

9-1992

Simultaneous Rational Approximations and Related Diophantine Equations

John Rickert
rickert@rose-hulman.edu

Follow this and additional works at: http://scholar.rose-hulman.edu/math_mstr

 Part of the [Number Theory Commons](#)

Recommended Citation

Rickert, John, "Simultaneous Rational Approximations and Related Diophantine Equations" (1992). *Mathematical Sciences Technical Reports (MSTR)*. 138.
http://scholar.rose-hulman.edu/math_mstr/138

This Article is brought to you for free and open access by the Mathematics at Rose-Hulman Scholar. It has been accepted for inclusion in Mathematical Sciences Technical Reports (MSTR) by an authorized administrator of Rose-Hulman Scholar. For more information, please contact weir1@rose-hulman.edu.

**SIMULTANEOUS RATIONAL APPROXIMATIONS
AND RELATED DIOPHANTINE EQUATIONS**

John Rickert

MS TR 92-11

September 1992

**Department of Mathematics
Rose-Hulman Institute of Technology
Terre Haute, IN 47803**

FAX(812) 877-3198

Phone: (812) 877-8391

1. Introduction

A famous theorem of Roth[8] states that if ϑ is an algebraic irrational number, and $\lambda > 1$, then there is a positive constant c , depending only on ϑ and λ , such that

$$|\vartheta - p/q| > c|q|^{-1-\lambda} \quad (1.1)$$

for all pairs of integers p, q , with $q > 0$.

This result is ineffective in the sense that no-one knows how to calculate the constant c explicitly in terms of ϑ and λ . If $\lambda + 1$ happens to be not less than the degree of ϑ then the classical theorem of Liouville does provide a simple explicit value for c . But the resulting inequality (1.1) has no interesting applications to the effective solution of diophantine equations.

The first effective versions of (1.1) with such applications were given by Baker [1], [2]. These involve numbers of the form $\vartheta = t^\nu$, where t, ν are rational and t is close to 1 with respect to its denominator. Taking $t = \frac{128}{125}$ and $\nu = \frac{1}{3}$ Baker deduces the particularly striking inequality

$$\left| \sqrt[3]{2} - p/q \right| > 10^{-6} q^{-2.955}. \quad (1.2)$$

This implies that all integer solutions x, y of the diophantine equation

$$x^3 - 2y^3 = u$$

satisfy

$$\max\{|x|, |y|\} \leq (3 \cdot 10^5 |u|)^{23}.$$

In this paper we shall consider analogous questions for simultaneous approximations to algebraic numbers $\vartheta_1, \dots, \vartheta_m$. Of course (1.1) trivially implies that if $\vartheta_1, \dots, \vartheta_m$ are not all rational and $\lambda > 1$, then there exists $c > 0$, depending only on $\vartheta_1, \dots, \vartheta_m$ and λ , such that

$$\max\{|\vartheta_1 - p_1/q|, \dots, |\vartheta_m - p_m/q|\} > cq^{-1-\lambda} \quad (1.3)$$

for all integers p_1, \dots, p_m, q with $q > 0$. But if $1, \vartheta_1, \dots, \vartheta_m$ are linearly independent over the rationals then (1.3) is known even for any $\lambda > 1/m$ by the celebrated theorem of Schmidt[9].

Again these results are ineffective, and several authors have found effective versions. Baker himself [3] gave inequalities for numbers of the form

$$(\vartheta_1, \dots, \vartheta_m) = (t^{\nu_1}, \dots, t^{\nu_m})$$

for rational t, ν_1, \dots, ν_m . Again if t is sufficiently close to 1 with respect to its denominator, he was able to give an effective version of (1.3) with λ arbitrarily close to the critical value $1/m$, and he also gave corresponding applications to diophantine equations involving norm forms.

At about the same time Osgood[7] found inequalities for numbers of the form

$$(\vartheta_1, \dots, \vartheta_m) = (t_1^{\nu}, \dots, t_m^{\nu}) \quad (1.4)$$

for rational t_1, \dots, t_m, ν . If now t_1, \dots, t_m are sufficiently close to 1 with respect to a common denominator, he was able again to prove an effective form of (1.3)

with λ arbitrarily close to $1/m$. He also gave applications to sets of simultaneous diophantine equations.

Numbers of the form (1.4) were also studied by Fel'dman [5],[6]. He was mainly interested in measures of linear independence between $1, \vartheta_1, \dots, \vartheta_m$ and the corresponding diophantine equations, but in [5] he was able to deduce a version of (1.3) using simple transference techniques.

