ and $\omega(8^{m/2}+1) = 1$ if $y = 8$ and this, by Lemma 1 and $m \neq 6$, is not possible. If m is odd, we argue, as above, to derive from (32) and $m \neq 9$ that m is prime.

Next, we prove (28). In view of (32), we may suppose that $(y+1, m) > 1$ and $y+1 \neq m$. Now, we apply Corollary 1 to conclude that $y = 8$ and $m = 3$. Then (28) is valid, since $B(3; 8) = 73$ is prime.

(b) Suppose that $m = 6$. Notice that $\omega'(y^6+1) \geqslant 2$ and $\omega'(B(6; y)) \geqslant 2$. Then, we see from (24) with $\omega(N-1) = 5$ that y is even and (32) and (33) are valid. Consequently, since $\omega(8^6+1) \geq 3$, we derive that $y \neq 8$. If $y \neq 2$, we conclude from an argument of Lemma 3(a) that $y = z^2$ with an integer $z > 1$ and $\omega(B(6; z)) = 1$ which is not possible. Thus $y = 2$. The proof for the case $m = 9$ is similar, since $\omega(8^9+1) \geq 3$. ∎

4. This section contains remaining lemmas for the proof of Theorem 1. Ramanujan [9] conjectured that

$$2^n - 7, \quad n = 3, 4, \ldots \tag{34}$$

is a square only if $n \in \{3, 4, 5, 7, 15\}$. Thus $1^2, 3^2, 5^2, (11)^2$ and $(181)^2$ are the only squares in (34). Nagell [8] confirmed this conjecture. We start with an application of this result.

Lemma 4. *Let $x_1 > 1$ and $x_2 > 1$ be integers. Let $\mu_1 \geq 11$ be an odd integer and put $v_1 = (\mu_1 - 1)/2$. Then*

$$B(\mu_1; x_1) = B(7; x_2) \tag{35}$$

implies that

$$B(v_1; x_1) \neq B(3; x_2).$$

Proof. Suppose that (35) is valid and

$$B(v_1; x_1) = B(3; x_2). \tag{36}$$

Then $x_2 > x_1$. If $x_1 = 2$, we re-write (36) as

$$(2x_2+1)^2 + 7 = 2^{v_1+2}$$

to apply the above mentioned result of Nagell to conclude that either $v_1 = 5$, $x_2 = 5$ or $v_1 = 13$, $x_2 = 90$ and then, (35) is not satisfied. Thus, we may assume that $x_1 \geq 3$ and $x_2 \geq 4$. Then, we derive from (35) and (36) that

$$2x_2^6 < 3x_1^{2v_1}, \quad 3x_1^{v_1-1} < 4x_2^2.$$

Therefore, since $v_1 \geq 5$, we see that

$$x_2^3 < 2x_2^{2v_1/(v_1-1)} \leq 2x_2^{5/2}$$

which implies that $x_2 < 4$ and this is a contradiction. ∎

Let m_1, m_2, n_1, n_2, A and B be given by (13), (14) and (8).

Lemma 5. *Let $N > 2$ be an integer. Suppose that y_1 and y_2 are elements of $S(N)$ such that $l(N; y_2) = 3$. Then $l(N; y_1) \neq 5$ whenever $N \neq 31$. Furthermore, $l(N; y_1) \neq 9$.*

Proof. Assume that $N \neq 31$ and $l(N; y_1) = 5$. Then, we see from (17) with $n_1 = 5$, $n_2 = 3$ that $y_1 \neq 2$ and

$$Y^2 = 4(y_1^4 + \ldots + y_1) + 1, \quad Y = 2y_2 + 1.$$

Therefore, since $y_1 \neq 2$, we obtain

$$2y_1^2 + y_1 < Y < 2y_1^2 + y_1 + 1$$

which is a contradiction. The proof for $l(N; y_1) \neq 9$ is similar. ∎

Next, as an immediate consequence of Lemma 3 (b) and simple computations, we obtain the following result whose proof is clear.

Lemma 6. *Let $N > 2$ be an integer satisfying $\omega(N-1) = 5$. Suppose that y_1 and y_2 are distinct elements of $S(N)$ satisfying $\omega(y_1(y_1+1)) = 2$ such that $l(N; y_1)$ and $l(N; y_2)$ are odd integers. Then*

(a) *If $N = 8191$, then $y_1 = 2$, $y_2 = 90$, $l(N; y_1) = 13$ and $l(N; y_2) = 3$.*

(b) *Suppose that $N \neq 8191$. Then $l(N; y_1) \neq 13$ and $l(N; y_2) \neq 19$.*

Lemma 7. *Let $N > 2$ be an integer satisfying $\omega(N-1) \leq 5$. Suppose that y_1 and y_2 are distinct elements of $S(N)$ satisfying $\omega(y_1(y_1+1)) = \omega(y_2(y_2+1)) = 2$ such that $l(N; y_1)$ and $l(N; y_2)$ are odd integers. Then $l(N; y_1) \neq 9$ and $l(N; y_2) \neq 9$.*

Proof. There is no loss of generality in assuming that $n_1 = 9$. Observe that $\omega(N-1) \geq 4$, $m_1 = 4$, $m_2 > 1$ and $m_2 \neq 4$. Let $m_2 = 2$. If y_1 is even, we count the power of 2 on both the sides of (18) with $m_1 = 4$, $m_2 = 2$ to conclude that $y_1 = 2(y_2+1)$ and thus $y_1 \geq y_2$ which is not possible. If y_1 is odd, then, as above, we see that either $4(y_1+1) = y_2$ or $4(y_1+1) = 2(y_2+1)$ which, by (17) with $n_1 = 9$, $n_2 = 5$, imply that either $y_1 | 340$ or $y_1 | 4$ and this, by Corollary 1, is not possible. Thus $m_2 \neq 2$. Let $m_2 = 8$. Then $\omega(N-1) = 5$ and each of the factors on the right-hand side of (18) with $m_1 = 4$, $m_2 = 8$ is a prime power or twice of a prime power. Now, we see from (18) and (20) with $m_1 = 4$, $m_2 = 8$ that $\omega'(y_1^4+1) = \omega'(y_1^2+1) = 1$ which implies that $\omega(N-1) = 4$. Thus $m_2 \neq 8$. Further, we see from Lemma 6 that $m_2 \neq 6$ and $m_2 \neq 9$ whenever $\omega(N-1) = 5$. Now, we apply Lemmas 2 and 3 to conclude that m_2 is an odd prime.

