CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

1

ON EFFECTIVE APPROXIMATIONS TO CUBIC IRRATIONALS

A. Baker and C. L. Stewart*

1. Introduction

The problem of obtaining effective measures of irrationality for algebraic irrationals has recently attracted considerable attention. The first result in this field was discovered by Baker [1], [2] in 1964. He used properties of hypergeometric series to obtain effective results for certain fractional powers of rationals. It was shown, in particular, that for all rationals p/q with $q > 0$ we have

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^{\kappa}}, \tag{1}$$

where $\alpha = \sqrt[3]{2}$, $c = 10^{-6}$ and $\kappa = 2.955$. A similar result was established for instance for $\alpha = \sqrt[3]{19}$ with $c = 10^{-9}$ and $\kappa = 2.56$. This work was recently refined by Chudnovsky [11]; by a careful study of the Padé approximants occurring in the hypergeometric method he obtained more precise values for κ and consequently he was able to deal with a wider range of algebraic numbers. Chudnovsky left the values for c occurring in his results unspecified but these have recently been established in some special cases by Easton [13]. Easton has shown in particular that (1) holds with $\alpha = \sqrt[3]{28}$, $c = 7.5 \times 10^{-7}$ and $\kappa = 2.9$.

The results above improved upon the relatively crude inequality of Liouville established in 1844 to the effect that (1) holds for any algebraic number α, where $\kappa = n$, $n \geq 1$, the degree of α and c is an effectively computable positive number depending only on α. The first general effective improvement on Liouville's theorem was obtained by Baker [3] in 1968 using the theory of linear forms in the logarithms of algebraic

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

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

numbers. A more precise version of the result was obtained subsequently by Feldman [14] and an explicit formulation of the theorem has recently been given by Győry and Papp [15]. In the present paper we shall sharpen the result of Győry and Papp in the case of cube roots of integers. We shall prove the following result.

Theorem 1. *Let a be a positive integer not a perfect cube, and let $\alpha = \sqrt[3]{a}$. Further let ϵ be the fundamental unit in the field $\mathbf{Q}(\sqrt[3]{a})$. Then* (1) *holds for all rational numbers p/q, $q > 0$, with $c = 1/(3ac_1)$ and $\kappa = 3 - 1/c_2$, where*

$$c_1 = \epsilon^{(50 \log\log \epsilon)^2}, \qquad c_2 = 10^{12} \log \epsilon. \tag{2}$$

Here $\mathbf{Q}$ denotes, as usual, the field of rational numbers and by the fundamental unit ϵ in $\mathbf{Q}(\sqrt[3]{a})$ we mean the smallest unit in the field larger than 1. Note that some authors adopt the alternative convention that the fundamental unit lies between 0 and 1. The result of Győry and Papp mentioned above yields a theorem similar to Theorem 1 but with

$$c_2 = 300^{60} \log \epsilon (\log\log \epsilon)^2 \tag{3}$$

and with a value for c_1 slightly greater than $(40a)^6\epsilon$. In both (2) and (3) we have made use of the fact, established in §2 below, that $\log \epsilon > 1$ for all fields $\mathbf{Q}(\sqrt[3]{a})$. Although our value for c_2 improves substantially on (3), the value for κ that it furnishes is far from the exponent $2+\delta$, $\delta > 0$, occurring in the Thue-Siegel-Roth theorem. As is well known the latter theorem is ineffective, that is, it does not provide an explicit value for the constant c in (1). But Bombieri [8] and Bombieri and Mueller [9] have recently shown that in certain special cases effective results can in fact be derived from the Thue-Siegel method. Nevertheless the restrictions attaching to α in their work are very stringent at present.

The inequality established in Theorem 1 is essentially equivalent to an upper bound for the solutions of the Diophantine equation

$$x^3 - ay^3 = n. \tag{4}$$

We have the following result.

Theorem 2. *Let a and n be positive integers with a not a perfect cube. Then all solutions in integers x and y of* (4) *satisfy*

$$\max(|x|, |y|) < (c_1 n)^{c_2},$$

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

where c_1 and c_2 are given by (2).