In the present paper we continue the study of the numbers (1.4) initiated by Osgood and Fel'dman. By using a different technique and estimating more carefully we are able to prove results with the same appeal as (1.2). One example is the inequality

$$\max\{|\sqrt{2} - p_1/q|, |\sqrt{3} - p_2/q|\} > 10^{-7} q^{-1.913}. \quad (1.5)$$

This implies that all integer solutions x, y, z of the simultaneous Pell-type equations

$$\begin{aligned} x^2 - 2z^2 &= u \\ y^2 - 3z^2 &= v \end{aligned} \quad (1.6)$$

satisfy

$$\max\{|x|, |y|, |z|\} \leq (10^7 \max\{|u|, |v|\})^{12}. \quad (1.7)$$

The arrangement of our paper is as follows. In section 2 we prove a general result that enables us to deduce (1.3) for arbitrary real numbers $\vartheta_1, \dots, \vartheta_m$ provided we have a suitable sequence of independent approximating forms.

Then in section 3 we construct a sequence of identities that will supply the appropriate approximating forms for the special numbers (1.4). Such identities were constructed by Osgood using fractional differentiation and by Fel'dman using certain determinants. We return to a more classical method of contour integration, which is similar to but not the same as that used by Baker in [3].

In section 4 we carry out the analytic and arithmetic estimates needed to apply the general result of section 2. But for simplicity we restrict ourselves to the case $m = 2$ and the examples

$$\vartheta_1 = \sqrt{1 - 1/N}, \quad \vartheta_2 = \sqrt{1 + 1/N}$$

for an integer $N \geq 2$. Finally in section 5 we prove our main result on the simultaneous approximation of these numbers, and we deduce (1.5) and (1.7) by choosing $N = 49$. We also add some comments about the linear independence of the numbers $1, \vartheta_1, \dots, \vartheta_m$.

This paper represents a development of part of my Ph.D. thesis at the University of Michigan (1990). I am grateful to my advisor David Masser for suggesting that the integrals (3.2) might have diophantine consequences, and also for discussions on the presentation of the paper.

2. Properties of approximating forms

In this section we consider arbitrary real numbers $\vartheta_1, \dots, \vartheta_m$, and we show how to prove results like (1.3) from the existence of a suitable family of independent

approximating forms. We put $\vartheta_0 = 1$.

Lemma 2.1 Suppose there are positive real numbers l, p, L, P, Q and positive integers d, D, f , with f dividing D , having the following property. For each positive integer k we can find rationals p_{ijk} ($0 \leq i, j \leq m$), with non-zero determinant, and positive integers $q_k \leq Q^k$, such that the $df^{-1}D^k q_k p_{ijk}$ ($0 \leq i, j \leq m$) are integers and

$$|p_{ijk}| \leq pP^k \quad (0 \leq i, j \leq m)$$

$$\left| \sum_{j=0}^m p_{ijk} \vartheta_j \right| \leq lL^{-k} \quad (0 \leq i \leq m).$$

Then if

$$U = \frac{L}{DQ} > 1$$

the numbers $\vartheta_1, \dots, \vartheta_m$ are not all rational.

Further, (1.3) holds with

$$\lambda = \frac{\log V}{\log U}, \quad V = PDQ$$

and

$$c^{-1} = 2(m+1)pdVC^\lambda f^{-1}, \quad C = \max\{1, 2dlf^{-1}\}.$$

Proof Let δ be the left-hand side of (1.3). Put $p_0 = q$,

$$\eta_{ik} = \sum_{j=0}^m p_{ijk} p_j \quad (0 \leq i \leq m)$$

and note that

$$q \sum_{j=0}^m p_{ijk} \vartheta_j - \eta_{ik} = q \sum_{j=0}^m p_{ijk} (\vartheta_j - p_j/q)$$

has absolute value at most $(m+1)pqP^k\delta$. It follows that

$$|\eta_{ik}| \leq (m+1)pqP^k\delta + lqL^{-k} \quad (0 \leq i \leq m). \quad (2.1)$$

Now our assumption about non-zero determinant shows that for each k the numbers η_{ik} ($0 \leq i \leq m$) are not all zero. Fix i with $0 \leq i \leq m$ and $\eta_{ik} \neq 0$. Since this is a rational number with denominator dividing $df^{-1}D^kq_k$, we have

$$|\eta_{ik}| \geq (df^{-1}D^kq_k)^{-1} \geq d^{-1}f(DQ)^{-k}. \quad (2.2)$$

Suppose $U > 1$ as in the hypothesis of the lemma. Then there exists a positive integer k with

$$U^k \geq Cq. \quad (2.3)$$

This implies

$$lqL^{-k} \leq \frac{1}{2}d^{-1}f(DQ)^{-k} \quad (2.4)$$

and so by comparing (2.1) and (2.2) we see that $\delta \neq 0$. This means that $\vartheta_1, \dots, \vartheta_m$ are not all rational as desired.