If y_1 is even, we count the power of 2 on both the sides of (18) with $m_1 = 4$ to conclude that $y_1 = y_2 + 1$ which, by (17) with $n_1 = 9$, implies that $y_2 | 8$ and this is a contradiction. Suppose that y_1 is odd. Then, as above, either $4(y_1+1) = y_2$ or $4(y_1+1) = y_2+1$. Thus $y_2 > y_1$ which implies that $n_2 = 7$. Now, we see from (17) with $n_1 = 9$, $n_2 = 7$ that y_1 divides $B(6; 4)$ or $3B(6; 3)$. Then we apply Corollary 1 to conclude that either $y_1 = 3$, $y_2 = 16$ or $y_1 = 7$, $y_2 = 31$ and now, (17) with $n_1 = 9$, $n_2 = 7$ is not satisfied. ∎

Lemma 8. *Let $N > 2$ be an integer satisfying $\omega(N-1) \leq 5$. Suppose that y_1 and y_2 are distinct elements of $S(N)$ satisfying $\omega(y_1(y_1+1)) = 2$ such that $l(N; y_1)$ and $l(N; y_2)$ are odd integers. Then $l(N; y_1) \neq 9$ and $l(N; y_2) \neq 9$.*

Proof. We may assume that either $m_1 = 4$ or $m_2 = 4$. Then $\omega(N-1) \geq 4$. First, we consider the case that $\omega(y_2(y_2+1)) \neq 3$. By Lemma 7, $\omega(y_2(y_2+1)) \in \{4, 5\}$. If either $\omega(N-1) = 4$ or $\omega(N-1) = 5$, $\omega(y_2(y_2+1)) = 5$, then $m_1 = 4$, $m_2 = 1$ which contradicts Lemma 5. Therefore $\omega(N-1) = 5$ and

$\omega(y_2(y_2+1)) = 4$ which implies that $m_1 = 4$, $m_2 = 2$, $\omega'(y_2^2+1) = 1$. Now, we apply (18) and (20) with $m_1 = 4$, $m_2 = 2$, to derive that

$$\delta(y_1)(y_1^4+1) = \delta(y_2)(y_2^2+1) \tag{37}$$

where $\delta(y_1)$ and $\delta(y_2)$ are given by (5). By (18), $\delta(y_1) \neq \delta(y_2)$. If $\delta(y_1) = \frac{1}{2}$, then $\delta(y_2) = 1$ and (37) is not satisfied. Thus, $\delta(y_1) = 1$, $\delta(y_2) = \frac{1}{2}$ which, together with (18) and (20) with $m_1 = 4$, $m_2 = 2$, implies that $2y_1^4 < y_2^2 < \sqrt{2}\, y_1^4$ and this is a contradiction. Therefore, $\omega(y_2(y_2+1)) = 3$. Then $y_2 \geqslant 5$. If $\omega(N-1) = 4$ then $m_1 = 4$, $m_2 = 2$, $\omega'(y_1^4+1) = \omega'(y_2^2+1) = 1$ and consequently, we obtain (37) which leads to a contradiction. Hence, we conclude that $\omega(N-1) = 5$.

First, we suppose that $m_1 = 4$. Then $y_1 \geqslant 5$ and $y_1 \neq 8$, since $\omega(N-1) = 5$. Observe that $m_2 > 1$. Let $m_2 = 2$. Then $y_2 \geqslant 12$, since $\omega(N-1) = 5$. Further, we see from (18) with $m_1 = 4$, $m_2 = 2$ that $3 \nmid y_2(y_2+1)$, otherwise $3 | y_1(y_1+1)$ which, by Corollary 1, implies that $y_1 = 2$, $y_1 = 3$ or $y_1 = 8$ and this is not possible. If $\omega'(y_1^4+1) = 1$, then $\omega'(y_2^2+1) = 1$ and $\omega(N-1) = 4$. Thus

$$\omega'(y_1^2+1) = 1, \quad \omega'(y_1^4+1) = 2. \tag{38}$$

Let y_1 and y_2 be even. Then, we count the power of 2 on both the sides of (18) with $m_1 = 4$, $m_2 = 2$ to observe that y_1 divides y_2. We write

$$y_2 = y_1 z. \tag{39}$$

Then, we see that $\omega(y_2+1) = 1$ and

$$1 < z < 2y_1 \tag{40}$$

is a power of an odd prime. Now, we show that

$$z = y_1+1. \tag{41}$$

By (18) and (39), it suffices to show that $(z, y_1^2+1) = (z, y_1^4+1) = 1$. If $(z, y_1^2+1) > 1$, then $z = y_1^2+1$ which contradicts (40). Suppose that $(z, y_1^4+1) > 1$. Then $(y_1^4+1)/z$ is a prime power $> y_2+1$. Therefore $(y_1^4+1)/z$ divides y_2^2+1. Since $y_1^2+1 \neq y_2+1$, we see from (18) with $m_1 = 4$, $m_2 = 2$, (38), (39) and (40) that y_1^2+1 divides y_2^2+1. Consequently,

