Math. Ann. 291, 225–230 (1991)

Mathematische Annalen


# On the *abc* conjecture

C. L. Stewart[1,*] and Kunrui Yu[2,**,***]

[1] Department of Pure Mathematics, Faculty of Mathematics, The University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada
[2] Institute of Mathematics, Academia Sinica, Beijing 100080, People's Republic of China

Received September 12, 1990

## 1 Introduction

Let $x$, $y$, and $z$ be positive integers and define $G=G(x,y,z)$ by

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

Thus $G$ is the greatest square-free factor of $xyz$. Oesterlé, motivated by a conjecture of Szpiro concerning elliptic curves (cf. Frey [2], Oesterlé [5], Szpiro [8]), asked if there exists a positive number $c_1$ such that for all positive integers $x$, $y$, and $z$ with

$$(x,y,z)=1 \quad \text{and} \quad x+y=z, \tag{1}$$

$$z<G^{c_1}. \tag{2}$$

Masser [4] then conjectured, by analogy with a result of Mason [3] in the function field case, that for each positive real number $\varepsilon$ there is a positive number $c_2(\varepsilon)$ which depends on $\varepsilon$ only such that in place of (2) we have

$$z<c_2(\varepsilon)G^{1+\varepsilon}. \tag{3}$$

Both (2) and (3) are known as the *abc* conjecture. We refer the reader to Chap. 5 of Vojta [9] for a generalization of (3) and the statement of several related conjectures. Conjectures (2) and (3) have profound implications, in particular for the study of Diophantine equations, cf. [7].

---

* Research supported in part by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada by a Killam Research Fellowship
** Member of Institute for Advanced Study, Princeton, 1989–90, supported by NSF grant DMS-8610730. The second author would like to express his cordial gratitude to IAS, Princeton for the hospitality
*** Current address: School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA

In [7] Stewart and Tijdeman proved that there exists an effectively computable constant $c_3$ such that for all positive integers $x$, $y$, and $z$ satisfying (1),

$$\log z < c_3 G^{15}.$$

The proof depends on a $p$-adic estimate for linear forms in the logarithms of algebraic numbers due to van der Poorten [6]. (However, see Yu [11] for a discussion of some defects in the proof of [6].) In this note we shall combine two estimates proved by Baker's method, a recent $p$-adic estimate for linear forms in the logarithms of algebraic numbers due to Yu [12] and an earlier Archimedean estimate due to Waldschmidt [10], to prove the following result.

**Theorem.** *There exists an effectively computable positive constant c such that for all positive integers x, y, and z with* $(x,y,z)=1$, $z>2$, *and* $x+y=z$,

$$\log z < G^{2/3 + c/\log\log G}.$$

In particular, for each $\varepsilon>0$ there exists a number $c_4(\varepsilon)$ which is effectively computable in terms of $\varepsilon$ such that for all positive integers $x$, $y$, and $z$ with $(x,y,z)=1$ and $x+y=z$,

$$z < \exp(c_4(\varepsilon) G^{2/3+\varepsilon}).$$

## 2 Preliminary lemmas

Let $p$ be a prime number and put

$$q=\begin{cases}2 & \text{if } p>2\\ 3 & \text{if } p=2\end{cases} \quad \text{and} \quad \alpha_0=\begin{cases}\zeta_4 & \text{if } p>2\\ \zeta_6 & \text{if } p=2\end{cases} \tag{4}$$

where $\zeta_m=e^{2\pi i/m}$ for $m=1,2,3,\ldots$. Put $K=\mathbb{Q}(\alpha_0)$ and let $\alpha_1,\ldots,\alpha_n$ be non-zero algebraic integers in $K$ with absolute values at most $A_1,\ldots,A_n$ respectively and with $A_i \geqq 4$ for $i=1,\ldots,n$. Put $A=\max\limits_{1\leqq i\leqq n} A_i$. Let $b_1,\ldots,b_n$ be rational integers with absolute values at most $B(\geqq 3)$. Let $\wp$ be a prime ideal of the ring of algebraic integers of $K$ lying above the prime $p$. For $\alpha\in K\backslash\{0\}$, write $\operatorname{ord}_\wp \alpha$ for the exponent of $\wp$ in the prime factorization of the fractional ideal $(\alpha)$. Denote by $e_\wp$ the ramification index of $\wp$ and by $f_\wp$ the residue class degree of $\wp$. Next put