In order to derive Theorem 1 from Theorem 2 we denote by p/q, $q > 0$, any rational number and we suppose that $|\alpha - p/q| \leq c$; then $|p/q| \leq \alpha + c$, whence

$$\left|\alpha^2 + \alpha(p/q) + (p/q)^2\right| \leq 3\alpha^2 + 3\alpha c + c^2 \leq 3a.$$

This gives

$$\left|a - (p/q)^3\right| \leq 3a\left|\alpha - p/q\right|. \tag{5}$$

We now apply Theorem 2 with $n = |p^3 - aq^3|$ and conclude that $q < (c_1 n)^{c_2}$ whence $n > (1/c_1)q^{1/c_2}$. By (5) we have $\left|\alpha - p/q\right| \geq n/(3aq^3)$ and our result follows.

The proof of Theorem 2 is based essentially on the methods of [3] and [4]. In particular we reduce the problem to the study of a linear form in three logarithms and we ultimately establish the bound $2{\cdot}10^{12}\log(c_1 n)$ for the size of the integer coefficients in that form. Our exposition will follow the general pattern of the earlier papers but we shall use a simplified auxiliary function, and also a more efficient extrapolation procedure to which Kummer theory can be applied directly. The work here together with the technique of Baker and Davenport [6] would enable the complete list of solutions of (4) to be computed for any moderately sized a and n. Indeed we have $\log\epsilon < (0.37)d^{1/2}(\log d)^2$ where d is the absolute value of the discriminant of $\mathbf{Q}(\sqrt[3]{a})$ (see [18]); thus, since $d \leq 27a^2$ we obtain, for $a > 3$,

$$\log c_1 \leq (50\log d)^2 \log\epsilon \leq (37\log a)^4 a.$$

Hence if, for example, $a \leq 10^3$ and $\log n \leq 10^{10}$ then the coefficients of the logarithms in the linear form will have sizes at most 10^{25}.

As a particular instance of Theorem 1 we take $\alpha = \sqrt[3]{5}$; this is the smallest cube root not covered by the papers employing the hypergeometric method. Then $\epsilon = 41 + 24\alpha + 14\alpha^2$ (see [10], Table 2, p. 270) and $\log\epsilon < 5$. Hence we conclude that (1) holds with $c = 10^{-12900}$ and

$$\kappa = 2.9999999999998.$$

We should like to express our thanks to Professor D. Djokovic for his generous assistance in the computational work referred to in §3. The latter was carried out while the first author was visiting the University of Waterloo and he is grateful for their hospitality.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

2. Preliminary lemmas

We shall require modified forms of two classical lemmas in transcendence theory. First we obtain the following sharpening of Lemma 4 of Baker and Stark [7].

Lemma 1. *Suppose that α, β are elements of an algebraic number field and that for some positive integer p we have $\alpha = \beta^p$. If a, b are the leading coefficients in the field polynomials defining α, β respectively then $b \leq a^{1/p}$.*

Here the field polynomials are, as usual, powers of the minimal polynomials with degree D, where D denotes the degree of the field. Lemma 4 of [7] gives the weaker inequality $b \leq a^{D/p}$, where a denotes any non-zero integer such that $a\alpha$ is an algebraic integer.

Proof. Let $\alpha^{(1)}, \ldots, \alpha^{(D)}$ and $\beta^{(1)}, \ldots, \beta^{(D)}$ be the field conjugates of α and β respectively. Then b is the least positive integer such that

$$f(x) = b(x - \beta^{(1)}) \ldots (x - \beta^{(D)})$$

has rational integer coefficients. We write

$$g(x) = a(x^p - \alpha^{(1)}) \ldots (x^p - \alpha^{(D)}), \qquad h(x) = \prod_{j=1}^{p} f(xe^{2\pi ij/p}).$$

Since, by hypothesis, $\alpha = \beta^p$ we have

$$b^p g(x) = (-1)^{D(p+1)} a h(x).$$

Arguing as in [7] we deduce from the algebraic generalization of Gauss' lemma that $h(x)$ has relatively prime rational integer coefficients. But $g(x)$ also has rational integer coefficients and so b^p divides a, whence $b \leq a^{1/p}$ as required.