$$(y_1^2+1)\left(\frac{y_1^4+1}{z}\right) \leqslant y_2^2+1$$

which, by (20) and (40), is not possible. This proves (41) which, together with (39), implies that $y_2 = y_1(y_1+1)$. Then $3 | y_2(y_2+1)$ which is a contradiction. The other cases can be dealt with similarly. Hence, we conclude that $m_2 \neq 2$. Since $m_2 \neq 4$ and $N \neq 127$, we derive from Lemma 2 that m_2 is an odd prime. If $m_2 \geqslant 5$, then $y_1 > y_2$ and we count the power of 2 on both the sides of (18) with $m_1 = 4$ to conclude that y_1 is even and $y_1 = y_2+1$ which, by (17) with $n_1 = 9$, implies that $y_2 | 8$ and this is a contradiction. Consequently, we conclude that $m_2 = 3$. If $3 | (y_2+1)$, then $9 | y_1(y_1+1)$ which, by Corollary 1 and $y_1 \neq 8$, is not possible. Thus $\eta(3; y_2) = 1$ and we refer to Lemma 2 to derive that $A(3; y_2)$ and $B(3; y_2)$ are distinct prime powers which, since $y_2 > y_1$, exceed y_1^2+1. Hence, we conclude from (18) with $m_1 = 4$, $m_2 = 3$ that

$$\delta(y_1)(y_1^4+1) = A(3; y_2) B(3; y_2)$$

which, since $y_2 > y_1$, is not possible.

Now, we turn to the case that $m_2 = 4$. It is easy to observe that $m_1 \notin \{1, 2, 4, 6, 8, 9\}$ and hence, by Lemma 3, we conclude that m_1 is an odd prime. Let $y_1 = 2$. Then $m_1 \geqslant 5$ and y_2 is even. Now, by Lemma 3, either $y_2^4+1 = A(m_1; y_1)$ or $y_2^4+1 = B(m_1; y_1)$. Consequently, $y_1 | y_2^4$ and $4\, \mathrm{ord}_p(y_2) = \mathrm{ord}_p(y_1)$ for every prime $p | (y_1, y_2)$. This contradicts (12). Thus $y_1 \neq 2$. Similarly $y_1 \neq 3$ and so $y_1 \geqslant 4$. Further $(y_2^4+1)/2 \leqslant B(m_1; y_1) < 3y_1^{m_1-1}/2$ and $y_1^{2m_1} < 5y_2^8/4$, since $y_2 \geqslant 5$. Consequently, we derive that $y_1 < 3(5/4)^{1/2} \leqslant 4$ which is a contradiction. ∎

LEMMA 9. *Let $N > 2$ be an integer satisfying $\omega(N-1) \leqslant 5$. Suppose that y_1 and y_2 are distinct elements of $S(N)$ such that $l(N; y_1)$ and $l(N; y_2)$ are odd integers. Then $l(N; y_1) \neq 17$ and $l(N; y_2) \neq 17$.*

Proof. There is no loss of generality in assuming that $m_1 = 8$. Then $\omega(N-1) = 5$, $\omega(y_1(y_1+1)) = 2$ and each of the factors on the left-hand side of (18) with $m_1 = 8$ is either a prime power or twice of a prime power. Further, we derive from our lemmas that m_2 is an odd prime number and $\omega(y_2(y_2+1)) \in \{2, 3\}$.

Let $\omega(y_2(y_2+1)) = 2$. We count the power of 2 on both the sides of (18) with $m_1 = 8$ to conclude that y_1 is odd and either $8(y_1+1) = y_2$ or $8(y_1+1) = y_2+1$. Thus $y_2 > y_1$ which implies that $m_2 \in \{3, 5, 7\}$. In particular, $y_2+1 \neq m_2$ and then, by Lemma 3,

$$\omega(A(m_2; y_2)) = 1 \quad \text{or} \quad \omega(B(m_2; y_2)) = 1.$$

Suppose that $\omega(B(m_2; y_2)) = 1$. Then $\omega(A(m_2; y_2)) = 2$. Furthermore,

$$\bar{P}(N-1) = (y_1^8+1)/2 = B(m_2; y_2), \quad A(m_2; y_2) \leqslant (y_1^4+1)(y_1^2+1)/4$$

which, together with (10), imply that $y_1^8+1 < 3(y_1^4+1)(y_1^2+1)/2$ and this is a contradiction. If $\omega(A(m_2; y_2)) = 1$, we secure similarly a contradiction.

Thus, we may suppose that $\omega(y_2(y_2+1)) = 3$. Then $y_2 \geqslant 5$. By (18) with $m_1 = 8$ and Lemma 2,

$$\bar{P}(N-1) = \delta(y_1)(y_1^8+1) = B(m_2; y_2)$$

and

$$y_1(y_1+1)(y_1^2+1)(y_1^4+1) = \delta(y_1) y_2(y_2+1) A(m_2; y_2).$$

Therefore, since $y_2 \geqslant 5$, we derive that

$$\delta(y_1) y_1^8 < 5y_2^{m_2-1}/4, \quad \delta(y_1) y_2^{m_2+1} < 5y_1^8/2$$

which imply that $2y_2^2 < 25$ and this is not possible. ∎

LEMMA 10. *Let $N > 2$ and $N \neq 31$ be an integer. Suppose that y_1 and y_2 are distinct elements of $S(N)$ such that $(l(N; y_1)-1)/2$ is a prime number and $l(N; y_2) = 3$. Then $\omega(N-1) \geqslant 6$.*

Proof. We suppose that $\omega(N-1) \leqslant 5$. Since $N \neq 31$, we see from Lemma 5 that $m_1 > 2$. Then, since $N \neq 127$ may be assumed, we derive from Lemma 2 that $\omega(N-1) \geqslant 4$ and

$$\omega(y_1(y_1+1)) = 2 \quad \text{or} \quad \omega(y_1(y_1+1)) = 3. \tag{42}$$

