ON THE FOURTH-POWERFREE PART OF $x^2 + 2$

by BENJAMIN M. M. DE WEGER[†]

(Received 1 December, 1996)

Abstract. We show that $x = 59$ is the largest positive integer for which the fourth-powerfree part of $x^2 + 2$ is at most 100. This implies the solution of the problem, posed recently by J.H.E. Cohn, to prove that $(x, y) = (1, 1)$ is the only solution in nonnegative integers to the diophantine equation $x^2 - 3y^4 = -2$, as well as a new solution to the problem, posed a long time ago by the same J.H.E. Cohn and solved before by R. Bumby and N. Tzanakis, to prove that $(x, y) = (1, 1), (11, 3)$ are the only solutions in nonnegative integers to the diophantine equation $2x^2 - 3y^4 = -1$.

1. Introduction. Recently, J.H.E. Cohn [4] asked to prove that the only solution in nonnegative integers to the diophantine equation $x^2 - 3y^4 = -2$ is given by $(x, y) = (1, 1)$. As Cohn showed, this statement implies that the diophantine equation $x^2 - kxy^2 + y^4 = -2$ (equation 4 in [4]) has only two solutions in nonnegative integers, namely $(x, y, k) = (1, 1, 4), (3, 1, 4)$.

The present note was originally set up to provide the proof Cohn asked for, but evolved naturally into the proof of a more general result. This was also inspired by the remarkable fact that almost 30 years earlier, the same J.H.E. Cohn [3] asked to prove that the only solutions in nonnegative integers to the diophantine equation $2x^2 - 3y^4 = -1$ are $(x, y) = (1, 1), (11, 3)$. This was done already in 1967, by R. Bumby [2], and again in 1995 by N. Tzanakis [7]. On multiplying the equation $2x^2 - 3y^4 = -1$ by 2 and then replacing $2x$ by x we obtain the equation $x^2 - 6y^4 = -2$, which is remarkably similar to $x^2 - 3y^4 = -2$.

We decided to solve the equations

$$x^2 + 2 = Dy^4 \tag{1}$$

for a reasonable range for the parameter D, including $D = 3$ and $D = 6$ referred to above. Indeed, it turned out to be possible to solve (1) in a routine way for all $D \leq 100$. It is the purpose of this note to show that such an equation for a not too large value for D can be solved in practice with a little effort, and that the method is uniform to some extent, but not entirely.

Unfortunately our proof is far from elementary, as Cohn expected, since it is based on the theory of linear forms in logarithms of algebraic numbers, and computer calculations. We note that the methods of Tzanakis [7] and of Mignotte and Pethő [6] should also work routinely for solving equation (1) for any reasonable value of D, and it would not surprise us at all when Bumby's more elementary but rather complicated method [2] would also work for equation (1) for at least some more values of D.

[†] The author's research was supported by the Netherlands Mathematical Research Foundation SWON with financial aid from the Netherlands Organization for Scientific Research NWO.

Glasgow Math. J. **40** (1998) 299–310.

Here is our main result, giving the complete set of solutions to equation (1) for all $D \leq 100$. As noted above, for $D = 3$ this answers Cohn's question in [C2], and for $D = 6$ the result was already known, cf. Bumby [2] and Tzanakis [7].

THEOREM 1. *The only nonnegative integers x such that the fourth-powerfree part of $x^2 + 2$ is at most* 100, *are* $x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 22, 59$.

2. Thue equations. Modulo 5 the only squares are 0, 1 and 4, and the only fourth powers are 0 and 1. Modulo 8 the only squares are 0, 1 and 4, and the only fourth powers are 0 and 1. It follows that equation (1) is solvable only if $D \equiv 1, 2$ or $3 \pmod 5$, and $D \equiv 2, 3$ or $6 \pmod 8$. Further, if p is an odd prime divisor of D, then equation (1) having a solution implies that -2 is a quadratic residue modulo p, hence that $p \equiv 1$ or $3 \pmod 8$. These observations imply that for $D \leq 100$ we only have to consider $D \in \{2, 3, 6, 11, 18, 22, 27, 38, 43, 51, 66, 67, 82, 83, 86\}$.

The case of $D = 2$ is easy. It is clear that then x is even and y odd, hence $y^4 \equiv 1 \pmod 8$, and it follows that x is divisible by 4. Put $x = 4z$, then we find $z^2 = \frac{y^2-1}{4}\frac{y^2+1}{2}$, in which the two factors in the right hand side are coprime, hence squares themselves. Put $\frac{y^2-1}{4} = u^2$, then $y^2 - (2u)^2 = 1$, and this obviously is possible only for $y = \pm 1$ and $u = 0$, implying $x = 0$.