Secondly, we shall establish a version of Siegel's lemma appropriate to our work here. We shall adapt the result of Dobrowolski [12] so as to deal with linear forms with arbitrary algebraic coefficients, not merely algebraic integers. Obviously it would suffice to multiply through each equation by a suitable common denominator but this would be too crude for our purpose. In order to state the lemma, we define K to be an algebraic number field with degree n over $\mathbf{Q}$ and we let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K in the complex numbers. Further we signify by b_{ij}, $1 \leq i \leq N$, $1 \leq j \leq M$, elements of K such that for each j not all b_{ij},

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

$1 \le i \le N$, are zero. We now define c_j, $1 \le j \le M$, to be a positive integer such that

$$c_j \sigma_1(b_{i_1,j}) \dots \sigma_n(b_{i_n,j})$$

is an algebraic integer for all choices of $i_1, \dots, i_n$.

Lemma 2. *If $N > nM$ then the system of equations*

$$\sum_{i=1}^{N} b_{ij} x_i = 0, \qquad 1 \le j \le M,$$

has a solution in rational integers $x_1, \dots, x_N$, not all 0, with absolute values at most

$$Y = \left(2\sqrt{2}(N+1) Z^{1/(nM)}\right)^{nM/(N-nM)},$$

where

$$Z = \prod_{j=1}^{M} \left(c_j \prod_{k=1}^{n} \max_i |\sigma_k(b_{ij})|\right).$$

Proof. The proof follows almost verbatim that of Dobrowolski [12]. the main idea is to select rational integers $x_1, \dots, x_N$ by the box principle such that

$$\left| c_j N_{K/\mathbf{Q}} \left(\sum_i b_{ij} x_i \right) \right| < 1, \qquad 1 \le j \le M.$$

This differs from [12] by virtue of the presence of c_j; our definition of c_j ensures that the expression on the left of the above inequality is a rational integer. The only significant modification in the proof concerns the quantity

$$C_j = \left(c_j \prod_{k=1}^{n} \max_i |\sigma_k(b_{ij})|\right)^{1/n}$$

which now includes c_j. This leads to the definition

$$\ell_j = (Y^N/Z)^{1/(nM)} C_j,$$

which gives

$$2\sqrt{2}(N+1) Y C_j - \ell_j = 0$$

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

as in [12]. Further, as there, we note that $C_j \geq 1$ and hence also $Y \geq 1$; this follows from our definition of c_j and the assumption that, for each j, not all b_{ij} are zero.†

We now record three lemmas that will be needed later. Lemma 3 is classical Kummer theory; for a proof see Baker and Stark [7]. Lemma 4 is a famous result of Delaunay and Nagell; for a proof see Nagell [17]. Lemma 5 is due to Ljunggren [16].

Lemma 3. *Let $\alpha_1, \ldots, \alpha_n$ be non-zero elements of an algebraic number field K and let $\alpha_1^{1/p}, \ldots, \alpha_{n-1}^{1/p}$ denote fixed pth roots for some prime p. Further, let $K' = K(\alpha_1^{1/p}, \ldots, \alpha_{n-1}^{1/p})$. Then either $K'(\alpha_n^{1/p})$ is an extension of K' of degree p or we have*

$$\alpha_n = \alpha_1^{j_1} \ldots \alpha_{n-1}^{j_{n-1}} \gamma^p$$

for some γ in K and some integers $j_1, \ldots, j_{n-1}$ with $0 \leq j_\ell < p$.

Lemma 4. *Let a be a positive integer, not a perfect cube. The equation*

$$x^3 - ay^3 = 1$$

has at most one solution in integers x, y with $y \neq 0$ and, for this, $x - y\sqrt[3]{a}$ is given by either $1/\epsilon$ or $1/\epsilon^2$, where ϵ is the fundamental unit of $\mathbb{Q}(\sqrt[3]{a})$ as in §1.

Lemma 5. *Let A, B, C be positive integers with $C = 1$ or $C = 3$ and suppose that A and B are > 1 when $C = 1$. Suppose further that AB is not divisible by 3 when $C = 3$. Then the equation*

$$Ax^3 + By^3 = C$$

has at most one solution in integers x, y and for this, $C^{-1}(x\sqrt[3]{A} + y\sqrt[3]{B})^3$ is either $1/\eta$ or $1/\eta^2$ where η is the fundamental unit in $\mathbb{Q}(\sqrt[3]{(AB^2)})$. The only exception is the equation $2x^3 + y^3 = 3$ which has two solutions, namely $x = y = 1$ and $x = 4$, $y = -5$.