As in the proof of Lemma 4, we apply a theorem of Nagell to conclude that $y_1 > 2$. We shall apply (18) with $m_2 = 1$ and (19) with $m_2 = 1$, $y_1 > 2$ without reference in the proof of Lemma 10. Let $\eta' = \eta'(m_1; y_1)$ be given by (7). We put

$$\psi = \begin{cases} 1, & \omega(y_1(y_1+1)) = 3, \\ \eta', & \omega(y_1(y_1+1)) = 2. \end{cases}$$

By Lemmas 2 and 3, there exist $v \in \{0, 1\}$ and a prime power

$$Q_v \in \{A(m_1; y_1)/\psi, B(m_1; y_1)\} := U$$

such that

$$y_2 + v = q_v Q_v \tag{43}$$

where q_v is a positive integer satisfying $(q_v, Q_v) = 1$ and

$$1 < q_v < (2y_1 - 1)\psi. \tag{44}$$

Let $v_1 \in \{0, 1\}$, $v_1 \neq v$ and $Q_{v_1} \in U$, $Q_{v_1} \neq Q_v$.

First, we consider the case that $\psi = 1$. If $q_v = y_1$, then we see from (43) that $y_2 + v_1 = (y_1+1)Q_{v_1}$ and

$$y_1(Q_v - Q_{v_1}) - Q_{v_1} = v - v_1;$$

thus $Q_{v_1} \equiv \pm 1 \pmod{y_1^2}$ which is not possible since $y_1 > 2$. Thus $q_v \neq y_1$. Similarly $q_v \neq y_1 + 1$. Let $\omega(y_1) = 1$. Then, by (44) and $q_v \neq y_1$, we observe that $(q_v, y_1) = 1$. Thus $y_2 + v_1 \equiv 0 \pmod{y_1}$. Also, by (43), $y_2 + v \equiv q_v \pmod{y_1}$. Consequently $q_v \equiv v - v_1 \pmod{y_1}$. Now, by (44) and $q_v \neq y_1 + 1$, we see that $v = 0$ and $q_0 = y_1 - 1$. Thus $y_2 + 1 = (y_1 - 1)Q_0 + 1$. If $\omega(B(m_1; y_1)) = 1$, we can take $Q_0 = B(m_1; y_1)$ and then, $y_2 + 1 = y_1^{m_1}$ which implies that $m_1 = 1$. Therefore, $\omega(B(m_1; y_1)) > 1$. Then $Q_0 = A(m_1; y_1)$ and $\omega(y_1(y_1+1)) = 2$. Now, we see that $(y_1 - 1) | B(m_1; y_1)$ which implies $y_1 - 1 = m_1$. Now, we verify that $y_1 \neq 4$ and $y_1 \neq 8$, since $\omega(A(7; 8)) > 1$. Consequently, $y_1 = 2^p$ for some prime $p \geqslant 5$ and $y_1 + 1 = 2^p + 1$ is prime. This is a contradiction. Thus, we may assume that $\omega(y_1) > 1$. Then, we derive from (42) that $\omega(y_1(y_1+1)) = 3$ and $\omega(y_1+1) = 1$. Now, we apply Lemma 2 to observe that $\omega(Q_{v_1}) = 1$ and

$$y_2 + v_1 = q_{v_1} Q_{v_1} \tag{45}$$

where q_{v_1} is an integer satisfying

$$(q_{v_1}, Q_{v_1}) = 1, \quad 1 < q_{v_1} < 2y_1 - 1. \tag{46}$$

We argue, as above, to show that $q_{v_1} \neq y_1 + 1$. By (43) and (45), we see that $q_v q_{v_1} = y_1(y_1+1)$ which, since $\omega(y_1+1) = 1$, implies that either $(y_1+1) | q_v$ or $(y_1+1) | q_{v_1}$. Now, we refer to (44) and (46) to conclude that either $q_v = y_1 + 1$ or $q_{v_1} = y_1 + 1$. This is again a contradiction.

Now, we turn to the case that $\psi \neq 1$. Then $\omega(y_1(y_1+1)) = 2$ and $\psi = \eta' = m_1 = y_1 + 1$. Then $y_1 = z_1^2$ for some integer $z_1 \geqslant 4$, since $y_1 \neq 4$ and $y_1 \neq 8$. Thus $m_1 \geqslant 17$ and

$$B(m_1; y_1) = A(m_1; z_1)\, B(m_1; z_1). \tag{47}$$

Then $\omega(N-1) = 5$ and each of the factors on the right-hand side of (47) is a prime power $> (2y_1 - 1)\psi$. Then, we see from (44) and (47) that $Q_{v_1} = B(m_1; y_1)$ and $(Q_{v_1}, y_2 + v) = 1$. Then, (45) and (46) are valid and, as earlier, $q_{v_1} \neq y_1$ and $q_{v_1} \neq y_1 + 1$. Consequently, since $\omega(y_1(y_1+1)) = 2$, we derive from (46) that $(q_{v_1}, y_1) = 1 = (q_{v_1}, y_1 + 1) = 1$. Thus $q_{v_1} = 1$ which contradicts (46). ∎

LEMMA 11. *Let $N > 2$, $N \neq 31$ and $N \neq 8191$ be an integer satisfying $\omega(N-1) \leqslant 5$. Suppose that y_1 and y_2 are distinct elements of $S(N)$ satisfying $\omega(y_1(y_1+1)) = 2$ such that $l(N; y_1)$ and $l(N; y_2)$ are odd integers. Then $(l(N; y_1)-1)/2$ and $(l(N; y_2)-1)/2$ are odd prime numbers.*

Proof. We may assume that $N \neq 127$. Either $m_1 > 1$ or $m_2 > 1$ which implies that $\omega(N-1) \geqslant 3$ and $m_1 > 1$. If $\omega(N-1) = 3$, then $m_1 = 2$, $m_2 = 1$ which is excluded by Lemma 5. Thus, either $\omega(N-1) = 4$ or $\omega(N-1) = 5$. By Lemmas 8 and 9, $m_1, m_2 \notin \{4, 8\}$. Further, by Lemma 6, $m_1 \notin \{6, 9\}$ and $m_2 \notin \{6, 9\}$ whenever $\omega(y_2(y_2+1)) = 2$. Now, we apply Lemmas 2, 3 and 10 to conclude that m_1 and m_2 are prime numbers. If $m_1 = 2$, we count the power of 2 on both the sides of (18) with $m_1 = 2$ to arrive at a contradiction. Similarly, we derive that $m_2 \neq 2$ whenever $\omega(y_2(y_2+1)) = 2$. Further, we argue, as earlier, to conclude that $\omega'(y_2^2+1) > 1$ whenever $m_2 = 2$.

