Mh. Math. 102, 251–257 (1986)

Monatshefte für
Mathematik

On the Oesterlé-Masser Conjecture

By

C. L. Stewart*, Waterloo, and **R. Tijdeman**, Leiden

(Received 17 February 1986)

Dedicated to Professor E. Hlawka on the occasion of his seventieth birthday

Abstract. Let x, y and z be positive integers such that $x = y + z$ and $\gcd(x, y, z) = 1$. We give upper and lower bounds for x in terms of the greatest squarefree divisor of xyz.

For any positive integers x, y and z define $G = G(x, y, z)$ by

$$G = G(x, y, z) = \prod_{\substack{p \mid xyz \\ p \, prime}} p \, .$$

J. Oesterlé posed the problem to decide whether there exists a constant C_1 such that for all positive integers x, y and z with $(x, y, z) = 1$ and $x = y + z$ we have

$$x < G^{C_1} \, . \tag{1}$$

This problem is related to some standard conjectures in the theory of elliptic curves. Masser [4] conjectured, in analogy to a result of R. C. Mason on the function field case, that for any positive real number ε we even have, instead of (1),

$$x < C_2(\varepsilon) \, G^{1+\varepsilon} \, , \tag{2}$$

where $C_2(\varepsilon)$ is a positive number which depends on ε only. For illustration we give two numerical examples:

* The research of the first author was supported in part by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

$$4375 = 5^4 \cdot 7 = 2 \cdot 3^7 + 1 \quad \text{yields} \quad x \approx G^{1.568};$$

$$48234496 = 2^{21} \cdot 23 = 3^2 5^6 7^3 + 11^2 \text{ yields } x \approx G^{1.626}$$

(example due to B. M. M. DE WEGER [9]).

Some well known conjectures would follow from inequalities (1) and (2). HALL JR. [3] conjectured that there is a constant C_3 such that $|x^2 - y^3| > C_3 y^{1/2}$ for all positive integers x, y with $x^2 \neq y^3$.

Inequality (2) would imply the following slightly weaker assertion: For every positive number ε there exists a positive number $C_4(\varepsilon)$ depending on ε only such that

$$|x^2 - y^3| > C_4(\varepsilon)\, y^{1/2-\varepsilon}$$

for all positive integers x, y with $x^2 \neq y^3$. Both (1) and (2) would imply, by FALTINGS' celebrated result [2], that there are only finitely many positive integers n, x, y and z with $n \geqslant 3$ such that

$$x^n = y^n + z^n\,,$$

that is, there are only finitely many exceptions in Fermat's Last Theorem. PILLAI [5] conjectured that for given positive integers a, b and k the equation

$$a x^m - b y^n = k$$

has only finitely many solutions in positive integers m, n, x and y with $m > 1, n > 1, x > 1, y > 1$ and $(m, n) \neq (2, 2)$. The only case for which this has been proved is $a = b = k = 1$ [8]. Pillai's assertion would follow immediately from (2), (but also from (1) in combination with some known results). Similarly (2) would imply that for given positive integers a, b and k there are only finitely many positive integers m, n, r, x, y, z with $\frac{1}{m} + \frac{1}{n} + \frac{1}{r} < 1$ and $x > 1$, $y > 1$, $z > 1$ such that

$$a x^m - b y^n = k z^r\,.$$

Thus it seems hopeless to prove (2). We shall show in Theorem 1 that a weaker inequality follows from a result of van der Poorten. There may be some hope, however, to disprove (2). In Theorem 2 we show that (2), if true, is not far from the best possible. We are grateful to

F. BEUKERS for his suggestions. In particular we owe to him the smooth proof of Theorem 2.

By $c_1, c_2, \ldots, c_6$ we denote certain effectively computable positive constants.

Theorem 1. *All positive integers x, y, z such that* g.c.d. $(x, y, z) = 1$ *and $x = y + z$ satisfy*

$$\log x < C_5 G^{15}$$

where C_5 is an effectively computable constant.

We shall deduce this result from the following lemma which is proved by the p-adic version of Baker's method.

Lemma 1. *Let $a_1, \ldots, a_n$ $(n \geqslant 2)$ be non-zero rational integers with absolute values at most $A\,(\geqslant 4)$. Let p be a prime number. Then the inequalities*

$$\infty > \operatorname{ord}_p(a_1^{b_1} \ldots a_n^{b_n} - 1) > (16(n+1))^{12(n+1)} \frac{p}{\log p} (\log A)^n (\log B)^2$$

have no solutions in rational integers with absolute values at most $B\,(\geqslant e^2)$.