$$\Theta=\alpha_1^{b_1}\ldots\alpha_n^{b_n}-1.$$

**Lemma 1.** *Suppose that* $[K(\alpha_0^{1/q},\ldots,\alpha_n^{1/q}):K]=q^{n+1}$, $\operatorname{ord}_\wp \alpha_j=0$ *for* $j=1,\ldots,n$, *and* $\Theta\neq 0$. *Then*

$$\operatorname{ord}_\wp \Theta < (c_5 n)^n p^2\cdot\log B\cdot\log\log A\cdot\log A_1\cdot\ldots\cdot\log A_n$$

*where* $c_5$ *is an effectively computable positive number.*

*Proof.* This follows from Corollary 2.3 of Yu [12] when $n\geqq 2$ and from Lemma 1.4 of [12] when $n=1$, on noting that $K$ is an imaginary quadratic field and so $f_\wp \leqq 2$ and $h(\alpha_j)=\log|\alpha_j|$.

**Lemma 2.** *If* $\alpha_1,\ldots,\alpha_n$ *are positive rational integers,*

$$[\mathbb{Q}(\alpha_1^{1/2},\ldots,\alpha_n^{1/2}):\mathbb{Q}]=2^n \quad \textit{and} \quad b_1\log\alpha_1+\ldots+b_n\log\alpha_n\neq 0$$

*then*

$$|b_1 \log\alpha_1 + \ldots + b_n \log\alpha_n| > \exp(-(c_6 n)^n \log B (\log\log A)^2 \log A_1 \ldots \log A_n),$$

*where $c_6$ is an effectively computable positive number.*

*Proof.* This follows from Proposition 3.8 of Waldschmidt [10].

**Lemma 3.** *Let $\alpha_1, \ldots, \alpha_n$ be prime numbers with $\alpha_1 < \alpha_2 < \ldots < \alpha_n$. Then*

$$[\mathbb{Q}(\alpha_1^{1/2}, \ldots, \alpha_n^{1/2}) : \mathbb{Q}] = 2^n .$$

*Let $q=2$ and $\alpha_0 = \zeta_4$ or $q=3$ and $\alpha_0 = \zeta_6$ and put $K = \mathbb{Q}(\alpha_0)$. Then*

$$[K(\alpha_0^{1/q}, \alpha_1^{1/q}, \ldots, \alpha_n^{1/q}) : K] = q^{n+1}$$

*except when $q=2$, $\alpha_0 = \zeta_4$, and $\alpha_1 = 2$ and in this case*

$$[K(\alpha_0^{1/2}, (1+i)^{1/2}, \alpha_2^{1/2}, \ldots, \alpha_n^{1/2}) : K] = 2^{n+1} .$$

*Proof.* We shall prove the result in the case when $q=2$, $\alpha_0 = \zeta_4 = i$, and $\alpha_1 = 2$. The other cases are proved in a similar fashion. For brevity we redefine $\alpha_1$ to be $1+i$ for the balance of the argument. Since $K = \mathbb{Q}(\alpha_0)$ and $\alpha_0 = i$ we have $[K(\alpha_0^{1/2}) : K] = 2$. Thus it suffices to prove that for each integer $j$ with $j = 1, \ldots, n$ that $[K_j(\alpha_j^{1/2}) : K_j] = 2$ where $K_j = K(\alpha_0^{1/2}, \ldots, \alpha_{j-1}^{1/2})$. If for some integer $j$ with $1 \leqq j \leqq n$ this is not the case then by Lemma 3 of Baker and Stark [1] we have