Note that if the condition in Lemma 5 that AB be not divisible by 3 when $C = 3$ is violated then the equation reduces to an equation with

† Professor Vaaler has pointed out to us that the result can also be obtained from Theorem 9 of Bombieri and Vaaler, "On Siegel's Lemma", *Invent. Math.* **73** (1983), 11–32, and in fact with $\sqrt{N}$ in place of $2\sqrt{2}\,(N+1)$.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

$C = 1$. Note further that if the condition that A and B be > 1 when $C = 1$ is violated then the equation reduces to one of the kind considered in Lemma 4. Hence, taking into account the possible replacement of x or y by $-x$ or $-y$, we see that the lemmas incorporate all equations $Ax^3 + By^3 = C$, where A, B are any integers and $C = 1$ or $C = 3$.

Now these results of Delaunay, Nagell and Ljunggren can be viewed as providing the complete solution to (4) when n divides the discriminant $-27a^2$ of $x^3 - a$; it is precisely this condition that will arise in our discussion later. In particular, we see that Theorem 2 certainly holds in this case. To verify the assertion, note that if n^2 divides $27a^2$ then n divides $3a$ and so also n divides $3x^3$. We write $3x^3/n = Az^3$ where A, z are integers and A divides $3n^2$. Further we put $B = -3a/n$ and $C = 3$. Then $Az^3 + By^3 = C$ and $AB^2 = (3x/nz)^3 a^2$. Hence Lemmas 4 and 5 give the possible values of y, z and thus also x, in terms of the fundamental unit ϵ in $\mathbf{Q}(\sqrt[3]{a})$.

3. On units in purely cubic fields

Let a be a positive integer, not a perfect cube and let $\alpha = \sqrt[3]{a}$ as in §1. Let ω be a primitive cube root of unity and put $\alpha' = \omega\alpha$, $\alpha'' = \omega^2\alpha$. Further let ϵ be the fundamental unit in $\mathbf{Q}(\alpha)$ with $\epsilon > 1$ as in §1. We define ϵ', ϵ'' to be the conjugates of ϵ corresponding to α', α'' and we put $\rho = \epsilon''/\epsilon'$. Throughout the paper, logarithms will have their principal values.

Lemma 6. *We have* $\log\epsilon > 1$. *Further, if* $\log\epsilon \le 3$ *then* $\mathbf{Q}(\alpha)$ *is* $\mathbf{Q}(\sqrt[3]{m})$ *where* m *is one of* 2, 3, 7, 19, 28. *Furthermore, if* $\mathbf{Q}(\alpha)$ *is not* $\mathbf{Q}(\sqrt[3]{28})$ *then we have* $|\log\rho| < \frac{\pi}{3}\log\epsilon$.

Proof. Since $\epsilon\epsilon'\epsilon'' = \epsilon|\epsilon'|^2 = 1$, the minimal polynomial defining ϵ has the form

$$x^3 + bx^2 + cx - 1.$$

Here b, c are integers and

$$b = -(\epsilon + \epsilon' + \epsilon''), \qquad c = \epsilon\epsilon' + \epsilon\epsilon'' + \epsilon'\epsilon''.$$

We have

$$-(\epsilon + 2/\epsilon^{1/2}) \le b \le 0, \qquad |c| \le 2\epsilon^{1/2} + 1/\epsilon.$$

If $\log\epsilon \le 3$ these give $-21 \le b \le 0$, $|c| \le 9$. The discriminant of the polynomial is

$$d = b^2c^2 + 4b^3 - 4c^3 - 27 - 18bc.$$

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

Now the discriminant of $\mathbf{Q}(\sqrt[3]{a})$ divides the discriminant $-27a^2$ of $x^3 - a$ and so it has the form $-3k^2$ for some divisor k of $3a$. Hence $d = -3\ell^2$ for some multiple ℓ of k. A computer search shows that the only possible b, c in the above ranges for which $d = -3\ell^2$ for some integer ℓ are given by $(-3,-3)$, $(-12,-6)$, $(-12,6)$, $(-14,2)$, $(-5,-1)$, $(-15,3)$, $(0,0)$ and $(-2,2)$. We find that the corresponding equations have precisely one real root; in the case of the first five pairs on the list the root is given respectively by

$$\begin{aligned}
1 + \sqrt[3]{2} + (\sqrt[3]{2})^2 &= 3.84\ldots \\
4 + 3\sqrt[3]{3} + 2(\sqrt[3]{3})^2 &= 12.48\ldots \\
4 + 2\sqrt[3]{7} + (\sqrt[3]{7})^2 &= 11.48\ldots \\
\tfrac{1}{3}\left(14 + 5\sqrt[3]{19} + 2(\sqrt[3]{19})^2\right) &= 13.86\ldots \\
\tfrac{1}{6}\left(10 + 4\sqrt[3]{28} + (\sqrt[3]{28})^2\right) &= 5.22\ldots
\end{aligned}$$

