New Advances in Transcendence Theory
Cambridge University Press, 1988.

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.

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* *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 $|\alpha - p/q| \le c$; then $|p/q| \le \alpha + c$, whence

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

This gives

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

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 $|\alpha - p/q| \ge n/(3aq^3)$ 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 $\mathbb{Q}(\sqrt[3]{a})$ (see [18]); thus, since $d \le 27a^2$ we obtain, for $a > 3$,

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

Hence if, for example, $a \le 10^3$ and $\log n \le 10^{10}$ 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.

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 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},

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

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

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

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

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

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

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

where

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

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

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

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

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

which now includes c_j. This leads to the definition

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

which gives

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

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, $C^{-1}\left(x\sqrt[3]{A} + y\sqrt[3]{B}\right)^3$ is either $1/\eta$ or $1/\eta^2$ where η is the fundamental unit in $\mathbb{Q}\left(\sqrt[3]{(AB^2)}\right)$. 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 $2\sqrt{2}\,(N+1)$.

$C = 1$. 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 $\mathbb{Q}(\sqrt[3]{a})$.

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 $\mathbb{Q}(\alpha)$ 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* $\log\epsilon \leq 3$ *then* $\mathbb{Q}(\alpha)$ *is* $\mathbb{Q}(\sqrt[3]{m})$ *where* m *is one of* 2, 3, 7, 19, 28. *Furthermore, if* $\mathbb{Q}(\alpha)$ *is not* $\mathbb{Q}(\sqrt[3]{28})$ *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

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

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

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

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

$$1+\sqrt[3]{2}+(\sqrt[3]{2})^2=3.84\ldots$$

$$4+3\sqrt[3]{3}+2(\sqrt[3]{3})^2=12.48\ldots$$

$$4+2\sqrt[3]{7}+(\sqrt[3]{7})^2=11.48\ldots$$

$$\tfrac{1}{3}\left(14+5\sqrt[3]{19}+2(\sqrt[3]{19})^2\right)=13.86\ldots$$

$$\tfrac{1}{6}\left(10+4\sqrt[3]{28}+(\sqrt[3]{28})^2\right)=5.22\ldots$$

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 $i=$

$\lambda + \mu\omega$ 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

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

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

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 $(x,y)\le n$ and hence $|x|\le n|x_2|$, $|y|\le n|y_2|$. 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

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

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

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

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 $|\beta'|\le n^{1/3}$, whence

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

Thus if (7) does not hold then $|x-\alpha' y|\le n^{c_2-2/3}$. 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 $|x|\le|\alpha y|+|x-\alpha' y|$, 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 $v\ge 0$ be an integer such that

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

where $t=2^v$ and t', t'' are integers with $0\le t'<t$, $0\le t''<t$ 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 of τ satisfies $q \le n^{2/t}$. Suppose now that $t \ge 3\log n$. Then, since q is assumed to be positive, we have $q = 1$. Hence τ is an algebraic integer and thus also λ is an algebraic integer. But we have $\nu = -\omega^2\rho^{-j}\lambda$ and it follows that ν is an algebraic integer. On the other hand, it is an immediate consequence of the definition of ν that its norm is 1. Thus ν is a unit contrary to our assumption above. We shall suppose henceforth that v is the largest integer such that (8) holds. Then, by Lemma 3, $\tau^{1/2}$ generates an extension of $K(\rho^{1/2}, \sigma^{1/2})$ of degree 2. Further, by Lemma 7, we see that $K(\rho^{1/2}, \sigma^{1/2}, \tau^{1/2})$ is an extension of K with degree 8.

We require estimates for the conjugates of τ. For this purpose we observe that the field conjugates of ρ are ϵ''/ϵ', ϵ'/ϵ'', ϵ/ϵ', ϵ/ϵ'', ϵ'/ϵ, ϵ''/ϵ and these have absolute values 1, 1, $\epsilon^{3/2}$, $\epsilon^{3/2}$, $\epsilon^{-3/2}$, $\epsilon^{-3/2}$ respectively. Further, from our estimates for $|\beta|$, $|\beta'|$ above we see that four of the conjugates of λ have absolute values at most 1 and the other two have absolute value at most $\epsilon^{3/2}$. Hence from (8) we see that two of the conjugates of τ^t have absolute values at most $\epsilon^{(3/2)(t'+1)}$ and the remainder have absolute value at most 1. Since $t'+1 \le t$, it follows that two of the conjugates of τ have absolute value at most $\epsilon^{3/2}$ and the remainder have absolute value at most 1.