$$\alpha_j = \alpha_0^{k_0} \ldots \alpha_{j-1}^{k_{j-1}} \gamma^2 \tag{5}$$

for some $\gamma$ in $K$ and some integers $k_0, \ldots, k_{j-1}$ with

$$0 \leqq k_l < 2 \quad \text{for} \quad l = 0, \ldots, j-1 .$$

Let $\wp$ be a prime ideal of the ring of algebraic integers of $K$ which divides the ideal generated by $\alpha_j$. Since $2(= -i(1+i)^2)$, $\alpha_2, \ldots, \alpha_j$ are distinct prime numbers we deduce from (5) that

$$\operatorname{ord}_\wp \alpha_j = 2 \operatorname{ord}_\wp \gamma . \tag{6}$$

The only prime number which ramifies in $K = \mathbb{Q}(i)$ is 2 and thus $\operatorname{ord}_\wp \alpha_j = 1$. By (6) this is a contradiction and the result follows.

**Lemma 4.** *Let $2 = p_1, p_2, \ldots$ be the sequence of prime numbers in increasing order. Then there is an effectively computable positive constant $c_7$ such that for every positive integer $r$ we have*

$$\prod_{j=1}^{r} \frac{p_j}{\log p_j} > \left(\frac{r+3}{c_7}\right)^{r+3} .$$

*Proof.* By the prime number theorem with error term, or indeed by the Chebyshev estimates for $\pi(x)$, there exists an effectively computable positive number $c_8$ for which

$$\frac{p_j}{\log p_j} > \frac{j}{c_8} .$$

We now apply the inequality $r! \geqq (r/e)^r$ to conclude that

$$\prod_{j=1}^{r} \frac{p_j}{\log p_j} > \frac{r!}{c_8^r} \geqq \left(\frac{r}{c_8 e}\right)^r > \left(\frac{r+3}{c_9}\right)^{r+3} .$$

## 3 Proof of main theorem

Let $c_{10}, c_{11}, \ldots$ denote effectively computable positive constants. We may suppose, without loss of generality, that $x \leqq y$. Since $x+y=z$, $(x,y,z)=1$ and $z>2$ we see that $x<y<z$ and that $G \geqq 6$. We write

$$x=g_1^{k_1}\ldots g_s^{k_s}, \qquad y=q_1^{l_1}\ldots q_t^{l_t}, \qquad z=h_1^{m_1}\ldots h_u^{m_u}, \tag{7}$$

where $g_1,\ldots,g_s, q_1,\ldots,q_t, h_1,\ldots,h_u$ are distinct prime numbers with $s \geqq 0$, $t \geqq 1$, and $u \geqq 1$ and $k_1,\ldots,k_s$, $l_1,\ldots,l_t$, $m_1,\ldots,m_u$ are positive integers. Denote the largest prime dividing $x$ by $p_x$ except when $x=1$ and in that case put $p_x=1$. Similarly denote the largest primes dividing $y$ and $z$ by $p_y$ and $p_z$ respectively. Plainly for any prime $p$,

$$\max\{\mathrm{ord}_p x,\ \mathrm{ord}_p y,\ \mathrm{ord}_p z\} \leqq \frac{\log z}{\log 2}. \tag{8}$$

Observe that we have

$$\log z = \sum_{p|z} (\mathrm{ord}_p z)\log p \leqq \left(\max_{p|z} \mathrm{ord}_p z\right)\cdot \log G. \tag{9}$$

Since $(x,y,z)=1$ and $x+y=z$ we have $(x,y)=(x,z)=(y,z)=1$. Thus for each prime $p$ which divides $z$,

$$\mathrm{ord}_p z = \mathrm{ord}_p\left(\frac{z}{-y}\right) = \mathrm{ord}_p\left(\frac{x}{-y}-1\right) \leqq \mathrm{ord}_p\left(\left(\frac{x}{y}\right)^4-1\right).$$

