ACTA ARITHMETICA
XXIV (1973)

Effective estimates of solutions of some diophantine equations

by

H. M. STARK* (Cambridge, Mass.)

To Prof. C. L. Siegel on his 75th birthday

1. Introduction. Four years ago, Baker [1] gave the first effective solution to the Mordell equation,

$$y^2 = x^3 + k, \tag{1}$$

where k is a non-zero integer. Namely, if x and y are integral solutions to (1), then

$$\max(|x|, |y|) < e^{c|k|^{10000}}, \tag{2}$$

where $c = 10^{10}$. The proof involves reducing equation (1) to an inequality involving linear forms in logarithms of algebraic numbers all but one of which are in fact units. Since then, the results on linear forms have been considerably improved and Siegel [5] has given improved estimates for units in algebraic number fields. These results enable us to considerably improve (2) and we can now prove

THEOREM 1. *Given $\varepsilon > 0$, there is an effectively computable constant $c = c(\varepsilon)$ depending only on ε such that if x and y satisfy* (1) *then*

$$\max(|x|, |y|) < e^{c|k|^{1+\varepsilon}}.$$

To put this another way, (2) implies that if x and y are positive integers with $x^3 \neq y^2$ then there is a constant $c' = c'(\varkappa)$ (effectively computable) such that

$$|x^3 - y^2| > c'(\log x)^{\varkappa}$$

where $\varkappa = .0001$ and by Theorem 1, this is now true for any $\varkappa < 1$.

As is well known, to prove Theorem 1, one first reduces equation (1) to a diophantine equation of the form $f(x, y) = m$ where $f(x, y)$ is a homogeneous binary cubic form with integral coefficients. To solve this equation

* Supported in part by NSF Grant No. P28969.

one needs an effective improvement of Liouville's theorem on approximations of algebraic numbers by rational numbers. When one is interested only in improving Liouville's theorem, it is useful to consider linear forms in logarithms of algebraic numbers with one algebraic number having a large height and the others taken as known. In this case the essentially best possible results have obtained [3]. However, in the typical diophantine equation, the known logarithms are as large as the unknown logarithms and [3] is unsuitable. For this purpose we need the result of [7] which is the first general improvement of Baker [2] and is particularly well suited to the problem at hand.

If α is an algebraic number, we let

$$h(\alpha) = \max_{\sigma} |\alpha^{(\sigma)}|$$

where $\alpha^{(\sigma)}$ runs through the conjugates of α. Then if a is the minimum positive rational integer such that $a\alpha$ is an algebraic integer we define the size of α to be the maximum of a and $h(\alpha)$.

THEOREM 2. *Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers of degrees less than or equal to d and sizes less than or equal to $A_1, \ldots, A_n$ respectively where $A_i \geqslant e$ $(1 \leqslant i \leqslant n)$. Suppose $\beta_1, \ldots, \beta_n$ are algebraic numbers of degree $\leqslant d$ and sizes less than $H^{\log H}$ such that*

$$0 < |\beta_1 \log \alpha_1 + \ldots + \beta_n \log \alpha_n| < e^{-H}$$

where the logarithms have their principal values. Then given $\varepsilon > 0$, there exists an effectively computable constant $c = c(n, d, \varepsilon)$ such that

$$H < c\Big(\prod_{i=1}^{n} \log A_i\Big)^{1+\varepsilon}.$$

This is Theorem 2 of [7] except that it is formulated in [7] in terms of heights (the maximum absolute value of the coefficients of the minimal defining polynomial) rather than sizes. However the transition from one formulation to the other is easy and sizes are more convenient here.