We now derive the basic inequality involving a linear form in logarithms. We have the identity

$$\beta\epsilon^{-j}(\alpha' - \alpha'') + \beta'\epsilon'^{-j}(\alpha'' - \alpha) + \beta''\epsilon''^{-j}(\alpha - \alpha') = 0.$$

Hence

$$\frac{\beta''}{\beta'}\left(\frac{\epsilon'}{\epsilon''}\right)^j \frac{\alpha - \alpha'}{\alpha'' - \alpha} + 1 = \frac{\beta}{\beta'}\left(\frac{\epsilon'}{\epsilon}\right)^j \frac{\alpha'' - \alpha'}{\alpha'' - \alpha}$$

and thus

$$\lambda\rho^{-j} - 1 = (\beta/(\omega\beta'))(\epsilon'/\epsilon)^j.$$

As above we have $|\beta/\beta'| < \epsilon^{3/2}$ and $|\epsilon'/\epsilon| = \epsilon^{-3/2}$. This gives

$$|\lambda\rho^{-j} - 1| < \epsilon^{-(3/2)(j-1)}.$$

We substitute for λ from (8) and obtain

$$|\rho^{t'-j}\sigma^{t''}\tau^t - 1| < \epsilon^{-(3/2)(j-1)}.$$

Since, for any complex number z, the inequality $|e^z - 1| < 1/4$ implies that $|z - ik\pi| \le 4|e^z - 1|$ for some rational integer k, we deduce that

$$\left|r\log\rho + s\log\sigma - t\log\tau\right| < 4\epsilon^{-(3/2)(j-1)}, \tag{9}$$

where $r = j - t'$ and s is a rational integer. We recall here that $t = 2^v < 3 \log n$ and that the logarithms have their principal values. Since $0 \le t' < t$, we see from (7) that $0 < r \le j$. Further we observe that

$$|s \log \sigma| \le \pi(r + t) + 1$$

and thus, since $\log \sigma = \pm \frac{\pi}{3} i$, we have

$$|s| \le 3(r + t) + 1 \le 3j + 10 \log n.$$

5. The auxiliary function

We shall now assume that (7) and (9) hold and that $n > c_1$, and we shall eventually deduce a contradiction. By virtue of the results referred to in §1 we can suppose that $\mathbf{Q}(\alpha)$ is not $\mathbf{Q}(\sqrt[3]{2})$ or $\mathbf{Q}(\sqrt[3]{28})$ (see [2], [13]).

We put $u = \max(1, v)$ and $h = 500u$. Further we put $L = \frac{2}{5}(j/h) \log \epsilon$ and we write

$$L_1 = [10^{-2} L / \log \epsilon], \qquad L_2 = [10^{-2} L], \qquad L_3 = [2 \cdot 5^7 L h^2 / j].$$

Then for any non-negative integers m_1, m_2 we define the function

$$f(z; m_1, m_2) = \sum_{\lambda_1=0}^{L_1} \sum_{\lambda_2=0}^{L_2} \sum_{\lambda_3=0}^{L_3} p(\lambda) \Delta(t\gamma_1; m_1) \Delta(t\gamma_2; m_2) \rho^{\gamma_1 z} \sigma^{\gamma_2 z},$$

where

$$\gamma_1 = \lambda_1 + (r/t)\lambda_3, \qquad \gamma_2 = \lambda_2 + (s/t)\lambda_3,$$

and the $p(\lambda) = p(\lambda_1, \lambda_2, \lambda_3)$ are integers to be determined later. The Δ-polynomials are defined, as usual, by

$$\Delta(x; 0) = 1, \quad \Delta(x; k) = (x+1) \ldots (x+k)/k!, \qquad k \ge 1,$$

and z^w means $e^{z \log w}$ where the logarithm has its principal value. We also introduce the function

$$g(z; m_1, m_2) = \sum_{\lambda_1=0}^{L_1} \sum_{\lambda_2=0}^{L_2} \sum_{\lambda_3=0}^{L_3} p(\lambda) \Delta(t\gamma_1; m_1) \Delta(t\gamma_2; m_2) \rho^{\lambda_1 z} \sigma^{\lambda_2 z} \tau^{\lambda_3 z}.$$

The coefficients $p(\lambda)$ are chosen so that $g(\ell; m_1, m_2) = 0$ for all odd integers ℓ with $1 \leq \ell \leq 2h$ and all non-negative integers m_1, m_2 with $m_1 + m_2 \leq L$. The number of such m_1, m_2 is $H = (1/2)(L+1)(L+2)$ and thus we have to solve $M = Hh$ linear equations in the $N = (L_1+1)(L_2+1)(L_3+1)$ unknowns $p(\lambda)$. By the definition of L we have $N > (25/4)L^2h$ and, from (7), it follows that $N > 12M$. We shall apply Lemma 2 with $K = \mathbb{Q}(\alpha, \omega)$ so that $n = 6$; we conclude that there exist rational integers $p(\lambda)$, not all 0, such that

$$|p(\lambda)| \leq 2\sqrt{2}(N+1)Z^{1/(6M)} \tag{10}$$

and our purpose now is to determine a bound for the quantity Z referred to in the lemma.