Thus, we may suppose that $m_2 = 2$, $\omega(y_2(y_2+1)) > 2$ and $\omega'(y_2^2+1) \geqslant 2$. Then $\omega(N-1) = 5$, $\omega(y_2(y_2+1)) = 3$, $\omega'(y_2^2+1) = 2$ and $y_2 \geqslant 12$. Let $y_1 = 2$. Then $m_1 \geqslant 5$, since $N \neq 127$. Further, since the left-hand side of (18) with $m_2 = 2$ is not divisible by 4 as well as 9 and $3 \nmid (y_2^2+1)$, we see that $\omega(y_2(y_2+1)) \geqslant 4$. Thus $y_1 \neq 2$. Similarly $y_1 = 3$ implies that $y_2 = 12$ which is easy to exclude. Similarly, we verify to exclude the possibilities $y_1 \in \{4, 7, 8\}$ whenever $m_1 = 3$ or $m_1 = 5$. Thus $y_1 \geqslant 4$ and, since $\omega(y_1(y_1+1)) = 2$, we observe that $y_1 \geqslant 16$ whenever $m_1 = 3$ or $m_1 = 5$. We shall utilise these observations and (18) with $m_2 = 2$, (19) with $m_2 = 2$, $y_2 > y_1$, $y_1 \geqslant 4$ and $y_1 \geqslant 16$ whenever $m_1 = 3$ or $m_1 = 5$ in the subsequent argument of this lemma without reference. First, we consider the case that $\eta' = 1$ where $\eta' = \eta'(m_1; y_1)$

is given by (7). Put $V = \{A(m_1; y_1), B(m_1; y_1)\}$. There exists a prime power $R_2 \in V$ such that

$$\delta(y_2)(y_2^2+1) = r_2 R_2 \tag{48}$$

where r_2 is a positive integer such that $\omega(r_2) = 1$, $(r_2, R_2) = 1$ and

$$r_2 < 2\delta(y_2)y_1. \tag{49}$$

Observe that $r_2 \equiv 1 \pmod 4$. Now, since $\omega(y_1(y_1+1)) = 2$, we derive that $r_2 \neq y_1$. If $r_2 = y_1+1$, we see from (49) that $\delta(y_2) = 1$ and then, as in Lemma 8, (48) and (12) lead to a contradiction. Then r_2 divides R_1 where $R_1 \in V$ such that $R_1 \neq R_2$ and $\omega(R_1 r_2^{-1}) = 1$. Further

$$\delta(y_2) y_1 (y_1+1) R_1 r_2^{-1} = y_2(y_2+1) \tag{50}$$

and

$$y_1(y_1+1) \leqslant 2(y_2+1) \quad \text{or} \quad y_1 R_1 r_2^{-1} \leqslant 2(y_2+1). \tag{51}$$

By (50) and $\omega(R_1 r_2^{-1}) = 1$, we derive that $R_1 r_2^{-1} \leqslant y_2+1$ which implies that $m_1 = 3$ and in this case, (51) is not satisfied.

Next, we turn to the case that $\eta' \neq 1$. Then $\eta' = m_1 = y_1+1$. Therefore $y_1 = z_1^2$, $z_1 \geqslant 4$, $m_1 \geqslant 17$ and the factors on the right-hand side of (47) are distinct prime powers. Then, by Lemma 3, $A(m_1; y_1)/\eta'$ is a prime power $> y_2+1$ and hence, it divides y_2^2+1. Now, neither of the factors on the right-hand side of (47) can divide y_2^2+1, otherwise

$$A(m_1; z_1) A(m_1; y_1) \leqslant \eta'(y_2^2+1)$$

which is not possible. Further, we notice that each of the factors on the right-hand side of (47) is less than y_2. Finally, one of these factors occurs in the factorisation of y_2 and the other in the factorisation of y_2+1. Consequently, $\omega(y_2(y_2+1)) \geqslant 4$ which is a contradiction. ∎

Lemma 12. *Let $N > 2$ be an integer satisfying $\omega(N-1) \leqslant 5$. There is at most one $y \in S(N)$ such that $\omega(y(y+1)) = 2$ and $l(N; y)$ is an odd integer.*

Proof. By Lemma 11, we may assume that y_1 and y_2 are distinct elements of $S(N)$ satisfying $\omega(y_i(y_i+1)) = 2$, $i = 1, 2$ and m_1, m_2 are odd prime numbers. We count the power of 2 on both the sides of (18) to conclude that $y_1 \not\equiv y_2 \pmod 2$. Now, there is no loss of generality in assuming that y_1 is even and y_2 is odd. Then

$$y_1 = y_2+1 \tag{52}$$

which, together with (17) and Lemma 1, implies that $y_1 \geqslant 6$. If $y_1 = 8$, then $m_1 = 3$ and the lemma can be verified. Thus $y_1 = z_1^2$ where $z_1 = 2^{2^{v-1}}$ for some integer $v \geqslant 2$. Then (47) is valid, the factors on the right-hand side of (47) are distinct prime powers and $\omega(N-1) = 5$. Further, they are less than

$A(m_1; y_1)/\eta'$ where $\eta' = \eta'(m_1; y_1)$ is given by (7). Each of these factors is coprime to y_2+1. If either of these factors is equal to y_2, we see that $y_2+1 \not\equiv 0 \pmod 4$ which implies that $y_2+1 = 2$ and this is a contradiction.