We now estimate

$$\mathrm{ord}_p\left(\left(\frac{x}{y}\right)^4-1\right) = \mathrm{ord}_p(g_1^{4k_1}\ldots g_s^{4k_s} q_1^{-4l_1}\ldots q_t^{-4l_t}-1)$$

for each prime $p$ which divides $z$ by means of Lemma 1. Put $\Theta=(x/y)^4-1$. If $p=2$ we put $K=\mathbb{Q}(\zeta_6)$ while if $p>2$ we put $K=\mathbb{Q}(\zeta_4)$. Further we define $q$ and $\alpha_0$ as in (4). We then take $\wp$ to be a prime ideal of the ring of algebraic integers of $K$ lying above the prime $p$. We have

$$\mathrm{ord}_p \Theta \leqq \mathrm{ord}_\wp \Theta$$

and we may estimate $\mathrm{ord}_\wp \Theta$ from above by applying Lemma 1 with $n=s+t$ and $\alpha_1,\ldots,\alpha_n$ given by the primes $g_1,\ldots,g_s$, $q_1,\ldots,q_t$ arranged in increasing order, except in the case when $p>2$ and $\alpha_1=2$, and in that case we take $\alpha_1=1+i$ in place of $\alpha_1=2$. In this connection, note that $2^4=(1+i)^8$. Since $p|z$ and $(x,z)=(y,z)=1$ we have $\mathrm{ord}_p \alpha_i=0$ for $i=1,\ldots,s+t$. Certainly $\Theta \neq 0$ and by Lemma 3,

$$[K(\alpha_0^{1/q}, \alpha_1^{1/q}, \ldots, \alpha_{s+t}^{1/q}):K] = q^{s+t+1}.$$

Further, we may take

$$B=\max\{8k_1,\ldots,8k_s,\ 8l_1,\ldots,8l_t\}$$

hence, by (8), $B \leqq 8\log z/\log 2$. Thus by Lemma 1

$$\mathrm{ord}_p z \leqq \mathrm{ord}_\wp \Theta < (c_{10}(s+t))^{s+t} p^2 \cdot \log\log z \cdot \log\log G \cdot \prod_{p|xy} \log p. \tag{10}$$

Similarly if $p|y$ then, by considering $\mathrm{ord}_p((z/x)^4-1)$ we find that

$$\mathrm{ord}_p y < (c_{11}(s+u))^{s+u} p^2 \cdot \log\log z \cdot \log\log G \cdot \prod_{p|xz} \log p \tag{11}$$

and if $p|x$ then by considering $\mathrm{ord}_p(z/y)^4-1)$ we find that

$$\mathrm{ord}_p x<(c_{12}(t+u))^{t+u}p^2\cdot\log\log z\cdot\log\log G\cdot\prod_{p|yz}\log p. \tag{12}$$

If follows from (9) and (10) that

$$\frac{\log z}{\log\log z}<(c_{10}(s+t))^{s+t}p_z^2\cdot\prod_{p|xy}\log p\cdot(\log G)^2. \tag{13}$$

Since $y>z/2$ and $z\geqq 3$,

$$\log y>\log z-\log 2>\frac{\log z}{4}.$$

But (9) holds with $z$ replaced by $y$ and so from (11)

$$\frac{\log z}{4\log\log z}<(c_{11}(s+u))^{s+u}p_y^2\cdot\prod_{p|xz}\log p\cdot(\log G)^2. \tag{14}$$

Next, either $x\geqq y^{1/2}$ in which case

$$\log x\geqq\frac{1}{2}\log y>\frac{\log z}{8}$$

or $x<y^{1/2}$ in which case

$$\log\left(\frac{x+y}{y}\right)=\log\left(1+\frac{x}{y}\right)<\log\left(1+\frac{1}{y^{1/2}}\right)<\frac{1}{y^{1/2}}<\frac{\sqrt{2}}{z^{1/2}}. \tag{15}$$