First we shall establish estimates for the Δ-polynomials. We shall write, for brevity,

$$U(m_1, m_2) = \max_{\lambda_1, \lambda_2, \lambda_3} |\Delta(t\gamma_1; m_1)\Delta(t\gamma_2; m_2)|.$$

Lemma 8. *We have*

$$U(m_1, m_2) \leq (2 \cdot 10^{11}t)^{m_1+m_2}2^{2L}.$$

Proof. We begin by noting that

$$L_3/L \leq 2 \cdot 5^7h^2/j = 2^{-7}5 \cdot 10^{12}u^2/j. \tag{11}$$

Since $u^2 \leq t$ except for $u = 3$, $t = 8$ we have $u^2/t \leq 9/8$ and this gives

$$L_3/L \leq 2^{-10} \cdot 45 \cdot 10^{12}(t/j) \leq 45 \cdot 10^9(t/j). \tag{12}$$

Further, from (7) and (11), we obtain

$$L_3/L \leq u^2/(50 \log n) \leq 9t/(400 \log n). \tag{13}$$

We can now estimate γ_1, γ_2. We have

$$|\gamma_1| \leq L_1 + (r/t)L_3 \leq L_1 + (j/t)L_3$$

and so from (12) we see that

$$|\gamma_1| \leq L_1 + 45 \cdot 10^9 L \leq 5 \cdot 10^{10}L.$$

Similarly we have

$$|\gamma_2| \le L_2 + \big(|s|/t\big)L_3 \le L_2 + \big((3j + 10\log n)/t\big)L_3$$

and so from (12) and (13) we see that $|\gamma_2| \le 15 \cdot 10^{10} L$. Thus we obtain

$$\big|\Delta(t\gamma_1; m_1)\big| \le t^{m_1} 10^{11m_1} \Delta(L/2; m_1) = t^{m_1} 10^{11m_1} 2^{L/2+m_1}.$$

Similarly we obtain

$$\big|\Delta(t\gamma_2; m_2)\big| \le t^{m_2} 10^{11m_2} 2^{3L/2+m_2},$$

and the lemma follows.

As a corollary we see that if $m_1 + m_2 \le L/2$ then $U(m_1, m_2) \le \Delta$, where

$$\Delta = (2^5 \cdot 10^{11} t)^{L/2}.$$

Now we have $t = 2^v \le 2^u \le e^{(0.7)u}$ and $(2^5 \cdot 10^{11})^{1/2} < e^{14.4}$. Hence we obtain $\Delta \le e^{14.75Lu}$ and since $h = 500u$, this gives $\Delta \le e^{(0.03)Lh}$.

We also wish to estimate

$$U = \prod_{m_1, m_2} U(m_1, m_2),$$

where the product is taken over all non-negative integers m_1, m_2 with $m_1 + m_2 \le L$. For this purpose we observe that

$$\sum_{m_1=0}^{L} \sum_{m_2=0}^{L-m_1} (m_1 + m_2) = \tfrac{2}{3} LH$$

where $H = \frac{1}{2}(L+1)(L+2)$ as above; indeed the left-hand side is

$$\tfrac{1}{2} \sum_{m_1=0}^{L} (L+m_1)(L-m_1+1) = (1/2)L(L+1)\big\{(L+1) + 1/2 - (1/6)(2L+1)\big\}.$$

Thus from Lemma 8 we obtain

$$U \le (2^4 \cdot 10^{11} t)^{(2/3)LH}.$$

Now $t \le e^{(0.7)u}$ and $(2^4 \cdot 10^{11})^{2/3} < e^{18.75}$. Hence we have

$$U \le e^{19.22LHu} \le e^{(0.0385)LHh}. \qquad (14)$$

Lemma 9. *For all λ_1, λ_2, λ_3, we have*

$$|p(\lambda)| \leq N^{-1} e^{(0.052)Lh}.$$

Proof. We apply Lemma 2 with

$$Z = \prod_{\ell, m_1, m_2} \{q^{L_3\ell}(U(m_1, m_2))^6 P\},$$

where

$$P = \prod_{k=1}^{6} \max_{\lambda_1,\lambda_2,\lambda_3} |\sigma_k(\rho^{\lambda_1\ell}\sigma^{\lambda_2\ell}\tau^{\lambda_3\ell})|.$$

Here we recall that q is the leading coefficient in the field polynomial for τ. Hence

$$q^{L_3\ell}\sigma_1(\tau^{\lambda_{3,1}\ell})\ldots\sigma_6(\tau^{\lambda_{3,6}\ell})$$

is an algebraic integer for all integer choices of $\lambda_{3,k}$ $(1 \leq k \leq 6)$ with $0 \leq \lambda_{3,k} \leq L_3$. Since clearly $U(m_1, m_2)$ is a rational integer and ρ and σ are units we see that the numbers $q^{L_3\ell}$ have the property required of the c_j in Lemma 2.