The sixth pair in the first list, that is $(-15,3)$, corresponds to an equation with real root $1/(\sqrt[3]{2}-1)^2$; this is the square of the first root above. The last two pairs of admissible values of (b,c), namely $(0,0)$ and $(-2,2)$, correspond to reducible equations with real root 1. This establishes the first two assertions of the lemma.

For the last assertion we note that $|\rho| = 1$ and so $|\log\rho| \leq \pi$. Hence the required inequality certainly holds if $\log\epsilon > 3$. If $\log\epsilon \leq 3$ we have the five possibilities for m above, and it is readily checked that the corresponding values of $|\log\rho|/(\pi\log\epsilon)$ are 0.27, 0.13, 0.13, 0.31, 0.50 to two decimal places. This establishes the result.

Let now $K = \mathbf{Q}(\alpha,\omega)$. We define σ as either $-\omega$ or $-\omega^2$ so that the real numbers $i\log\rho$ and $i\log\sigma$ have opposite signs.

Lemma 7. *$K(\rho^{1/2},\sigma^{1/2})$ is an extension of K of degree 4.*

Proof. First we show that $[K(\rho^{1/2}) : K] = 2$. We have $\epsilon\epsilon'\epsilon'' = 1$ and so $\rho = \epsilon''/\epsilon' = 1/\epsilon(\epsilon')^2$. Hence if $K(\rho^{1/2})$ were not an extension of K with degree 2 then we would have $\epsilon = \eta^2$ for some $\eta \in K$. Thus $\epsilon^{1/2}$ is in K. But ϵ is the fundamental unit in $\mathbf{Q}(\alpha)$ whence $\epsilon^{1/2}$ is not in $\mathbf{Q}(\alpha)$ and thus $\mathbf{Q}(\alpha,\epsilon^{1/2})$ is a field with degree 6 over $\mathbf{Q}$. On the other hand, K has degree 6 and is not a real field whence K is not $\mathbf{Q}(\alpha,\epsilon^{1/2})$. Thus $\epsilon^{1/2}$ is not in K, a contradiction.

Secondly, we show that $\left[K(\rho^{1/2},\sigma^{1/2}) : K(\rho^{1/2})\right] = 2$. If this does not hold then $\sigma^{1/2}$ is in $K(\rho^{1/2})$. But $K(\rho^{1/2}) = K(\epsilon^{1/2})$ and so $i =$

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

$\lambda + \mu\omega$ for some λ, μ in $\mathbf{Q}(\alpha, \epsilon^{1/2})$. This gives $2i = \mu(\omega - \omega^2)$, that is $2 = \pm\sqrt{3}\,\mu$. Hence $\sqrt{3} = \gamma + \delta\epsilon^{1/2}$, where γ, δ are in $\mathbf{Q}(\alpha)$. Thus $3 = \gamma^2 + \epsilon\delta^2 + 2\gamma\delta\epsilon^{1/2}$. If $\gamma\delta \neq 0$ then this implies that $\epsilon^{1/2}$ is in $\mathbf{Q}(\alpha)$, a contradiction. We cannot have $\delta = 0$ for this would give $\sqrt{3} = \gamma$, contrary to the fact that $\mathbf{Q}(\alpha)$ does not have a quadratic subfield. Hence $\gamma = 0$ and thus $\sqrt{3} = \delta\epsilon^{1/2}$. This gives $3 = \delta^2\epsilon$ and consequently, taking norms from $\mathbf{Q}(\alpha)$ to $\mathbf{Q}$, we get $27 = (N\delta)^2$, a contradiction since $N\delta$ is rational. This proves the result.