Now, we apply Lemma 3 to conclude that

$$\bar{P}(N-1) = A(m_1; y_1)/\eta'$$

and

$$\bar{P}(N-1) = A(m_2; y_2) \quad \text{or} \quad \bar{P}(N-1) = B(m_2; y_2).$$

Suppose that $\bar{P}(N-1) = A(m_2; y_2)$. Then

$$A(m_1; y_1)/\eta' = A(m_2; y_2).$$

Further, since $\omega(N-1) = 5$, we see that $\omega(B(m_2; y_2)) = 2$ and therefore

$$B(m_1; y_1) = B(m_2; y_2). \tag{53}$$

By (17), (53) and (52), we see that $y_2 | 2m_1$ and $y_2 | (m_1-1)$ which, since y_2 is odd, imply that $y_2 = 1$. Thus, we may assume that $\bar{P}(N-1) = B(m_2; y_2)$. Then

$$A(m_1; y_1)/\eta' = B(m_2; y_2), \quad B(m_1; y_1) = A(m_2; y_2).$$

Therefore

$$B(m_1; y_1) < A(m_1; y_1)/\eta' \leqslant A(m_1; y_1)$$

which is a contradiction. ∎

Lemma 13. *Let $N > 2$, $N \neq 31$ and $N \neq 8191$ be an integer satisfying $\omega(N-1) \leqslant 5$. Suppose that y_1 and y_2 are distinct elements of $S(N)$ such that $l(N; y_1)$ and $l(N; y_2)$ are odd integers. Then*

$$\omega(y_1(y_1+1)) \geqslant 3 \quad \textit{and} \quad \omega(y_2(y_2+1)) \geqslant 3.$$

Proof. By Lemma 12, we may assume that $\omega(y_1(y_1+1)) = 2$ and $\omega(y_2(y_2+1)) \geqslant 3$. Further, we apply Lemmas 11 and 2 to derive that m_1, m_2 are odd primes and $\omega(N-1) = 5$, $\omega(y_2(y_2+1)) = 3$, $y_2 \geqslant 5$. If $m_1 = 3$, we derive, as earlier, that y_1 is even, $y_1 = y_2+1$ and $y_2 | 6$ which imply that $y_2 = 3$ and this is a contradiction.

Thus, we may assume that $m_1 \geqslant 5$. Then $y_1 \neq 8$, otherwise $\omega(N-1) > 5$. Let $\eta' = \eta'(m_1; y_1)$ and $\eta = \eta(m_2; y_2)$ be given by (7) and (6). Then, we observe from (18) and Corollary 1 that

$$\eta(3; y_2) = 1. \tag{54}$$

Then, by (19), (54) and $y_2 \geqslant 5$,

$$A(m_2; y_2)/\eta > (y_1+1)^2. \tag{55}$$

By Lemmas 2 and 3,

$$\bar{P}(N-1) = B(m_2; y_2) \tag{56}$$

and

(57) $\bar{P}(N-1) = A(m_1; y_1)/\eta'$ or $\bar{P}(N-1) = B(m_1; y_1)$.

First, suppose that

(58) $\bar{P}(N-1) = B(m_1; y_1)$.

Then, by (56) and (57),

(59) $B(m_1; y_1) = B(m_2; y_2)$

which, together with (18), implies that

(60) $$y_1(y_1+1)\eta' \frac{A(m_1; y_1)}{\eta'} = y_2(y_2+1)\eta \frac{A(m_2; y_2)}{\eta}.$$

By Lemma 2 and (55), the last factor on the right-hand side of (60) is a prime power dividing the last factor on the left-hand side of (60). If $\eta = m_2$, then we see from (54), (60) and Corollary 1 that $m_2 \geqslant 5$ and $(y_1(y_1+1), m_2) = 1$. Consequently,

(61) $$\frac{A(m_2; y_2)}{\eta} \text{ divides } \frac{A(m_1; y_1)}{\eta^2\eta'}.$$

Therefore

(62) $$A(m_2; y_2) < \frac{A(m_1; y_1)}{\eta\eta'}.$$

We combine (62), (59), (9) and $y_2 \geqslant 5$ to obtain

$$A(m_2; y_2) < 2A(m_2; y_2)/\eta\eta'$$

which implies that

(63) $\eta = \eta' = 1$.

Then

(64) $A(m_1; y_1) = A(m_2; y_2)$;

otherwise, by (61), (63), (59), (9) and $y_2 \geqslant 5$,

$$A(m_2; y_2) \leqslant A(m_1; y_1)/3 < 2A(m_2; y_2)/3$$

which is not possible. Now, we combine (60), (63) and (64) to conclude that $y_1(y_1+1) = y_2(y_2+1)$ and this is not possible, since $y_1 \neq y_2$.

Thus, by (57), we may assume that

(65) $\bar{P}(N-1) = A(m_1; y_1)/\eta'$.

Further, by (65) and (56),

(66) $A(m_1; y_1)/\eta' = B(m_2; y_2)$

which, together with (18) and Lemma 2, implies that

(67) $$y_1(y_1+1)\eta' B(m_1; y_1) = y_2(y_2+1)\eta \frac{A(m_2; y_2)}{\eta}, \quad \omega\left(\frac{A(m_2; y_2)}{\eta}\right) = 1.$$

We argue, as before, to derive from (67) that

(68) $A(m_2; y_2)/\eta$ divides $B(m_1; y_1)/\eta^2$

which implies that

(69) $\eta < 5\eta'$.