In the expression for Z above, the product is over all odd integers ℓ with $1 \leq \ell < 2h$ and all non-negative integers m_1, m_2 with $m_1 + m_2 \leq L$. Note that the sum of the integers ℓ is

$$\sum_{j=0}^{h-1}(2j+1) = 2\big((1/2)h(h-1)\big) + h = h^2.$$

To estimate P we recall that two of the conjugates of τ have absolute values at most $\epsilon^{3/2}$ and that the remainder have absolute values at most 1; moreover the same holds for the conjugates of ρ. Since also σ is a root of unity it follows that

$$P \leq \epsilon^{3(L_1+L_3)\ell}.$$

Now by the definition of U we obtain

$$Z \leq q^{L_3Hh^2} U^{6h} \epsilon^{3(L_1+L_3)Hh^2}.$$

Hence, since $M = Hh$, we deduce from (10) that

$$|\rho(\lambda)| \leq 2\sqrt{2}(N+1)q^{L_3h/6}U^{1/H}\epsilon^{(1/2)(L_1+L_3)h}.$$

We have $q \le n^{2/t}$ and thus, by (13), $q^{L_3 h/6} \le e^{(3/400)Lh}$. Further, by (14), $U^{1/H} \le e^{(0.0385)Lh}$. Furthermore, we have $\epsilon^{(1/2)L_1 h} \le e^{(1/200)Lh}$. We shall verify in a moment that, since $n > c_1$,

$$u^2/\log n < 1/(10.4\log\epsilon). \tag{15}$$

This together with (13) gives $\epsilon^{(1/2)L_3 h} \le e^{(1/1040)Lh}$. Hence, on combining our estimates, we get

$$|p(\lambda)| \le 2\sqrt{2}(N+1)e^{(0.05197)Lh}.$$

Then Lemma 9 follows since clearly $2\sqrt{2}(N+1)N < e^{(0.00001)Lh}$.

It remains to verify (15). Since $2^u < 3\log n$ we have $u < \psi(n)$, where

$$\psi(n) = (1/\log 2)(\log 3 + \log\log n).$$

Now $(\psi(n))^2/\log n$ is a decreasing function of n for $n > c_1$, and thus it suffices to prove that

$$(\psi(c_1))^2/\log c_1 < 1/(10.4\log\epsilon).$$

We have

$$\log c_1 = (50\log\log\epsilon)^2\log\epsilon$$

and thus we require that

$$50\log\log\epsilon > (\sqrt{10.4}/\log 2)(\log 3 + \log\log c_1).$$

The expression on the right is

$$42 + 5\log\log\epsilon + 10\log\log\log\epsilon,$$

with constants rounded up slightly, and if $\log\epsilon \ge 3$ then the desired inequality is obvious. If $\log\epsilon < 3$ we have the five possibilities for ϵ listed in the proof of Lemma 6. We have already remarked that we can exclude the fields $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{28})$; and the desired inequality is readily checked for the three remaining values of ϵ.

6. Basic estimates

Our purpose here is to establish the main estimates needed for the extrapolation algorithm described in the next section. The object is to prove that $g(\ell/2; m_1, m_2) = 0$ for all odd integers ℓ with $1 \le \ell < 4h$ and all non-negative integers m_1, m_2 with $m_1 + m_2 \le L/2$. Accordingly we shall suppose that

$$g = g(\ell/2; m_1, m_2) \neq 0$$

for some such ℓ, m_1, m_2 and we shall ultimately obtain a contradiction.

First we note that g is an algebraic number in the field $K(\rho^{1/2}, \sigma^{1/2}, \tau^{1/2})$, and consequently g has degree at most 48. We proceed to estimate the field norm $N(g)$ of g. By Lemma 9 we have $|p(\lambda)| \le N^{-1}X$, where $X = e^{(0.052)Lh}$. Further, as in the proof of the lemma, we see that

$$\prod_{k=1}^{6} \max_{\lambda_1,\lambda_2,\lambda_3} \left|\sigma_k(\rho^{\lambda_1\ell/2}\sigma^{\lambda_2\ell/2}\tau^{\lambda_3\ell/2})\right| \le \epsilon^{(3/2)\ell(L_1+L_3)}.$$