To find a lower bound for δ , we note that the positive integer

$$k = 1 + \left\lceil \frac{\log(Cq)}{\log U} \right\rceil$$

certainly satisfies (2.3). Now (2.1), (2.2) and (2.4) lead to

$$(m+1)pqP^k\delta \geq \frac{1}{2}d^{-1}f(DQ)^{-k}.$$

The definition of V gives

$$df^{-1}(m+1)pq\delta \geq \frac{1}{2}V^{-k}$$

and we also have

$$V^{-k} \geq V^{-1-\log(Cq)/\log U} = V^{-1}(Cq)^{-\lambda};$$

and now the desired inequality

$$\delta \geq \frac{1}{2}f((m+1)pqV)^{-1}C^{-\lambda}q^{-1-\lambda}$$

follows at once.

3. Contour Integrals

In this section we set up some contour integrals which will eventually yield the approximating forms for our numbers (1.4). For the moment we fix any complex number ν . Then for any complex number t with $|t| < 1$ we may define $f(t) = (1+t)^\nu$ by the binomial series

$$(1+t)^\nu = \sum_{h=0}^{\infty} \binom{\nu}{h} t^h. \quad (3.1)$$

Fix distinct non-zero complex numbers a_1, \dots, a_m ; then for sufficiently small x our numbers (1.4) will have the form

$$\vartheta_i = f(a_i x) \quad (1 \leq i \leq m).$$

Define also $a_0 = 0$ and

$$A(z) = (z - a_0) \cdots (z - a_m).$$

Then for any integer i with $0 \leq i \leq m$, any positive integer k , and any contour γ not passing through a_0, \dots, a_m the integral

$$I_i(x, k, \gamma) = \frac{1}{2\pi i} \oint_{\gamma} \frac{(1 + zx)^k f(zx)}{(z - a_i)(A(z))^k} dz \quad (3.2)$$

defines a function of x analytic near the origin. Suppose henceforth that γ is closed, counterclockwise and contains a_0, \dots, a_m . Then $I_i(x, k, \gamma)$ is independent of γ . We shall also suppress the dependence on k for the moment, so we write the integral as $I_i(x)$.

Lemma 3.1

For $0 \leq i \leq m$, the function $I_i(x)$ has a zero of order at least $(m + 1)k$ at $x = 0$.

Proof

We may expand

$$(1 + zx)^k f(zx) = (1 + zx)^{k+\nu}$$

as in (3.1) and deduce that

$$I_i(x) = \sum_{h=0}^{\infty} \binom{k+\nu}{h} x^h J_{ih} \quad (0 \leq i \leq m) \quad (3.3)$$

where

$$J_{ih} = \frac{1}{2\pi i} \oint_{\gamma} \frac{z^h}{(z - a_i)(A(z))^k} dz. \quad (3.4)$$

But the integrand is a rational function $P(z)/Q(z)$ and if $\deg Q > 1 + \deg P$ the integral over any closed contour containing all the zeroes of Q is well-known to be zero. It follows that $J_{ih} = 0$ whenever $h < (m+1)k$. This completes the proof of the lemma.

For sufficiently small complex x we define for later use the generating functions

$$J_i(x) = \sum_{h=0}^{\infty} x^h J_{ih} \quad (0 \leq i \leq m)$$

of the numbers J_{ih} in (3.4).

Lemma 3.2

Suppose $|x|^{-1} > \max\{|a_0|, |a_1|, \dots, |a_m|\}$. Then

$$J_i(x) = \frac{-1}{(1 - a_i x)(A(1/x))^k} \quad (0 \leq i \leq m).$$

Proof In the integrals (3.4) defining J_{ih} we can choose γ to be a circle centered at $z = 0$ with radius slightly larger than $\max\{|a_0|, \dots, |a_m|\}$. Then $\sum_{h=0}^{\infty} x^h z^h$

converges to $(1 - xz)^{-1}$ on γ and we see that

$$J_i(x) = \frac{1}{2\pi i} \oint_{\gamma} \frac{1}{(1 - xz)(z - a_i)(A(z))^k} dz.$$

Since $1/x$ is outside γ , this is the opposite of the residue of the integrand at $z = 1/x$ and the lemma follows.