Using Theorem 2 we can now prove

THEOREM 3. *Let $f(x, y)$ be an irreducible binary form of degree $n \geqslant 3$ with integral coefficients of absolute value less than or equal to A. Given $\varepsilon > 0$, there exists an effectively computable number $c = c(n, \varepsilon)$ depending only on n and ε such that if x, y and m are integers with*

$$f(x, y) = m$$

then

$$\max(|x|, |y|) < \exp\{c[A^{n(n-1)}(A^{n(n-1)} + \log|m|)]^{1+\varepsilon}\}. \tag{3}$$

This represents a considerable improvement on [1]. However (3) can often be further improved if one has a knowledge of the regulator or discriminant of the field generated by a root of $f(x, 1) = 0$ as will be apparent from Lemma 3. In particular, we see from the regulator form of Lemma 3 that we have improved the recent result of Sprindžuk [6] (however, his result is p-adic and allows m to be multiplied by high powers of fixed primes). It is the discriminant form of Lemma 3 that is most easily applied to Theorem 1.

2. On the units in algebraic number fields. In this section, K will be an algebraic number field of degree n whose discriminant has absolute value D. We suppose that there are r_1 real conjugate fields to K and $2r_2$ complex conjugates to K and that they are chosen in the usual manner: if α is in K then $\alpha^{(i)}$ is real $1 \leqslant i \leqslant r_1$, $\alpha^{(i+r_2)} = \overline{\alpha^{(i)}}$, $r_1+1 \leqslant i \leqslant r_1+r_2$. If $r = r_1+r_2-1$ then there are units $\varepsilon_1, \ldots, \varepsilon_r$ such that every unit of K may be written in the form $\zeta\varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}$ where ζ is a root of unity in K and $a_1, \ldots, a_n$ are integers. We define the regulator R of K to be

$$R = \big|\det(\log|\varepsilon_j^{(i)}|)\big| \qquad (1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant r).$$

Here it is convenient to leave out the factor of 2 that sometimes appears when $i > r_1$ and hence when $r_2 > 0$, R is 2^{1-r_2} times the regulator as given by Siegel [5]. Siegel gives the estimate

$$R < c_1(\log D)^{n-1}\sqrt{D} \tag{4}$$

where c_1 is explicitly given in terms of n, r_1, r_2 and the number of roots of unity in K and hence may be effectively estimated from above in terms of n alone. The numbers $c_2, \ldots, c_8$ in this section are likewise effectively determinable and depend on n alone.

Consider the r linear forms

$$y_i = \sum_{j=1}^{r} x_j \log|\varepsilon_j^{(i)}|, \qquad 1 \leqslant i \leqslant r. \tag{5}$$

If η is a unit of K we let $L(\eta) = \max_{1 \leqslant i \leqslant r} \big|\log|\eta^{(i)}|\big|$. When we apply Minkowski's theorem on consecutive minima to the system of linear forms (5), we get a set of r independant units, $\eta_1, \ldots, \eta_r$ such that

$$L(\eta_1) \ldots L(\eta_r) \leqslant R. \tag{6}$$

Siegel uses (4), (6) and a lower estimate for $L(\eta_1)$ to get estimates for $L(\eta_j)$, $1 \leqslant j \leqslant n$. However, due to the form of the result in Theorem 2, the estimate (6) is more useful than an estimate of each $L(\eta_j)$ separately and indeed gives us better results since there is necessarily some loss in going from (6) to each $L(\eta_j)$ and back to (6).

If α is an algebraic number, we let $M(\alpha) = \max\big|\log|\alpha^{(\sigma)}|\big|$ where $\alpha^{(\sigma)}$ runs through the conjugates of α. If η is a unit in K, we get $M(\eta)$

from $L(\eta)$ by estimating $|\mathrm{Log}\,|\eta^{(r+1)}|\,|$ which, since the norm of η is ± 1, gives

$$M(\eta) \leqslant (n-1)L(\eta).$$

It follows from (6) that

$$M(\eta_1)\dots M(\eta_r) \leqslant c_2 R.$$

Thus for any g and h between 1 and n we have

$$M\left(\frac{\eta_1^{(g)}}{\eta_1^{(h)}}\right)\dots M\left(\frac{\eta_r^{(g)}}{\eta_r^{(h)}}\right) \leqslant 2^r c_2 R \leqslant c_3 R \tag{7}$$

with $c_3 = 2^{n-1}c_2$.