4. Reduction to a linear form in logarithms

Let n be a positive integer and let x, y be integers satisfying (4). With the notation of §3 we have

$$(x - \alpha y)(x - \alpha' y)(x - \alpha'' y) = n.$$

We shall prove that if $n > c_1$ then

$$\max(|x|, |y|) < n^{c_2}. \tag{6}$$

This will suffice to establish Theorem 2. For if $n \leq c_1$ then we put

$$x_1 = Cx, \qquad y_1 = Cy, \qquad n_1 = C^3 n,$$

where $C = \left[(c_1/n)^{1/3}\right] + 1$; this gives $x_1^3 - ay_1^3 = n_1$ with $n_1 > c_1$, whence, by (6), we have

$$\max(|x_1|, |y_1|) < (c_1^{1/3} + n^{1/3})^{3c_2}$$

and Theorem 2 follows.

We now show that we can assume that the quotient

$$\nu = (x - \alpha'' y)/(x - \alpha' y)$$

is not a unit in K. Put

$$x_2 = x/(x, y), \qquad y_2 = y/(x, y), \qquad n_2 = n/(x, y)^3.$$

Then x_2, y_2 are relatively prime and we have $x_2^3 - ay_2^3 = n_2$. Further we have

$$(\alpha'' - \alpha')x_2 = (x_2 - \alpha' y_2)(\alpha'' - \alpha'\nu),$$
$$(\alpha'' - \alpha')y_2 = (x_2 - \alpha' y_2)(1 - \nu).$$

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-0-521-09029-2 - New Advances in Transcendence Theory
Edited by Alan Baker
Excerpt
More information

Hence, if ν is a unit, then, taking norms from K to $\mathbf{Q}$, we find that $N(x_2-\alpha' y_2)$ divides $N(\alpha''-\alpha')N(x_2)$ and $N(\alpha''-\alpha')N(y_2)$. But $N(x_2)$ and $N(y_2)$ are relatively prime whence $N(x_2-\alpha' y_2)$ divides $N(\alpha''-\alpha')$, that is n_2^2 divides $27a^2$. We have $(x,y) \leq n$ and hence $|x| \leq n|x_2|$, $|y| \leq n|y_2|$. Now Lemmas 4 and 5 give bounds for x_2, y_2 in terms of the fundamental unit in $\mathbf{Q}(\alpha)$ as in §2, and Theorem 2 follows in this case.

We define $\beta = (x-\alpha y)\epsilon^j$, where j is the integer such that

$$1 \leq n^{-1/3}|\beta| < \epsilon.$$

We put

$$\beta' = (x-\alpha' y)\epsilon'^j, \qquad \beta'' = (x-\alpha'' y)\epsilon''^j.$$

Then $\beta\beta'\beta'' = n$ and since $|\beta'| = |\beta''|$ we obtain

$$\epsilon^{-1/2} < n^{-1/3}|\beta'| \leq 1.$$

We shall assume in the sequel that

$$j > 2(10^{12}-1)\log n \tag{7}$$

and we shall ultimately derive a contradiction. This will suffice to prove Theorem 2; for we have $|\beta'| \leq n^{1/3}$, whence

$$|x-\alpha' y| \leq n^{1/3}|\epsilon'|^{-j} = n^{1/3}\epsilon^{j/2}.$$

Thus if (7) does not hold then $|x-\alpha' y| \leq n^{c_2-2/3}$. But since the imaginary part of ω is $\pm\sqrt{3}/2$ this gives $|\alpha y| < (2/\sqrt{3})n^{c_2-2/3}$. We have $n > c_1$ and $|x| \leq |\alpha y| + |x-\alpha' y|$, and (6) follows.

We now consider the number $\lambda = -\omega\beta''/\beta'$. Ideally we would like $\lambda^{1/2}$ to generate an extension of $K(\rho^{1/2}, \sigma^{1/2})$ of degree 2; but this is not necessarily so. We overcome the problem by substituting τ for λ as described below. Our argument is apparently novel and more efficient than those applied previously in this context. Let $v \geq 0$ be an integer such that

$$\lambda = \rho^{t'}\sigma^{t''}\tau^t, \tag{8}$$

where $t = 2^v$ and t', t'' are integers with $0 \leq t' < t$, $0 \leq t'' < t$ and τ is in K. Plainly at least one such v exists since we can take $t' = t'' = 0$ and $t = 1$. We proceed to prove that $t < 3\log n$. Now λ is an element of K and the leading coefficient in the field polynomial of λ divides n^2. Since ρ and σ are units, the same holds for the field polynomial of τ^t. It follows from Lemma 1 that the leading coefficient, say q, in the field polynomial

© Cambridge University Press www.cambridge.org