Lemma 3.3

There are polynomials $p_{ij}(x)$ ($0 \leq i, j \leq m$) of degree at most k such that

$$I_i(x) = \sum_{j=0}^m p_{ij}(x)(1 + a_j x)^\nu \quad (0 \leq i \leq m).$$

Proof

It is clear that $I_i(x) = \sum_{j=0}^m R_{ij}(x)$, where $R_{ij}(x)$ is the residue of the integrand in (3.2) at $z = a_j$. To calculate this residue let δ_{il} be the Kronecker delta and write $k_{il} = k + \delta_{il}$. Thus the integrand is

$$(1 + zx)^{k+\nu} \prod_{l=0}^m (z - a_l)^{-k_{il}}.$$

So $R_{ij}(x)$ is the coefficient of $y^{k_{ij}-1}$ in the expansion of

$$(1 + zx)^{k+\nu} \prod_j^* (z - a_l)^{-k_{il}}$$

as a power series in $y = z - a_j$, where the \prod_j^* indicates the product from $l = 0$ to $l = m$ omitting $l = j$. We express

$$1 + zx = (1 + a_j x)(1 + Y_j y) \quad (3.5)$$

for

$$Y_j = x(1 + a_j x)^{-1}$$

and

$$z - a_l = (a_j - a_l)(1 + Y_l y) \quad (l \neq j) \quad (3.6)$$

for

$$Y_l = (a_j - a_l)^{-1}.$$

We raise (3.5) to the power $k + \nu$ and (3.6) to the power $-k_{il}$ using binomial expansions similar to (3.1) with summation indices $h = h_j$, $h = h_l$ ($l \neq j$) respectively.

We find that

$$R_{ij}(x) = (1 + a_j x)^{k+\nu} \sum_{ij} \binom{k+\nu}{h_j} Y_j^{h_j} \prod_j^* \binom{-k_{il}}{h_l} (a_j - a_l)^{-k_{il}} Y_l^{h_l}$$

where \sum_{ij} denotes the sum over all non-negative integers h_0, \dots, h_m with sum $k_{ij} - 1$. Thus

$$p_{ij}(x) = \sum_{ij} \binom{k+\nu}{h_j} (1 + a_j x)^{k-h_j} x^{h_j} \prod_j^* \binom{-k_{il}}{h_l} (a_j - a_l)^{-k_{il}-h_l} \quad (3.7)$$

is clearly a polynomial of degree at most k .

Lemma 3.4

We have

$$\det_{0 \leq i, j \leq m} (p_{ij}(x)) = \beta \alpha^{-1} x^{(m+1)k} \quad (3.8)$$

where

$$\beta = \prod_{j=-1}^{m-1} \binom{\nu - jk}{k} \quad (3.9)$$

and

$$\alpha = \prod_{l=0}^m \prod_{\substack{j=0 \\ j \neq l}}^m (a_j - a_l)^k. \quad (3.10)$$

Proof

Let $\Delta(x)$ be the determinant in question. Since $a_0 = 0$ we can replace the elements $p_{i0}(x)$ of the first column by

$$I_i(x) = p_{i0}(x) + \sum_{j=1}^m p_{ij}(x)(1 + a_j x)^\nu$$

without changing its value. It follows from Lemma 3.1 that $\Delta(x)$ has a zero of order at least $(m+1)k$ at $x = 0$. On the other hand, by Lemma 3.3 it is a polynomial of degree at most $(m+1)k$. Therefore $\Delta(x) = cx^{(m+1)k}$ for some c independent of x .

Furthermore c is the determinant whose entries are the coefficients c_{ij} of x^k in $p_{ij}(x)$. By (3.7) all these coefficients are polynomials in ν of degree at most $k_{ij} - 1 \leq k$. So $c = c(\nu)$ is a polynomial in ν of degree at most $(m+1)k$. On the

other hand, suppose ν is an integer satisfying

$$-k \leq \nu < mk. \quad (3.11)$$

Then the integrand in (3.2) is a rational function of z with no poles except possibly at a_0, \dots, a_m . Also by comparing degrees of numerator and denominator we see as in the proof of Lemma 3.1 that $I_i(x) = 0$ for $0 \leq i \leq m$. So $\Delta(x) = 0$, and it follows that $c(\nu) = 0$. Since this holds for the $(m+1)k$ values of ν satisfying (3.11), we conclude that $c(\nu)$ is divisible by any polynomial with these values as simple zeroes and no other zeroes. But β in (3.9) is such a polynomial, and we deduce (3.8) itself for some α independent of x and ν .