If α is a non-zero algebraic integer which is not a root of unity with size A (which is here $= h(\alpha)$) then

$$\max(1, \log A) < c_4 M(\alpha)$$

where c_4 depends solely upon the degree of α. This is because we may effectively bound $M(\alpha)$ away from zero. That this may be done is shown both in [5] and [7] but the best known bound appears in [4]. Let A_j be the maximum of the size of $\eta_j^{(g)}/\eta_j^{(h)}$ and e. From (4) and (7) we derive immediately

LEMMA 1. *There exist independent units $\eta_1, \dots, \eta_r$ in K such that for any g and h between 1 and n,*

$$\prod_{j=1}^{r} \log A_j \leqslant c_5 R \leqslant c_6 (\log D)^{n-1} D^{1/2},$$

where A_j is the greater of e and the size of $\eta_j^{(g)}/\eta_j^{(h)}$.

Let $E = (\log|\eta_j^{(i)}|)$ $(1 \leqslant i \leqslant r,\ 1 \leqslant j \leqslant r)$ where the η_j are the units above. Set $E^{-1} = (e_{ij})$. We need an estimate for each $|e_{ij}|$. This will be worse than what Siegel gets for the units that he has choosen but it comes at a point that is not harmful.

LEMMA 2. *There are independent units $\eta_1, \dots, \eta_r$ satisfying Lemma 1 such that $|e_{ij}| < c_7$ for all i and j.*

Proof. We calculate E^{-1} from the adjoint matrix to E. We note that $|\det E| \geqslant R$. Since for each J, $1 \leqslant J \leqslant r$ we have $c_8 L(\eta_J) \geqslant 1$, we see that

$$\prod_{\substack{j=1 \\ j\neq J}}^{r} L(\eta_j) \leqslant c_8 R$$

and thus

$$|e_{ij}| \leqslant (r-1)!\, c_8 \leqslant c_7,$$

with $c_7 = (n-2)!\, c_8$.

3. Proof of Theorem 3. Let $f(x, y)$ be an irreducible binary form of degree $n \geqslant 3$ with integral coefficients all of which are bounded in absolute value by A. In particular we let $a \neq 0$ be the coefficient of x^n. Let α be a root of $f(x, 1) = 0$ and $K = Q(\alpha)$. We let D be the absolute value of the discriminant of K and we number the conjugates of K as in Section 2. By Lemmas 1 and 2, there are r independent units $\eta_1, \dots, \eta_r$ of K such that for each g and h, $1 \leqslant g \leqslant n$, $1 \leqslant h \leqslant n$,

$$\prod_{i=1}^{r} \log A_i \leqslant c_5 R \tag{8}$$

where A_i is the maximum of e and the size of $\eta_i^{(g)}/\eta_i^{(h)}$. We note that nA is a trivial upper estimate for the size of α.

Suppose that x, y and m are integers such that

$$f(x, y) = m.$$

By changing signs we may assume x, y and m/a are non-negative. If we set $\beta = x - \alpha y$, this may be written as

$$\beta^{(1)}\dots\beta^{(n)} = m/a = m_1. \tag{9}$$

We assume that

$$y > c_9 |m| A^{4n^3}. \tag{10}$$

The constants $c_9, \dots, c_{25}$ are dependant only upon n and will be assumed to be sufficiently large (where "sufficiently large" is effectively computable); c_{26} and c_{27} will also be dependant upon an $\varepsilon > 0$ to be introduced later. Now $\alpha^{(i)} - \alpha^{(j)} \neq 0$ if $i \neq j$ and

$$|\alpha^{(i)} - \alpha^{(j)}| \leqslant 2nA \tag{11}$$

so that since $a(\alpha^{(i)} - \alpha^{(j)})$ is an algebraic integer,

$$|\alpha^{(i)} - \alpha^{(j)}| \geqslant [A^{n(n-1)}(2nA)^{n(n-1)-1}]^{-1}. \tag{12}$$