Furthermore it is clear that one of the conjugates of g is in fact the complex conjugate $g(-\ell/2; m_1, m_2)$. Hence we obtain

$$|N(g)| \le |g|^2 (X\Delta)^{46} \epsilon^{12\ell(L_1+L_3)}.$$

Now we have $X\Delta \le e^{(0.082)Lh}$ and so $(X\Delta)^{46} \le e^{(3.772)Lh}$. Also, as in Lemma 9, we see that if $\ell < 4h$, then $\epsilon^{12\ell L_1} \le e^{(0.48)Lh}$ and $\epsilon^{12\ell L_3} \le e^{(0.093)Lh}$. This gives

$$|N(g)| \le |g|^2 e^{(4.345)Lh}$$

To obtain a lower bound for $|N(g)|$, we observe that $\tau^{\lambda_3\ell/2}$ can be expressed as τ^{λ} or $\tau^{\lambda+1/2}$, where λ is an integer with $0 \le \lambda \le L_3\ell/2$. Now, since $\ell < 4h$, it follows that $q^{16L_3h}N(g)$ is an algebraic integer. By supposition $g \neq 0$, and hence

$$|N(g)| \ge q^{-16L_3h} \ge e^{-(0.72)Lh}.$$

On comparing estimates we obtain $|g|^2 \ge e^{-(5.065)Lh}$ and so $|g| \ge e^{-(2.533)Lh}$.

This gives a similar estimate for

$$f = f(\ell/2; m_1, m_2).$$

Indeed, for any complex number z we have $|e^z - 1| \le |z|e^{|z|}$ and thus, by (9), we obtain

$$\left|(\rho^{r/t}\sigma^{s/t})^{\lambda_3\ell/2} - \tau^{\lambda_3\ell/2}\right| \le (9L_3h)\epsilon^{-(3/2)(j-1)}.$$

Now $9L_3h \leq e^{(0.001)Lh}$ and, by the definition of L, we have $\epsilon^{(3/2)j} = e^{(15/4)Lh}$. Hence the number on the right is at most $e^{-(3.7)Lh}$. This gives

$$|f-g| \leq X\Delta e^{-(3.7)Lh} \leq e^{-(3.6)Lh} \tag{16}$$

and so certainly $|f-g| \leq |g|/2$. It follows that $|f| \geq |g|/2$, whence

$$|f| > e^{-(2.54)Lh}. \tag{17}$$

We shall also require an upper bound for $|f(z; m_1, m_2)|$ with $m_1 + m_2 \leq L/2$. By the definition of σ, the numbers $i\log\rho$ and $i\log\sigma$ take opposite signs. Hence

$$\left|\rho^{\lambda_1 z}\sigma^{\lambda_2 z}\right| \leq \max\left(e^{L_1|z\log\rho|}, e^{L_2|z\log\sigma|}\right).$$

We have $|\log\sigma| = \pi/3$ and, by Lemma 6, if $\mathbf{Q}(\alpha)$ is not $\mathbf{Q}(\sqrt[3]{28})$, as we can assume, then $|\log\rho| < (\pi/3)\log\epsilon$. thus we obtain

$$\left|\rho^{\lambda_1 z}\sigma^{\lambda_2 z}\right| \leq e^{(\pi/3)L_2|z|}.$$

Further we have, by (9),

$$\left|\log(\rho^{r/t}\sigma^{s/t}) - \log\tau\right| < 4\epsilon^{-(3/2)(j-1)}$$

for some value of the first logarithm. This gives

$$\left|(\rho^{r/t}\sigma^{s/t})^{\lambda_3 z}\right| \leq e^{(|\log\tau|+0.001)L_3|z|}$$

and since $|\log\tau| \leq \pi$, the number on the right is at most $e^{(3.15)L_3|z|}$. It follows that

$$\left|f(z; m_1, m_2)\right| \leq X\Delta e^{((\pi/3)L_2+(3.15)L_3)|z|}.$$

Now $X\Delta \leq e^{(0.082)Lh}$ and $L_2 \leq 10^{-2}L$, whence $e^{(\pi/3)L_2} \leq e^{(0.0105)L}$. Further, by (13) and (15), we have $L_3/L \leq 1/(520\log\epsilon)$. If we exclude the fields $\mathbf{Q}(\sqrt[3]{2})$ and $\mathbf{Q}(\sqrt[3]{28})$ which, as we noted in §5, we may, then $\log\epsilon \geq \log(11.48) > 2.44$. Hence $L_3/L \leq 1/(1268)$ and so $e^{(3.15)L_3} \leq e^{(0.0025)L}$. We conclude that

$$\left|f(z; m_1, m_2)\right| \leq e^{(0.082)Lh+(0.013)L|z|}. \tag{18}$$

7. Extrapolation

Let ℓ be any odd integer with $1 \leq \ell \leq 4h$. Suppose that m_1, m_2 are non-negative integers with $m_1 + m_2 \leq L/2$ and let $f(z) = f(z; m_1, m_2)$. Our purpose here is to obtain an upper bound for $f = f(\ell/2)$ which is stronger than the lower bound given by (17). Thus we shall conclude that $g = 0$ as required.