Finally, to verify the value (3.10) for α we note that the determinant $c^{(0)}$ whose entries are the coefficients $c_{ij}^{(0)}$ of ν^k in c_{ij} is $(k!)^{-(m+1)}\alpha^{-1}$. These coefficients can be read off from (3.7). Since

$$h_j \leq h_0 + \dots + h_m = k_{ij} - 1 = k + \delta_{ij} - 1$$

we get $c_{ij}^{(0)} = 0$ if $i \neq j$. So $c^{(0)}$ comes from a diagonal matrix. Also if $i = j$ then we get ν^k in $c_{ij}^{(0)}$ only by taking $h_j = k$. This forces $h_l = 0$ for $l \neq j$ and we end up with

$$c_{jj}^{(0)} = (k!)^{-1} \prod_j^* (a_j - a_l)^{-k}.$$

Because $c^{(0)} = \prod_{j=0}^m c_{jj}^{(0)}$, this verifies the value of α and therefore completes the proof of the lemma.

Suppose we now specialize ν and a_1, \dots, a_m to rational numbers, and we also fix some rational value of x . Then the $p_{ij}(x)$ are rational and as k varies they provide the numbers p_{ijk} in Lemma 2.1 for the numbers

$$\vartheta_j = (1 + a_j x)^\nu \quad (1 \leq j \leq m).$$

If further $x \neq 0$ and ν is not an integer, Lemma 3.4 shows that their determinant is non-zero for each fixed k . To conclude (1.3) we need suitable estimates for L, P, Q and D as well as l, p, d and f . These will satisfy the crucial inequality $L > DQ$ if x is sufficiently small with respect to its denominator. In this paper we content ourselves with taking $x = 1/N$ for a large positive integer N , although it is clear that other choices are available.

If we now take N sufficiently large, we will be able to establish (1.3) for values of λ that approach the critical value $1/m$ as N tends to infinity and ν, a_1, \dots, a_m stay fixed. This is essentially the conclusion of the papers of Osgood[7] and Fel'dman[5], and we see little point in reiterating such a general conclusion in the present paper. What we intend instead to do is restrict ourselves from now on to a very special case with the diophantine applications mentioned in the introduction, and to work out the estimates for this.

4. Two square roots

We therefore suppose from now on that

$$m = 2, \quad \nu = \frac{1}{2}, \quad a_1 = -1, \quad a_2 = 1 \quad (\text{and } a_0 = 0)$$

so that

$$\vartheta_1 = \sqrt{1 - 1/N}, \quad \vartheta_2 = \sqrt{1 + 1/N} \quad (\text{and } \vartheta_0 = 1)$$

and $A(z) = z^3 - z$. We proceed to find values for the quantities l, L, p, P, Q, d, D, f occurring in Lemma 2.1, where p_{ijk} are the values $p_{ij}(1/N)$ for varying values of k . We suppose only that $N \geq 2$ in this section.

Lemma 4.1

We may take $p = 11/4$ and

$$P = \frac{3\sqrt{3}}{2} \left(1 + \frac{2}{N\sqrt{3}} \right).$$

New Proof

We use the fact that each part $p_{ijk}\theta_j$ of I_i is given by the same integral (3.2) as I_i except that the contour γ is replaced by a contour γ_j containing only the zero $z = a_j$ of $A(z)$. Now the lemniscate defined by

$$|A(z)| = \frac{1}{3}\tau, \quad \tau = \frac{2}{\sqrt{3}}$$

is given in polar coordinates ($z = re^{i\theta}$) by

$$108r^4 \sin^2 \theta = (1 - 3r^2)^2(4 - 3r^2),$$

and it is easy to see that this splits into three such contours $\gamma_0, \gamma_1, \gamma_2$. Further, on γ_0 we have $\alpha \leq r \leq \sigma$, where

$$\alpha = \frac{(\sqrt{2} + 1)^{1/3} - (\sqrt{2} - 1)^{1/3}}{\sqrt{3}}, \quad \sigma = \frac{1}{\sqrt{3}},$$

and on γ_1, γ_2 we have $\sigma \leq r \leq \tau$. So on γ_0 we have also

$$|z \pm 1| = \frac{1}{3}\tau|z^2 \mp z|^{-1} \geq \frac{1}{3}\tau(r^2 + r)^{-1} \geq \frac{1}{3}\tau(\sigma^2 + \sigma)^{-1} = 1 - \sigma$$

and therefore

$$|z - a_i| \geq \min\{\alpha, 1 - \sigma\} = \alpha > .344 \quad (i = 0, 1, 2).$$