Let k be chosen so that $|\beta^{(k)}| \leqslant |\beta^{(j)}|$ for all j. Then for $j \neq k$,

$$|\beta^{(j)}| > c_{10}^{-1} y A^{-2n(n-1)}. \tag{13}$$

Therefore from (9),

$$|\beta^{(k)}| < \frac{m_1}{[c_{10}^{-1} y A^{-2n(n-1)}]^{n-1}} < c_{11}|m| A^{2n^3} y^{-n+1}. \tag{14}$$

This, (10), and (11) give us the estimate for all j,

$$|\beta^{(j)}| \leqslant |\beta^{(j)} - \beta^{(k)}| + |\beta^{(k)}| < c_{12} A y.$$

There exist integers $b_1, \dots, b_r$ such that for $1 \leqslant i \leqslant r$,

$$\left| b_1 \log|\eta_1^{(i)}| + \dots + b_r \log|\eta_r^{(i)}| + \log\left(\frac{|\beta^{(i)}|}{m_1^{1/n}}\right)\right| \leqslant c_{13} \max_{1\leqslant j\leqslant r} L(\eta_j) \leqslant c_{14} R. \tag{15}$$

Let

$$\gamma = \beta\eta_1^{b_1} \dots \eta_r^{b_r}.$$

Then (15) says $\left|\log(|\gamma^{(i)}|/m_1^{1/n})\right| \leqslant c_{14}R$ for $1 \leqslant i \leqslant r$ and since $|\gamma^{(1)} \dots \gamma^{(n)}| = m_1$, we see that

$$\left|\log(|\gamma^{(i)}|/m_1^{1/n})\right| \leqslant c_{15}R, \quad 1 \leqslant i \leqslant n. \tag{16}$$

We may also get bounds for the integers $b_1, \dots, b_r$ from the equations

$$b_1\log|\eta_1^{(i)}| + \dots + b_r\log|\eta_r^{(i)}| = \log\left|\frac{\gamma^{(i)}}{\beta^{(i)}}\right| = \log\left(\frac{|\gamma^{(i)}|}{m_1^{1/n}}\right) + \frac{1}{n}\log m_1 - \log|\beta^{(i)}|.$$

The absolute value of the right side is less than

$$c_{15}R + \frac{1}{n}|\log m_1| + \log(c_{12}Ay) + |\log[m_1/(c_{12}Ay)^{n-1}]|$$

so that by Lemma 2

$$|b_i| \leqslant c_{16}(R + \log|m| + \log A + \log y). \tag{17}$$

We use the identity,

$$(\alpha^{(g)} - \alpha^{(k)})\beta^{(h)} - (\alpha^{(h)} - \alpha^{(k)})\beta^{(g)} = (\alpha^{(g)} - \alpha^{(h)})\beta^{(k)}$$

with $g \neq h \neq k \neq g$. This gives

$$\alpha_1^{b_1} \dots \alpha_r^{b_r}\alpha_{r+1} - 1 = \frac{\alpha^{(g)} - \alpha^{(h)}}{\alpha^{(h)} - \alpha^{(k)}} \cdot \frac{\beta^{(k)}}{\beta^{(g)}}$$

where

$$\alpha_i = \begin{cases} \eta_i^{(g)}/\eta_i^{(h)}, & 1 \leqslant i \leqslant r \\ \dfrac{\alpha^{(g)} - \alpha^{(k)}}{\alpha^{(h)} - \alpha^{(k)}} \cdot \dfrac{\gamma^{(h)}}{\gamma^{(g)}}, & i = r+1. \end{cases}$$

By (11), (12), (13) and (14)

$$|\alpha_1^{b_1}\alpha_2^{b_2} \dots \alpha_r^{b_r}\alpha_{r+1} - 1| < c_{17}A^{4n^3}|m|y^{-n} < y^{-2}. \tag{18}$$