We shall denote the mth derivative of $f(z)$ by $f_m(z)$. Our first objective is to estimate $f_m(\ell')/m!$, where ℓ' is any odd integer with $1 \leq |\ell'| < 2h$ and m is any integer with $0 \leq m \leq L/2$. We have

$$f_m(\ell')/m! = \sum (\mu_1!\mu_2!)^{-1}(\log\rho)^{\mu_1}(\log\sigma)^{\mu_2} f'(\ell'; m_1', m_2'),$$

where the sum is over all non-negative integers μ_1, μ_2 with $\mu_1 + \mu_2 = m$ and $m_1' = m_1 + \mu_1$, $m_2' = m_2 + \mu_2$. Here $f'(\ell'; m_1', m_2')$ is defined like $f(\ell'; m_1', m_2')$ but with $\Delta(t\gamma_j; m_j + \mu_j)$ replaced by $\gamma_j^{\mu_j}\Delta(t\gamma_j; m_j)$. Now the auxiliary function was constructed so that $g(\ell'; m_1', m_2') = 0$ for positive ℓ', and in fact this holds also for negative ℓ', since $g(-\ell'; m_1', m_2')$ is a conjugate of $g(\ell'; m_1', m_2')$. Further arguing inductively with respect to $\mu_1 + \mu_2$ and observing that $\Delta(t\gamma_j; m_j)$ is a polynomial in γ_j with coefficients independent of the λ's we deduce that $g'(\ell'; m_1', m_2') = 0$, where g' is the analogue of f'. Hence we obtain

$$\left|f_m(\ell')/m!\right| \leq A\left|f(\ell'; m_1, m_2) - g(\ell'; m_1, m_2)\right|^*,$$

where

$$A = \max_{\lambda_1,\lambda_2,\lambda_3} \sum \left|(\mu_1!\mu_2!)^{-1}(\gamma_1 \log\rho)^{\mu_1}(\gamma_2 \log\sigma)^{\mu_2}\right|$$

and the $*$ signifies that each term in the sum over λ_1, λ_2, λ_3 representing $f - g$ is to be replaced by its absolute value. We have $|\gamma_1| \leq 5 \cdot 10^{10} L$ and $|\log\rho| \leq \pi$, and thus

$$\left|(\gamma_1 \log\rho)^{\mu_1}/\mu_1!\right| \leq (5 \cdot 10^{10}\pi L)^{\mu_1}/\mu_1! \leq 10^{10\mu_1} e^{5\pi L}.$$

Similarly since $|\log\sigma| \leq \pi/3$ we have

$$\left|(\gamma_2 \log\sigma)^{\mu_2}/\mu_2!\right| \leq 10^{10\mu_2} e^{5\pi L}.$$

Hence, since $m \leq L/2$ and $h \geq 500$, we obtain

$$A \leq L\, 10^{10m} e^{10\pi L} < e^{(0.1)Lh},$$

and it follows from the estimates of §6 (cf. (16)) that

$$\left|f_m(\ell')/m!\right| \leq e^{-(3.5)Lh}. \tag{19}$$

Now let $S = [L/2]$ and let

$$F(z) = \left((z^2 - 1^2)(z^2 - 3^2)\dots(z^2 - (2h-1)^2)\right)^{S+1}.$$

Further let Γ and $\Gamma_{\ell'}$ be the circles $|z| = 76h$ and $|z - \ell'| = 1/4$, described in the positive sense. By Cauchy's theorem we have

$$\frac{1}{2\pi i}\int_\Gamma \frac{f(z)dz}{(z-\ell/2)F(z)} = \frac{f(\ell/2)}{F(\ell/2)} + \frac{1}{2\pi i}\sum{}' \sum_{m=0}^{S} \frac{f_m(\ell')}{m!}\int_{\Gamma_{\ell'}} \frac{(z-\ell')^m dz}{(z-\ell/2)F(z)},$$

where $\sum'$ signifies summation over all odd integers ℓ' with $1 \le |\ell'| < 2h$. We require an estimate for the last integral, and for this purpose we note that

$$\left(F(z)\right)^{1/(S+1)} = 2^{2h}\prod_{k=-h}^{h-1}(z' + k)$$

where $z' = \frac{1}{2}(z+1)$. Further, for z on $\Gamma_{\ell'}$, we have $|z - \ell'| = 1/4$ and hence $|z' - \ell''| = 1/8$, where $\ell'' = \frac{1}{2}(l' + 1)$. Thus we obtain

$$|z' + k| = \left|(z' - \ell'') + (k + \ell'')\right| \ge |k + \ell''| - 1/8.$$

It follows that if $k > -\ell'' + 1$ then we have $|z' + k| > k + \ell'' - 1$, and if $k < -\ell'' - 1$, then $|z' + k| > -k - \ell'' - 1$. Since also $|z' + k| \ge 7/8$ for $k = -\ell'' \pm 1$ and $|z' + k| = 1/8$ for $k = -\ell''$, we obtain

$$\left|F(z)\right|^{1/(S+1)} \ge 2^{2h}(1/8)(7/8)^2(h + \ell'' - 2)!\,(h - \ell'' - 1)!,$$