Proof. Apply Theorem 2 of VAN DER POORTEN [6] with $K = \mathbb{Q}$, $D = 1$, $\alpha_j = a_j$, $\Omega = \prod_{j=1}^{n} \log|a_j| \leqslant (\log A)^n$ and $G_p \leqslant p$. □

Proof of Theorem 1. Let

$$x = \prod_{i=1}^{r} p_i^{k_i}, \quad y = \prod_{i=1}^{r} p_i^{l_i}, \; z = \prod_{i=1}^{r} p_i^{m_i},$$

where $p_1 < p_2 < \ldots < p_r$ are prime numbers and k_i, l_i, m_i are integers for $i = 1, \ldots, r$. Put $K = \max_i k_i$, $L = \max_i l_i$, $M = \max_i m_i$, $H = \max(K, L, M)$ and $P = p_r$. By Lemma 1 we have

$$H = \max(K, L, M) \leqslant (16(r+1))^{12(r+1)} \frac{P}{\log P} (\log P)^r (\log H)^2 . \quad (3)$$

ROSSER [7] proved that $p_j > j \log j$ for $j = 1, 2, \ldots$. This implies

$$G = \prod_{j=1}^{r} p_j \geqslant r! \prod_{j=2}^{r} \log j > c_1 \left(\frac{r\sqrt{\log r}}{e}\right)^r .$$

Hence

$$(16(r+1))^{r+1} < c_2 G . \tag{4}$$

This implies $r < \log(c_3 G)/\log\log G$. Hence, by $P \leqslant G$,

$$(\log P)^r \leqslant c_3 G . \tag{5}$$

By (3), (4) and (5), we obtain

$$\frac{H}{(\log H)^2} \leqslant c_4 G^{14} .$$

Hence

$$H \leqslant c_5 G^{14} (\log G)^2 .$$

Thus

$$\log x < H \log(p_1 \ldots p_r) < H \log G < c_6 G^{15} . \square$$

Theorem 2. *Let $\delta > 0$. Then there exist infinitely many positive integers x, y and z such that $x = y + z$,* g.c.d. $(x, y) = 1$ *and*

$$x > G \exp\left((4-\delta)\frac{\sqrt{\log G}}{\log\log G}\right) .$$

We shall apply the following estimates in the proof.

Lemma 2. *Let $p_1 < p_2 < \ldots < p_r$ be the first r odd prime numbers. Let $\delta > 0$. Then, for sufficiently large r, we have*

i) $p_r < r\log r + r\log\log r - (1-\delta) r$;

ii) $\sum_{i=1}^{r} \log p_i < r\log r + r\log\log r - (1-\delta) r$;

iii) $\sum_{i=1}^{r} \log\log p_i < r(\log\log r + \delta)$.

Proof. The prime number theorem with error term implies

$$\pi(X) = \int_2^X \frac{dx}{\log x} + O\left(\frac{X}{(\log X)^3}\right) =$$

$$= \frac{X}{\log X} + \frac{X}{(\log X)^2} + O\left(\frac{X}{(\log X)^3}\right) .$$

Hence

$$r = \pi(p_r) - 1 = \frac{p_r}{\log p_r} + \frac{p_r}{(\log p_r)^2} + O\left(\frac{p_r}{(\log p_r)^3}\right)$$

which gives

$$p_r = r\log p_r\left(1+\frac{1}{\log p_r}+O\left(\frac{1}{\log^2 p_r}\right)\right)^{-1} =$$

$$= r\log p_r - r + O\left(\frac{r}{\log p_r}\right)$$

and part i) follows in a straightforward manner.

To prove ii), notice

$$\sum_{i=1}^{r}\log p_i = \int_{2^+}^{p_r^+}\log x\, d\pi(x) =$$

$$= [\pi(x)\log x]_{2^+}^{p_r^+} - \int_2^{p_r}\frac{\pi(x)}{x}\,dx < r\log p_r - \int_2^{p_r}\frac{dx}{\log x}$$

for r large. Using

$$\int_2^{p_r}\frac{dx}{\log x} = \pi(p_r) + O\left(\frac{p_r}{\log^2 p_r}\right)$$

and i) we obtain ii).