Let $\alpha_0 = -1$, $A_0 = e$. We see from (18) that

$$0 < |b_0\log\alpha_0 + b_1\log\alpha_1 + \dots + b_r\log\alpha_r + \log\alpha_{r+1}| < c_{18}e^{-2\log y} < e^{-\log y}, \tag{19}$$

where b_0 is an integer and makes up for the fact that log denotes the principal value,

$$|b_0| < |b_1| + \dots + |b_r|,$$

and so

$$|b_i| \leqslant c_{19}(R + \log|m| + \log A + \log y), \quad 0 \leqslant i \leqslant r. \tag{20}$$

We have everything we need except for an estimate of the size of α_{r+1}. For this, we see from (11), (12) and (16) that if $\alpha_{r+1}^{(\sigma)}$ is a conjugate of α_{r+1} then

$$|\alpha_{r+1}^{(\sigma)}| \leqslant c_{20}A^{2n(n-1)}\exp(2c_{15}R).$$

Now

$$\frac{a\alpha^{(g)} - a\alpha^{(k)}}{a\alpha^{(h)} - a\alpha^{(k)}}$$

multiplied by the norm, N, of $a\alpha^{(h)} - a\alpha^{(k)}$ is an algebraic integer. We see that

$$|N| < (2nA^2)^{n(n-1)}.$$

The same holds for $a\gamma^{(h)}/a\gamma^{(g)}$; $a\gamma^{(g)}$ is an integer of norm $\leqslant A^n|m|$. Therefore if A_{r+1} is the maximum of e and the size of α_{r+1} then

$$A_{r+1} < c_{21}A^{2n^2}|m|\exp(2c_{15}R). \tag{21}$$

Let $B = \max_i |b_i|$. To estimate B we need to estimate R and hence D. If

$$f(x, 1) = ax^n + a_1x^{n-1} + \dots + a_n$$

then $a\alpha$ is an algebraic integer generating the same field as α and is a root of

$$g(x) = x^n + a_1x^{n-1} + \dots + a^{n-1}a_n = 0.$$

The maximum absolute value of the coefficients of $g(x)$ is $A' \leqslant A^n$. Baker [1] gives the following estimate for the discriminant of $g(x)$ which therefore certainly holds for D,

$$D < c_{22}(A')^{2n-2} \leqslant c_{22}A^{2n(n-1)}. \tag{22}$$

It follows from (4) that

$$R < c_{23}A^{n^2}$$

and now from (20) and our assumption (10),

$$B < c_{24}(A^{n^2} + \log y) < 2c_{24}y < (\log y)^{\log y}.$$

Hence by (8), (21) and Theorem 2, given $\varepsilon > 0$, there are constants c_{25}, c_{26} and c_{27} (the latter two depending upon ε also) such that

$$\begin{aligned} \log y &< c_{26}[c_5R \cdot c_{25}(R + \log A + \log|m|)]^{1+\varepsilon/2} \\ &< c_{27}[D^{1/2}(D^{1/2} + \log A + \log|m|)]^{1+\varepsilon}. \end{aligned} \tag{23}$$

This has been derived under the assumption (10) but (23) is clearly true if (10) is false. We also get precisely the same bound for x by starting with a root of $f(1, y) = 0$. Thus we have proved

LEMMA 3. *Let $f(x, y)$ be an irreducible binary form of degree $n \geqslant 3$ with integral coefficients whose absolute values are bounded above by A. Let α be a root of $f(x, 1) = 0$ and D and R be the absolute value of the discriminant and regulator respectively of $Q(\alpha)$. Let x, y and m be integers such that*

$$f(x, y) = m.$$

Then given $\varepsilon > 0$, there exist effectively computable constants $c = c(n, \varepsilon)$ and $c' = c'(n, \varepsilon)$ such that

$$\max(|x|, |y|) < \exp\{c'[R(R + \log A + \log|m|)]^{1+\varepsilon}\}$$

and

$$\max(|x|, |y|) < \exp\{c[D^{1/2}(D^{1/2} + \log A + \log|m|)]^{1+\varepsilon}\}.$$

Theorem 3 follows from Lemma 3 and (22).