In the former case we may appeal to (9), with $z$ replaced by $x$, and (12) to conclude that

$$\frac{\log z}{8\log\log z}<(c_{12}(t+u))^{t+u}p_x^2\cdot\prod_{p|yz}\log p\cdot(\log G)^2. \tag{16}$$

In the latter case,

$$0<\log\left(\frac{z}{y}\right)=\log\left(\frac{x+y}{y}\right)=m_1\log h_1+\ldots+m_u\log h_u-l_1\log q_1-\ldots-l_t\log q_t.$$

By Lemma 3 we may apply Lemma 2 to obtain a lower bound for $\log(z/y)$. Comparing this with the upper bound given by (15) we again obtain (16) with $c_{12}$ replaced by $c_{13}$. Put $r=t+s+u$. From (13), (14), and (16), we deduce that

$$\left(\frac{\log z}{4\log\log z}\right)^3<(c_{14}r)^{2r}(p_xp_yp_z)^2\Big(\prod_{p|xyz}\log p\Big)^2(\log G)^6. \tag{17}$$

By Lemma 4,

$$\left(\frac{r}{c_{15}}\right)^r<\prod_{i=1}^{r-3}\frac{p_i}{\log p_i}<2\prod_{\substack{p|xyz\\ p\notin\{p_x,p_y,p_z\}}}\frac{p}{\log p},$$

with the usual convention that the empty product is 1. Thus, by (17),

$$\left(\frac{\log z}{4\log\log z}\right)^3<c_{16}^rG^2(\log G)^{12}. \tag{18}$$

Again by Lemma 4 we see that

$$c_{16}^{r} < G^{c_{17}/\log\log G},$$

and the result now follows from (18).

## References


1. Baker, A., Stark, H.M.: On a fundamental inequality in number theory. Ann. Math. **94**, 190–199 (1971)
2. Frey, G.: Elliptic curves and solutions of $A-B=C$. In: Goldstein, C. (ed.) Séminaire de Théorie des Nombres Paris 1985–86. (Prog. Math., vol. 71, pp. 39–51) Boston Basel Stuttgart: Birkhäuser 1987
3. Mason, R.C.: Diophantine equations over function fields. (Lond. Math. Soc. Lect. Note Ser., vol. 96). Cambridge: Cambridge University Press 1984
4. Masser, D.W.: Open problems. In: Chen, W.W.L. (ed.) Proc. Symp. Analytic Number Theory. London: Imperial College 1985
5. Oesterlé, J.: Nouvelles approches du "Théorème" de Fermat: Séminaire Bourbaki, 1987–88, no. 694. (Astérisque, vols. 161–162, pp. 165–186) Paris: Soc. Math. Fr. 1988
6. Van der Poorten, A.J.: Linear forms in logarithms in the $p$-adic case. In: Baker, A., Masser, D.W. (ed.) Transcendence Theory: Advances and Applications, pp. 29–57. London: Academic Press 1977
7. Stewart, C.L., Tijdeman, R.: On the Oesterlé-Masser conjecture. Monatsh. Math. **102**, 251–257 (1986)
8. Szpiro, L.: La conjecture de Mordell [d'après Faltings]. Séminaire Bourbaki, 1983–84, no. 619. (Astérisque, vols. 121–122, pp. 93–103) Paris: Soc. Math. Fr. 1985
9. Vojta, P.: Diophantine approximations and value distribution theory. (Lect. Notes Math., vol. 1239) Berlin Heidelberg New York: Springer 1987
10. Waldschmidt, M.: A lower bound for linear forms in logarithms. Acta Arith. **37**, 257–283 (1980)
11. Yu, Kunrui: Linear forms in $p$-adic logarithms. Acta Arith. **53**, 107–186 (1989)
12. Yu, Kunrui: Linear forms in $p$-adic logarithms. II. Compos. Math. **74**, 15–113 (1990)