Now, we show that $\eta' = 1$. Suppose that $\eta' \neq 1$. Then $\eta' = m_1 = y_1+1$. Then, it is easy to see that $y_1 = z_1^2$ for some integer $z_1 \geqslant 4$ and (47) is valid. Observe that the factors on the right-hand side of (47) are prime powers and, by (20), each of these factors exceeds $(y_2+1)^2$ whenever $m_2 \geqslant 7$. Then, by counting the power of m_2 on both the sides of (67), we see from Corollary 1 that $\eta(m_2; y_2) = 1$ for $m_2 \geqslant 7$. If $m_2 = 5$, then $m_1 \geqslant 7$ and the left-hand side of (67) is not divisible by 25; thus $\eta(5; y_2) = 1$. Hence, by (54),

(70) $\eta(m_2; y_2) = 1, \quad m_2 \geqslant 3$.

Now, we see from (68), (70) and (47) that

(71) $A(m_2; y_2) \leqslant B(m_1; z_1)$.

Then, we combine (66) and (71) to derive that

$$(y_1^{m_1}+1)/m_1^2 < 5y_2^{m_2-1}/4 < 25A(m_2; y_2)/16 < 25z_1^{m_1-1}/12,$$

since $y_2 \geqslant 5$ and $z_1 \geqslant 4$. Thus

$$y_1^{(m_1+1)/2} < 25m_1^2/12$$

which is not possible, since $y_1 \geqslant 4$ and $m_1 \geqslant 5$. This proves that $\eta' = 1$ which, together with (54) and (69), implies that $\eta = 1$. Now, we argue, as earlier, to derive from (68) that $B(m_1; y_1) = A(m_2; y_2)$. Then, (67) implies that $y_1 = y_2$ which is a contradiction. ■

5. Proof of Theorem 1. We verify that $s(127) = 1$ and thus, we may assume that $N \neq 127$. Suppose that y_1 and y_2 are distinct elements of $S(N)$ such that $l(N; y_1)$ and $l(N; y_2)$ are odd integers. Let m_1, m_2, n_1, n_2, A and B be given by (13), (14) and (8). By Lemma 13, we conclude that $\omega(y_1(y_1+1)) \geqslant 3$ and $\omega(y_2(y_2+1)) \geqslant 3$. Thus $y_1 \geqslant 5$ and $y_2 \geqslant 5$. If $m_1 = 4$, then $\omega'(y_1^4+1) = \omega'(y_1^2+1) = 1$ and we argue, as in Section 4, to conclude that (18) with $m_1 = 4$ is not possible. Similarly $m_2 \neq 4$. For $i = 1, 2$, we apply Lemma 2 to derive that m_i is a prime number whenever $m_i > 1$ and the possibility $m_i = 1$ is excluded by Lemma 10. Thus m_1 and m_2 are prime numbers.

First, we consider the case that $m_1 \geqslant 3$ and $m_2 \geqslant 3$. By Lemma 2, we derive that $\omega(N-1) = 5$, $\omega(y_1(y_1+1)) = \omega(y_2(y_2+1)) = 3$ and

(72) $$\bar{P}(N-1) = B(m_1; y_1) = B(m_2; y_2).$$

Now, we apply Lemma 4 to derive from (17) and (72) that $m_1 \geqslant 5$ and $m_2 \geqslant 5$. Then, by (19) with $y_1 \geqslant 5$, $y_2 \geqslant 5$,

(73) $$A(m_1; y_1)/\eta_1 > (y_2+1)^2, \quad A(m_2; y_2)/\eta_2 > (y_1+1)^2$$

where $\eta_1 = \eta(m_1; y_1)$ and $\eta_2 = \eta(m_2; y_2)$ are given by (6). Now, we see from Lemma 2, (18), (72) and (73) that

(74) $$A(m_1; y_1)/\eta_1 = A(m_2; y_2)/\eta_2.$$

We combine (18), (72) and (74) to derive that

(75) $$\eta_1 y_1(y_1+1) = \eta_2 y_2(y_2+1).$$

By (17), (72) and $y_1 \geqslant 5$, $y_2 \geqslant 5$, we see that

(76) $$y_1 < (5/4)^{3/2} y_2, \quad y_2 < (5/4)^{3/2} y_1.$$

Since $y_1 \neq y_2$, we observe from (75) that either $\eta_1 \neq 1$ or $\eta_2 \neq 1$. Furthermore, (75) and (76) imply that $\eta_1 = m_1$ and $\eta_2 = m_2$. Now, we combine (74) and (75) to obtain

$$y_1^{m_1+1} - y_2^{m_2+1} = y_2 - y_1$$

which, since m_1 and m_2 are odd, implies that

$$y_1^2 + y_2^2 \leqslant |y_2 - y_1| < \max(y_1, y_2)$$

and this is not possible.

Thus, we may assume that either $m_1 = 2$ or $m_2 = 2$. There is no loss of generality in assuming that $m_2 = 2$. Then $m_1 \geqslant 3$, $\omega(N-1) = 5$ and $\omega(y_1(y_1+1)) = 3$. By (18) with $m_2 = 2$, Lemma 2 and (19) with $m_2 = 2$, $y_1 \geqslant 5$, $y_2 \geqslant 5$, we see that

$$A(m_1; y_1)/\eta_1 \leqslant y_2 + 1$$

which implies that $m_1 = 3$, $\eta_1 = 3$ and $y_1 \leqslant 20$. If $y_1 = 5$, then $B(3; y_1) = 31$ divides $y_2(y_2+1)$ which implies that $y_2 \geqslant 30$ and this is not possible. Similarly, $y_1 \notin \{11, 17, 20\}$. Furthermore, $y_1 \neq 8$ and $y_1 \neq 14$, since $\omega(y_1(y_1+1)) = 3$. ∎