4. Proof of Theorem 1. Suppose

$$y^2 = x^3 + k$$

where $k \neq 0$. We set

$$f(X, Y) = X^3 - 3xXY^2 - 2yY^3$$

and suppose $f(X, Y)$ is irreducible.

The discriminant of f is $-108\,k$ and if α is a root of $f(X, 1) = 0$ then α is an integer and hence the absolute value, D, of the discriminant of $Q(\alpha)$ is bounded above by $108\,|k|$. Baker [1] shows that there is a substitution

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} X_1 \\ Y_1 \end{pmatrix}, \qquad ps - qr = \pm 1 \tag{24}$$

such that

$$\pm f(X, Y) = f_1(X_1, Y_1) = aX_1^3 + bX_1^2 Y_1 + cX_1 Y_1^2 + dY_1^3$$

with

$$\max(|a|, |b|, |c|, |d|) < (108\,|k|)^{1/2}. \tag{25}$$

Further, replacing X_1 and Y_1 by $\pm(sX - qY)$ and $(-rX + pY)$ respectively and identifying the coefficients of X^3 gives

$$f_1(s, -r) = \pm 1.$$

There is a root of $f_1(X_1, 1) = 0$ which generates the same field $Q(\alpha)$ and thus we have an estimate $108\,|k|$ for the discriminant whereas if we used (25) and (22) we would have the much worse result $D < c_{28}|k|^6$. This takes a factor of 6 out of the 10000 all by itself. By Lemma 3,

$$\max(|r|, |s|) \leqslant M = \exp(c\,|k|^{1+\varepsilon}).$$

Further, Baker shows that

$$\max(|x|, |y|) < c_{29} k^2 M^6 < \exp(c_{30}\,|k|^{1+\varepsilon})$$

and this completes the case that $f(x, y)$ is irreducible. The case that $f(x, y)$ is reducible is much simpler and what Baker does already suffices to prove much more than Theorem 1.

Added in proof. The estimate for D in (22) is needlessly high. It is better to use the estimate $c_{22}(A/|a|)^{2n-2}$ for the discriminant of $a^{-1}f(x, 1)$ and use the fact that the discriminant of $g(x)$ is $a^{n(n-1)}$ times this. This gives

$$D < c_{22} A^{n(n-1)} \tag{22'}$$

and improves (3) of Theorem 3 to

$$\max(|x|, |y|) < \exp\{c[A^{n(n-1)/2}(A^{n(n-1)/2} + \log|m|)]^{1+\varepsilon}\}. \tag{3'}$$

References

[1] A. Baker, *Contributions to the theory of diophantine equations II: the diophantine equation $y^2 = x^3 + k$*, Philos. Trans. Roy. Soc. London Ser. A 263 (1967/68), pp. 193–208.

[2] — *Linear forms in the logarithms of algebraic numbers IV*, Mathematika 15 (1968), pp. 204–216.

[3] A. Baker and H. M. Stark, *On a fundamental inequality in number theory*, Ann. Math. 94 (1971), pp. 190–199.

[4] P. E. Blanksby and H. L. Montgomery, *Algebraic integers near the unit circle*, Acta Arith. 18 (1971), pp. 355–369.

[5] C. L. Siegel, *Abschätzung von Einheiten*, Nachr. Akad. Wiss. Göttingen Math. Phys. Kl. II (1969), pp. 71–86.

[6] V. G. Sprindžuk, *On the estimate of the solutions of Thue's equation* (in Russian), Izv. Akad. Nauk SSSR Ser. Mat. 36 (1972), pp. 744–773.

[7] H. M. Stark, *Further advances in the theory of linear forms in logarithms*, Proceedings of the conference on Diophantine Approximation and its Applications held in Washington D. C. in 1972, to appear.

Received on 10. 10. 1972 (337)