Also numerical integration shows that γ_0 has length $\ell_0 < 2.775$. Thus

$$|p_{i0k}\theta_k| \leq \frac{1}{2\pi} \frac{\ell_0}{\alpha} \left(1 + \frac{2}{N\sqrt{3}}\right)^{1/2} P^k < (1.613)P^k.$$

For $j = 1, 2$ we have similarly

$$|z \pm 1| \geq \frac{1}{3}\tau(\tau^2 + \tau)^{-1} = \tau - 1$$

so

$$|z - a_i| \geq \beta = \min\{\sigma, \tau - 1\} = \tau - 1 > .154 \quad (i = 0, 1, 2)$$

and γ_j has length $l_j < 1.496$. Thus

$$|p_{ijk}\vartheta_j| \leq \frac{1}{2\pi} \frac{l_j}{\beta} \left(1 + \frac{2}{N\sqrt{3}}\right)^{1/2} P^k < (1.942)P^k \quad (j = 1, 2).$$

Now Lemma 4.1 follows on noting that $\vartheta_1 \geq 1/\sqrt{2}$.

Lemma 4.2

We may take $l = 27/32$ and

$$L = \frac{27}{4}(N^3 - N).$$

Proof

The equations (3.3) give

$$|I_i(1/N)| \leq \sum_{h=0}^{\infty} b_h |J_{ih}| N^{-h}$$

for $b_h = \binom{k+1/2}{h}$. It is easily seen that the b_h decrease as $h \geq 3k$ increases, and since $J_{ih} = 0$ for $h < 3k$ we get

$$|I_i(1/N)| \leq b_{3k} \sum_{h=0}^{\infty} |J_{ih}| N^{-h}. \quad (4.1)$$

Now Lemma 3.2 gives for any x with $|x| < 1$ the generating series

$$J_0(x) = -(A(1/x))^{-k} = -x^{3k}(1-x^2)^{-k}$$

$$J_2(x) = -(1-x)^{-1}x^{3k}(1-x^2)^{-k}$$

and it follows easily that the J_{0h}, J_{2h} are all non-positive. Hence

$$\sum_{h=0}^{\infty} |J_{ih}| N^{-h} = -J_i(1/N) \leq 2(N^3 - N)^{-k} \quad (i = 0, 2).$$

The case $i = 1$ is slightly more delicate. We have

$$J_1(x) = -(1+x)^{-1}x^{3k}(1-x^2)^{-k} = -(1-x)x^{3k}(1-x^2)^{-k-1}$$

and this shows that the J_{1h} are alternating in sign. More precisely, the

$(-1)^{h+3k+1}J_{1h}$ are all non-negative. Hence in this case

$$\sum_{h=0}^{\infty} |J_{1h}|N^{-h} = (-1)^{3k+1}J_1(-1/N) \leq 2(N^3 - N)^{-k}.$$

So we find from (4.1) that

$$|I_i(1/N)| \leq 2b_{3k}(N^3 - N)^{-k} \quad (i = 0, 1, 2).$$

Finally the inequality

$$b_{3k} \leq \frac{27}{64} \left(\frac{4}{27} \right)^k \quad (k \geq 1)$$

is readily verified by induction on k , and now the lemma follows at once.

Lemma 4.3

We may take $Q = 1$, $d = 1$, $f = 2$ and $D = 8N$.

Proof

We put $x = 1/N$ in (3.7) to investigate the denominator of $p_{ij}(1/N)$. Now the coefficients $C = \binom{k+1/2}{h_j}$ are well known to have denominators composed only of

powers of 2. Also $|a_j - a_l| = 1$ or 2 , and it follows that $2^e N^k p_{ij}(1/N)$ is a rational integer for some non-negative integer e depending only on k .

To estimate e we note that the $h_j! 2^{h_j} C$ are integers. Further the power of 2 dividing $h_j!$ is well-known to be

$$\sum_{r=1}^{\infty} [h_j/2^r] = h'_j \leq \max\{0, h_j - 1\}.$$

Thus the $2^{h_j+h'_j} C$ are integers.

Finally for each j there is at most one l in the product \prod_j^* such that $|a_j - a_l| \neq 1$. The corresponding term in the sum \sum_{ij} therefore contributes at most $h_j + h'_j + k_{il} + h_l$ powers of 2. Now $l \neq j$ and if $h_j = 0$ this is at most

$$k_{il} + k_{ij} - 1 \leq 2k \leq 3k - 1,$$

while if $h_j \neq 0$ it is at most

$$2(h_0 + h_1 + h_2) - 1 + k_{il} = 2(k_{ij} - 1) - 1 + k_{il} \leq 3k - 1.$$

Therefore $e \leq 3k - 1$, and this completes the proof.