6. Proof of Theorem 2. If $x \in S(N)$, we see from (3) that $\omega(N-1) \geqslant 2$. Thus, we may suppose that $\omega(N-1) \geqslant 2$. Further, we may also suppose that $N \neq 31$. We assume that

(77) $$s(N) > \begin{cases} 2\omega(N-1)-3, & \omega(N-1) \leqslant 4, \\ 2\omega(N-1)-4, & \omega(N-1) \geqslant 5 \end{cases}$$

and we shall arrive at a contradiction. We denote by $T(N)$ the set of all $x \in S(N)$ such that

(78) $$l(N; x) \geqslant \omega(N-1)+1$$

and let $T_1(N)$ be the complement of $T(N)$ in $S(N)$. We write $t(N)$ and $t_1(N)$ for the number of distinct elements of $T(N)$ and $T_1(N)$, respectively. By (4) and Lemma 5, we derive that

(79) $$t_1(N) \leqslant \begin{cases} \omega(N-1)-2, & \omega(N-1) \leqslant 4, \\ \omega(N-1)-3, & \omega(N-1) \geqslant 5. \end{cases}$$

By (77) and (79),

(80) $$t(N) \geqslant \omega(N-1).$$

Let

(81) $$x_1 > x_2 > \ldots > x_t, \quad t = t(N),$$

be elements of $T(N)$. By (3), we see that

(82) $$\mathrm{Supp}(x_1 \ldots x_t) \subseteq \mathrm{Supp}(N-1)$$

which, together with (80), implies that

(83) $$t \geqslant \omega(N-1) \geqslant \omega(x_1 \ldots x_t).$$

Suppose that

(84) $$t = \omega(x_1 \ldots x_t).$$

Then, we observe from (83) and (84) that $\omega(x_1 \ldots x_t) = \omega(N-1)$ which, together with (82), implies that $\mathrm{Supp}(x_1 \ldots x_t) = \mathrm{Supp}(N-1)$. Now, we refer to (3) to observe that

(85) $$N-1 = [x_1, \ldots, x_t]$$

where the right-hand side denotes the least common multiple of $x_1, \ldots, x_t$. We put $\mu_1 = l(N; x_1)$. Then, by (78), $\mu_1 > \omega(N-1)$ and we see from (3), (85) and (81) that

$$x_1^{\mu_1-2} < B(\mu_1-1; x_1) \leqslant x_2 \ldots x_t < x_1^{t-1}.$$

Consequently, we derive that $t > \omega(N-1)$ which, by (83) and (84), is not possible.

Thus, we have shown that

(86) $$t > \omega(x_1 \ldots x_t).$$

For every prime divisor p of $x_1 \dots x_t$, we choose $f(p) \in T(N)$ such that $l(N; f(p))$ is maximal among all the elements $x \in T(N)$ such that $p|x$. In view of (86), there exists $x_0 \in T(N)$ which is not in the range of f. We put $\mu_0 = l(N; x_0)$. For a prime p dividing x_0, we see from (12) that

$$\mathrm{ord}_p(x_0) = \mathrm{ord}_p(x'_0), \quad x'_0 = f(p) \neq x_0.$$

By (78),

$$l(N; x'_0) > \mu_0 \geqslant \omega(N-1)+1. \tag{87}$$

Now, we derive from (17) that

$$p^{\mathrm{ord}_p(x_0)} \leqslant (x_0, x'_0) < N^{1/\mu_0(\mu_0-1)} \tag{88}$$

for every prime p. By (3), we see that $\omega(x_0) < \omega(N-1)$ and consequently, we derive from (88) that

$$x_0 < N^{(\omega(N-1)-1)/\mu_0(\mu_0-1)}. \tag{89}$$

On the other hand, we see from (2) that

$$x_0 > \left(\frac{N}{2}\right)^{1/(\mu_0-1)}. \tag{90}$$

Finally, we combine (90), (89) and (87) to obtain

$$N^2 < 2^{\omega(N-1)+1} \leqslant 2N$$

which is not possible. ∎

References

[1] R. Balasubramanian and T. N. Shorey, *On the equation* $\frac{a(x^m-1)}{x-1} = \frac{b(y^n-1)}{y-1}$, Math. Scand. 46 (1980), 177–182.

[2] H. Davenport, D. J. Lewis and A. Schinzel, *Equations of the form* $f(x) = g(y)$, Quart. J. Math. 12 (1961), 304–312.

[3] L. E. Dickson, *History of the Theory of Numbers*, Chelsea Publishing Company, New York 1952.

[4] Richard K. Guy, *Unsolved problems in Number Theory*, Springer-Verlag, New York, Heidelberg, Berlin 1981.

[5] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. 37 (1986), 27–38.

[6] J. H. Loxton, *Some problems involving powers of integers*, Acta Arith. 46 (1986), 113–123.

[7] A. Mąkowski and A. Schinzel, *Sur l'équation indéterminée de R. Goormaghtigh*, Mathesis 68 (1959), 128–142.

[8] T. Nagell, *The diophantine equation* $x^2+7 = 2^n$, Ark. Mat. 4 (1961), 185–187.

[9] S. Ramanujan, *Question 464*, J. Indian Math. Soc. 5 (1913), 120. *Collected papers*, Cambridge University Press, 1927, 327.

[10] T. N. Shorey, *On the equation* $a(x^m-1)/(x-1) = b(y^n-1)/(y-1)$ (II), Hardy–Ramanujan Journ. 7 (1984), 1–10.

[11] — *On the equation* $ax^m - by^n = k$, Indag. Math. (1986), 353–358.

TATA INSTITUTE OF FUNDAMENTAL RESEARCH
Bombay 400005, India

THE INSTITUTE FOR ADVANCED STUDY
Princeton, NJ 08540, U.S.A.

Received on 1.7.1987
and in revised form on 6.1.1988 (1732)