where, for brevity, we have adopted the convention that $(-1)! = 1$. The number on the right is at least $(2h-3)!\,(7/8)^2$ and since $(2h)^3(7/8)^{-2} < e^{(0.05)h}$ this gives

$$\left|F(z)\right|^{1/(S+1)} \ge (2h)!e^{-(0.05)h}.$$

Now clearly, for z on $\Gamma_{\ell'}$, we have

$$\left|(z-\ell')^m/(z-\ell/2)\right| \le 4.$$

Further, the number of terms in the double sum above is $2h(S+1) < e^{(0.02)Lh}$. Hence, from (19), the absolute value of the sum is at most

$$e^{-(3.4)Lh}\left((2h)!\right)^{-(S+1)}. \qquad (20)$$

It is readily verified that, for $z = \ell/2$, we have

$$|F(z)|^{1/(S+1)} \leq 2^{2h}(h+[z'])!\,(h-[z'])! \leq 2^{2h}(2h)!\,.$$

This gives

$$|F(\ell/2)| \leq 2^{Lh+2h}\big((2h)!\big)^{S+1},$$

and hence (20) is at most

$$e^{-(2.7)Lh}|F(\ell/2)|^{-1}.$$

Let now θ and Θ denote respectively the upper bound of $|f(z)|$ and the lower bound of $|F(z)|$ with z on Γ. Since $2|z-\ell/2|$ with z on Γ exceeds the radius of Γ, we obtain

$$|f(\ell/2)| \leq (2\theta/\Theta)|F(\ell/2)| + e^{-2.7Lh}.$$

On noting that

$$|z^2-k^2| \geq |z|^2(1-k/|z|)$$

for each odd integer k with $1 \leq k < 2h$, and recalling that Γ has radius $76h$, we deduce that

$$\Theta \geq \big((37/38)^{1/2}76h\big)^{2h(S+1)}.$$

Thus, from the trivial estimate

$$|F(\ell/2)| \leq (2h)^{2h(S+1)},$$

it follows that

$$\Theta/|F(\ell/2)| \geq \big((37/38)^{1/2}38\big)^{2h(S+1)} \geq e^{3.62Lh}.$$

But from (18) we have $\theta \leq e^{1.07Lh}$ and hence

$$|f(\ell/2)| \leq 2e^{-2.55Lh} + e^{-2.7Lh}.$$

This contradicts (17), and the contradiction implies that $g = 0$, as required.

8. Kummer theory

The equation $g(\ell/2; m_1, m_2) = 0$, where ℓ is any odd integer with $1 \le \ell < 4h$ and m_1, m_2 are non-negative integers with $m_1 + m_2 \le L/2$, can be replaced by eight equations formed by restricting λ_1, λ_2, λ_3 to run through residue classes (mod 2). This is a consequence of the fact, established in §4, that $K(\rho^{1/2}, \sigma^{1/2}, \tau^{1/2})$ is an extension of K with degree 8. Hence for any λ_1', λ_2', λ_3' given by 0 or 1 we have

$$\sum_{\mu_1=0}^{L_1} \sum_{\mu_2=0}^{L_2} \sum_{\mu_3=0}^{L_3} p(\mu)\Delta(\gamma_1'; m_1)\Delta(\gamma_2'; m_2)\rho^{\mu_1\ell/2}\sigma^{\mu_2\ell/2}\tau^{\mu_3\ell/2} = 0,$$

where $\mu_j = \lambda_j' + 2\lambda_j$, $1 \le j \le 3$, $p(\mu) = p(\mu_1, \mu_2, \mu_3)$ and

$$\gamma_1' = \mu_1 + (r/t)\mu_3, \qquad \gamma_2' = \mu_2 + (s/t)\mu_3;$$

it is understood that λ_1, λ_2, λ_3, are allowed to run through all integers compatible with the ranges of μ_1, μ_2, μ_3. The above equation gives

$$\sum_{\lambda_1=0}^{L_1'} \sum_{\lambda_2=0}^{L_2'} \sum_{\lambda_3=0}^{L_3'} p'(\lambda)\Delta(\gamma_1'; m_1)\Delta(\gamma_2'; m_2)\rho^{\lambda_1\ell}\sigma^{\lambda_2\ell}\tau^{\lambda_3\ell} = 0$$

where $L_j' = [(L_j - \lambda_j')/2]$, $1 \le j \le 3$. The coefficients $p'(\lambda) = p'(\lambda_1, \lambda_2, \lambda_3)$ are a subset of the original $p(\lambda)$ and we can suppose that λ_1', λ_2', λ_3' are chosen such that the $p'(\lambda)$ are not all 0. Furthermore it is clear that $\Delta(\gamma_1'; m_1)$ and $\Delta(\gamma_2'; m_2)$ are polynomials in γ_1 and γ_2 with degrees m_1 and m_2 and with coefficients independent of the λ's. Hence, arguing by induction with respect to $m_1 + m_2$, we see that they can be replaced by $\Delta(\gamma_1; m_1)$ and $\Delta(\gamma_2; m_2)$. Thus we have shown that there is a function