We also note that this is best possible, at least for $N = 1$, by considering $p_{11}(1)$ for $k = 2^K$. If $h_1 < k$ then the power of 2 in the denominator must be at most $h_1 + (k - K - 1) + (2k - h_1) = 3k - K - 1$. There is only one term with $h_1 = k$ and this has denominator exactly 2^{3k-1} .

5. Diophantine results

We can now prove our main result on simultaneous approximations.

Theorem

For an integer $N \geq 2$ the numbers

$$\vartheta_1 = \sqrt{1 - 1/N}, \quad \vartheta_2 = \sqrt{1 + 1/N}$$

satisfy

$$\max(|\vartheta_1 - p_1/q|, |\vartheta_2 - p_2/q|) > (271N)^{-1} q^{-1-\lambda}$$

for all integers p_1, p_2, q with $q > 0$, where

$$\lambda = \lambda(N) = \frac{\log(12N\sqrt{3} + 24)}{\log(27\{N^2 - 1\}/32)}.$$

Proof

We apply lemma 2.1 with the values of l, p, L, P, Q, d, D, f found in lemmas 4.1, 4.2 and 4.3. We find that $U = 27(N^2 - 1)/32 > 1$ as required and the constant c is estimated using $C = 1$ and

$$V = 12N\sqrt{3} + 24 \leq 12N(1 + \sqrt{3}).$$

This result has applications to diophantine equations as soon as $\lambda < 1$, which holds if $N \geq 26$. We deduce in particular the inequality (1.5) by choosing $N = 49$ in the Theorem and applying it with p_1, p_2, q replaced by $4p_2, 5p_1, 7q$ respectively. We find the lower bound

$$\frac{1}{2} \cdot \frac{7}{5} (271 \cdot 49)^{-1} (7q)^{-1-\lambda}$$

for the left-hand side of (1.5) and by a simple computation this exceeds the right-hand side.

We deduce the result (1.7) from (1.5) as follows. We may assume $x \geq 0, y \geq 0$ and $z \geq 0$, and we shall first establish that

$$z \leq (10^6 M / \sqrt{2})^{12} \tag{5.1}$$

where $M = \max\{|u|, |v|\}$. If $z = 0$ this is clear, so we assume $z \geq 1$. Now we have

$$|\sqrt{2} - x/z| = |2 - x^2/z^2| \cdot |\sqrt{2} + x/z|^{-1} \leq Mz^{-2}.$$

A similar argument with $\sqrt{3} - y/z$ shows that

$$\max\{|\sqrt{2} - x/z|, |\sqrt{3} - y/z|\} \leq Mz^{-2}.$$

Comparing this with the lower bound (1.5), we find (5.1) as required. Finally

$$y \leq (M + 3z^2)^{12} \leq (10^6 M)^{12}$$

and a similar argument for x yields (1.7). Of course the equations (1.6) can be solved effectively also by multiplying them together to give a hyperelliptic equation $Z^2 = f(z)$ for $Z = xy$, $f(z) = (2z^2 + u)(3z^2 + v)$, and then using the estimates of Baker [4]. But this does not lead to bounds depending polynomially on u and v .

Another approach is through linear forms in logarithms directly, as in the argument below. Using the latest estimates, this will provide polynomial bounds, but the exponent is likely to be very large. However, we may use this approach in conjunction with (1.7) to solve explicit equations rather quickly in practice. As an example, we shall prove that the only integers x, y, z satisfying

$$x^2 - 2z^2 = 1, \quad y^2 - 3z^2 = 1 \tag{5.2}$$

are $(x, y, z) = (\pm 1, \pm 1, 0)$. We may suppose $z \geq 0$. Then the only solutions to the first equation are given by

$$z = a_r = \frac{\alpha^r - \alpha^{-r}}{2\sqrt{2}}, \quad \alpha = 3 + 2\sqrt{2}$$

and the only solutions to the second equation are given by

$$z = b_s = \frac{\beta^s - \beta^{-s}}{2\sqrt{3}}, \quad \beta = 2 + \sqrt{3}$$

for non-negative integers r, s . Since

$$a_r = 6a_{r-1} - a_{r-2}, \quad b_s = 4b_{s-1} - b_{s-2}$$

we may quickly verify by hand that

$$a_r = b_s = z < 1000$$

has only the solution $r = s = 0$. But if

$$a_r = b_s = z \geq 1000$$

it is easy to establish that the quantity

$$\frac{s \log \beta - \log(\sqrt{3/2})}{\log \alpha} \tag{5.3}$$

is within 10^{-6} of an integer. For then

$$\alpha^{-r} < (2z\sqrt{2})^{-1}, \quad \beta^{-s} < (2z\sqrt{3})^{-1}$$

and so

$$\eta = \alpha^{-r} \beta^s \sqrt{2/3} = 1 + \alpha^{-r} \beta^s \sqrt{2/3} - \alpha^{-2r}$$