Part iii) is proved by the trivial estimate

$$\sum_{i=1}^{r}\log\log p_i < r\log\log p_r \text{ and i)} . \square$$

Lemma 3. *Let $\delta > 0$. Let $p_1, \ldots, p_r$ be the first r odd primes. Let $N(X)$ be the number of positive integers not exceeding X and composed of $p_1, \ldots, p_r$. Then, for sufficiently large r,*

$$N(X) > \left(\frac{e^{1-2\delta}\log X}{r\log r}\right)^r .$$

Proof. Note that $N(X)$ is exactly the number of solutions of the inequality

$$|\sum_{i=1}^{r} n_i \log p_i| \leqslant \log X$$

in non-negative integers $n_1, \ldots, n_r$. This number is clearly bounded below by the volume of the generalized tetrahedron $|\sum_i x_i \log p_i| \leqslant \log X$, $x_i \geqslant 0$, divided by the volume of the unit block $(x_1\log p_1, \ldots, x_r \log p_r)$, $0 \leqslant x_i \leqslant 1$, with $i = 1, \ldots, r$. Hence

$$N(X) > \frac{(\log X)^r}{r! \prod_{i=1}^{r} \log p_i}.$$

The above argument is due to ENNOLA, see [1]. The lemma now follows from the estimate in Lemma 2 iii) and the inequality $r! < (r/e^{1-\delta})^r$ for r sufficiently large. □

Proof of Theorem 2. Let c_7, c_8, c_9, c_{10} denote positive numbers which are effectively computable in terms of δ. Let r be a positive integer and let $p_1, \ldots, p_r$ be the first r odd primes. Let $X = \exp((r \log r)^2)$. Let S be the set of positive integers not exceeding X and composed of $p_1, \ldots, p_r$. By the box principle, there exist $x, y \in S$, $x > y$ such that $|x - y|_2 \leqslant 2/|S|$ where $| \ |_2$ denotes the 2-adic valuation. Put $z = x - y$. Without loss of generality we may assume g.c.d. $(x, y) = 1$. For the triple x, y, z we have

$$G(x, y, z) \leqslant (\prod_{i=1}^{r} p_i) z \cdot \frac{4}{|S|} < 4x (\prod_{i=1}^{r} p_i) \frac{1}{|S|}.$$

Using that, by Lemma 2 ii),

$$\prod_{i=1}^{r} p_i < \left(\frac{r \log r}{e^{1-\delta}}\right)^r \quad \text{for} \quad r > c_7,$$

and, by Lemma 3,

$$|S| > \left(\frac{e^{1-2\delta} \log X}{r \log r}\right)^r \quad \text{for} \quad r > c_8$$

and $\log X = (r \log r)^2$, we obtain

$$G < x e^{-2(1-2\delta) r} \quad \text{for} \quad r > c_9.$$

From $r \log r = (\log X)^{1/2}$ it follows that

$$r > (2 - \delta)(\log X)^{1/2}/\log\log X > (2 - \delta)(\log x)^{1/2}/\log\log x$$

for $r > c_{10}$. Hence

$$G < x \exp\left(-4(1 - 3\delta) \frac{\sqrt{\log x}}{\log\log x}\right)$$

and thus

$$x > G\exp\left(4(1-4\delta)\frac{\sqrt{\log G}}{\log\log G}\right).$$

From $|z|_2 = |x-y|_2 \leqslant 2/|S|$ we see that $|z|_2 \to 0$ as $r \to \infty$, hence $z \to \infty$ as $r \to \infty$. So we find that infinitely many triples x, y, z satisfy the conditions of Theorem 2. □

References

[1] ENNOLA, V.: On numbers with small prime divisors. Ann. Acad. Sci. Fenn. Series A I **440**, 1—16 (1969).

[2] FALTINGS, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. **73**, 349—366 (1983).

[3] HALL JR., M.: The diophantine equation $x^3 - y^2 = k$. In: Computers in Number Theory. A. O. L. Atkin and B. J. Birch (eds.). Proc. Sci. Res. Council Atlas Symp. No. 2, Oxford 1969, pp. 173—198. London: Academic Press. 1971.

[4] MASSER, D. W.: Open problems. Proc. Symp. Analytic Number Th. W. W. L. Chen (ed.). London: Imperial College. 1985.

[5] PILLAI, S. S.: On the equation $2^x - 3^y = 2^X + 3^Y$. Bull. Calcutta Math. Soc. **37**, 15—20 (1945).

[6] VAN DER POORTEN, A. J.: Linear forms in logarithms in the p-adic case. In: Transcendence Theory: Advances and Applications. A. Baker (ed.), pp. 29—57. London: Academic Press. 1977.

[7] BARKLEY ROSSER, J.: The n-th prime is greater than $n \log n$. Proc. London Math. Soc. (2) **45**, 21—44 (1939).

[8] TIJDEMAN, R.: On the equation of Catalan. Acta Arith. **29**, 197—209 (1976).

[9] DE WEGER, B. M. M.: Solving exponential diophantine equations using lattice basis reduction algorithms. Report Math. Inst. University of Leiden. 1986, No. 13.

C. L. STEWART
Department of Pure Mathematics
University of Waterloo
Waterloo, Ont. N2L 3G1
Canada

and

R. TIJDEMAN
Mathematical Institute
University of Leiden
NL-2300 RA Leiden
The Netherlands