$$g^{(1)}(z) = \sum_{\lambda_1=0}^{L_1'} \sum_{\lambda_2=0}^{L_2'} \sum_{\lambda_3=0}^{L_3'} p'(\lambda)\Delta(\gamma_1; m_1)\Delta(\gamma_2; m_2)\rho^{\lambda_1 z}\sigma^{\lambda_2 z}\tau^{\lambda_3 z}$$

such that $g^{(1)}(\ell) = 0$ for all odd integers ℓ with $1 \le \ell < 4h$ and all non-negative integers m_1, m_2 with $m_1 + m_2 \le L/2$; and here we have $L_j' \le L_j/2$, $1 \le j \le 3$.

The argument can now be repeated by induction and we deduce that for each integer $J = 0, 1, \ldots$ there exist integers $p^{(J)}(\lambda)$, not all 0, given by a subset of the original $p(\lambda)$, such that the function

$$g^{(J)}(z) = \sum_{\lambda_1=0}^{L_1^{(J)}} \sum_{\lambda_2=0}^{L_2^{(J)}} \sum_{\lambda_3=0}^{L_3^{(J)}} p^{(J)}(\lambda)\Delta(\gamma_1; m_1)\Delta(\gamma_2; m_2)\rho^{\lambda_1 z}\sigma^{\lambda_2 z}\tau^{\lambda_3 z}$$

satisfies $g^{(J)}(\ell) = 0$ for all odd integers ℓ with $1 \le \ell < 2^{J+1}h$ and all non-negative integers m_1, m_2 with $m_1 + m_2 \le (1/2)^J L$; and we have

$$L_j^{(J)} \le (1/2)^J L_j, \qquad 1 \le j \le 3.$$

But when J is large enough it follows that $L_j = 0$, $1 \le j \le 3$, and since then $p^{(J)}(0) \ne 0$, we plainly have a contradiction. This proves the theorems.

References

[1] A. Baker, Rational approximations to certain algebraic numbers, *Proc. London Math. Soc.* 4 (1964), 385–398.

[2] A. Baker, Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers, *Quart J. Math. Oxford*, **15** (1964), 375–383.

[3] A. Baker, Contributions to the theory of Diophantine equations I: On the representation of integers by binary forms, *Phil. Trans. Royal Soc.* **A 263** (1968), 173–191.

[4] A. Baker, A sharpening of the bounds for linear forms in logarithms I, II, III *Acta. Arith.* **21** (1972), 117–129; **24** (1973), 33–36; **27** (1975), 247–252.

[5] A. Baker, The theory of linear forms in logarithms. *Transcendence theory: advances and applications*, edited by A. Baker and D. W. Masser, Academic Press, 1977, pp. 1–27.

[6] A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford* **90** (1969), 129–137.

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

[8] E. Bombieri, On the Thue-Siegel-Dyson theorem, *Acta. Math.* **148** (1982), 255–296.

[9] E. Bombieri and J. Mueller, On effective measures of irrationality for $\sqrt[r]{(a/b)}$ and related numbers, *J. reine angew. Math.* **342** (1983), 173–196.

[10] J. W. S. Cassels, The rational solutions of the Diophantine equation $Y^2 = X^3 - D$, *Acta Math.* **82** (1950), 243–273.

[11] G. V. Chudnovsky, On the method of Thue-Siegel, *Ann. Math.* **117** (1983), 325–382.

[12] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta. Arith.* **34** (1979), 391–401.

[13] D. Easton, Effective irrationality measures for certain algebraic numbers, *Math. Comp.*, **46** (1986), 613–622.

[14] N. I. Feldman, An effective refinement of the exponent in Liouville's theorem (in Russian), *Izv. Akad. Nauk. SSSR*, **35** (1971), 973–990.

[15] K. Győry and Z. Z. Papp, Norm form equations and explicit lower bounds for linear forms with algebraic coefficients, *Studies in Pure Mathematics* (to the memory of Paul Turán) (Budapest, 1983), pp. 245–257.

[16] W. Ljunggren, On an improvement of a theorem of T. Nagell concerning the Diophantine equation $Ax^3 + By^3 = C$, *Math. Scand.* 1 (1953), 297–309.

[17] T. Nagell, Solution complète de quelques équations cubiques à deux indéterminées, *J. de Math.*, **4** (1925), 209–270.

[18] C. L. Siegel, Abschätzung von Einheiten, *Nachrichten Akad. Wiss. Göttingen*, Math-phys. Klasse 1969, No. 9, 71–86.