has the form $1 + \theta$ for

$$|\theta| < (12 \text{ or } 4z^2)^{-1} < \frac{1}{4} 10^{-6} = \epsilon.$$

Thus

$$|\log \eta| < -\log(1 - \epsilon) < \frac{1}{2} 10^{-6}$$

and it follows that (5.3) is within 10^{-6} of r as asserted. Finally we can assume $z = a_r \leq 10^{72}$ by (1.7), which implies $r \leq 94$, and it is then easy to check that

(5.3) is not within 10^{-6} of an integer. Hence indeed the only solutions of (5.2) are the obvious ones.

We may obtain similar results with even smaller exponents by working with larger values of N . Choosing $N = 9801$ we are able to obtain a result similar to (1.7) for the simultaneous equations

$$x^2 - 58z^2 = u, \quad y^2 - 2z^2 = v$$

showing that x, y, z satisfy

$$\max\{|x|, |y|, |z|\} \leq 10^{28} (\max\{|u|, |v|\})^{3.1}.$$

We conclude this paper with some remarks about the linear independence of $1, \vartheta_1, \dots, \vartheta_m$ over the rationals. It is well-known that (1.3) implies by transference techniques this linear independence as soon as $\lambda < 1/(m-1)$ and one even obtains a measure of the form

$$|x_0 + x_1\vartheta_1 + \dots + x_m\vartheta_m| \geq c'X^{-\lambda'} \tag{5.4}$$

where x_0, \dots, x_m are rational integers, not all zero, with absolute values at most X , and $c' > 0$ is independent of X . But also in the general situation of Lemma 2.1, it is easy to prove the linear independence provided

$$U' = L(P^{m-1}D^mQ^m)^{-1} > 1.$$

One then obtains (5.4) with the explicit exponent

$$\lambda' = \frac{\log V'}{\log U'}, \quad V' = (PDQ)^m.$$

In the special situation described at the end of section 3, this leads to values of λ' that approach the best possible value m as the parameter N gets large with respect to fixed a_0, \dots, a_m and ν . Such results were also obtained by Osgood[7] and Fel'dman[5], and they were applied to the solution of diophantine equations in norm form by Fel'dman[6]. However, even with the refined estimates of section 4 we do not seem to obtain very appealing examples. We would need $\lambda' < 3$ in the above, which does not happen until $N \geq 6,457,560$. In the event that this could be reduced to $N \geq 49$, we would be able to solve the norm equation

$$\text{Norm}(x + y\sqrt{2} + z\sqrt{3}) = u$$

effectively.

- [1] Baker A. "Rational approximations to certain algebraic numbers. *Proc. London Math. Soc.* **14** (1964), 385-398.
- [2] Baker A. "Rational Approximations to $\sqrt[3]{2}$ and other algebraic numbers. *Quart. J. Math. Oxford* **15** (1964), 375-383.
- [3] Baker, A. "Simultaneous Rational Approximations to Certain Algebraic Numbers" *Proc. Camb. Phil. Soc.* **63** (1967), 693-702.

- [4] Baker, A. *Transcendental Number Theory*, Cambridge University Press, 1975.
- [5] Fel'dman, N.I. "An estimate of an Incomplete Linear Form in Several Algebraic Variables" *Matem. Zametki*. **7** (1970), 565–580 (Russian); English transl., *Math Notes* **7** (1970), 343–349.
- [6] Fel'dman, N.I. "Effective Bounds for the Number of Solutions of certain Diophantine Equations" *Matem. Zametki*. **8** (1970), 361–371 (Russian); English transl., *Math Notes* **8** (1970), 674–679.
- [7] Osgood, C.F. "The Simultaneous Diophantine Approximation of Certain k th Roots" *Proc. Camb. Phil. Soc.* **67** (1970), 75–86.
- [8] Roth, K.F. "Rational approximations to algebraic numbers" *Mathematika* **2** (1955), 1–20; corrigendum, *ibid.* 168.
- [9] Schmidt, W.M. "Simultaneous Approximation to Algebraic Numbers by Rationals" *Acta Math.* **125** (1970), 189–201.