We consider equation (1) over the field $\mathbb{Q}(\sqrt{-2})$. We put

$$\begin{array}{lll} \pi_2 = \sqrt{-2}, & \pi_3 = 1 + \sqrt{-2}, & \pi_{11} = 3 + \sqrt{-2}, \\ \pi_{17} = 3 + 2\sqrt{-2}, & \pi_{19} = 1 + 3\sqrt{-2}, & \pi_{41} = 3 + 4\sqrt{-2}, \\ \pi_{43} = 5 + 3\sqrt{-2}, & \pi_{67} = 7 + 3\sqrt{-2}, & \pi_{83} = 9 + \sqrt{-2}. \end{array}$$

Thus for each prime dividing one of the remaining values for D we have a prime $\pi_p \in \mathbb{Z}[\sqrt{-2}]$ of norm p. We write

$$x + \sqrt{-2} = \alpha\beta^4 \tag{2}$$

for $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$, with α fourth-powerfree. Our first aim is to determine all possible values for α. Equations (1) and (2) imply $x^2 + 2 = N(x + \sqrt{-2}) = N(\alpha)N(\beta)^4 = Dy^4$, hence D is the fourth-powerfree part of N(α).

If x is even then $\mathrm{ord}_{\pi_2}(x + \sqrt{-2}) = 1$, hence $\mathrm{ord}_{\pi_2}(\alpha) = 1$, hence $\mathrm{ord}_2(N(\alpha)) = 1$, hence D is even. If x is odd then $\mathrm{ord}_{\pi_2}(x + \sqrt{-2}) = 0$, hence $\mathrm{ord}_{\pi_2}(\alpha) = 0$, hence $\mathrm{ord}_2(N(\alpha)) = 0$, hence D is odd. So π_2 divides α (and exactly once) if and only if D is even.

If p is an odd prime that splits in $\mathbb{Z}[\sqrt{-2}]$ say $p = \pi\bar{\pi}$, then we put $k = \mathrm{ord}_\pi(\alpha)$ and $\ell = \mathrm{ord}_{\bar{\pi}}(\alpha) = \mathrm{ord}_\pi(\bar{\alpha})$. Then $k, \ell \in \{0, 1, 2, 3\}$. If $\min\{k, \ell\} \geq 1$ then $p|\alpha$ and $p|\bar{\alpha}$, hence $p|x + \sqrt{-2}$ and $p|x - \sqrt{-2}$, hence $p|(x + \sqrt{-2}) - (x\sqrt{-2}) = 2\sqrt{-2}$, which is impossible for an odd prime p. Hence $\min\{k, \ell\} = 0$. By switching to the complex conjugate and noting that the sign of x is irrelevant, we may assume without loss of generality that $\ell = 0$. Hence $k = \mathrm{ord}_p(N(\alpha))$, so by $k \leq 3$ also $k = \mathrm{ord}_p(D)$, and we find $\mathrm{ord}_\pi(\alpha) = \mathrm{ord}_p(D)$.

If p is an odd prime that does not split in $\mathbb{Z}[\sqrt{-2}]$ then it is inert. Hence $p|\alpha$ implies $p|\bar{\alpha}$, and as above this implies $p|2\sqrt{-2}$, which is impossible.

From the above considerations it follows that α is a product of π_p's and $\bar{\pi}_p$'s for the primes p dividing D. Of each pair of complex conjugate values for α we have to consider only one. We thus have the following possibilities, where we put $\pm\alpha = a + b\sqrt{2}$ and we can take both a and b positive. Note that always $D = a^2 + 2b^2$.

D	$\pm\alpha$			a	b
3	π_3	$=$	$1+\sqrt{-2}$	1	1
6	$\pi_2\bar{\pi}_3$	$=$	$2+\sqrt{-2}$	2	1
11	π_{11}	$=$	$3+\sqrt{-2}$	3	1
18	$-\pi_2\pi_3^2$	$=$	$4+\sqrt{-2}$	4	1
22	$\pi_2\bar{\pi}_{11}$	$=$	$2+3\sqrt{-2}$	2	3
27	$-\bar{\pi}_3^3$	$=$	$5+\sqrt{-2}$	5	1
38	$\pi_2\pi_{19}$	$=$	$6+\sqrt{-2}$	6	1
43	π_{43}	$=$	$5+3\sqrt{-2}$	5	3

D	$\pm\alpha$			a	b
51	$-\bar{\pi}_3\bar{\pi}_{17}$	$=$	$1+5\sqrt{-2}$	1	5
	$\pi_3\bar{\pi}_{17}$	$=$	$7+\sqrt{-2}$	7	1
66	$\pi_2\bar{\pi}_3\bar{\pi}_{11}$	$=$	$8+\sqrt{-2}$	8	1
	$\pi_2\bar{\pi}_3\pi_{11}$	$=$	$4+5\sqrt{-2}$	4	5
67	π_{67}	$=$	$7+3\sqrt{-2}$	7	3
82	$\pi_2\bar{\pi}_{41}$	$=$	$8+3\sqrt{-2}$	8	3
83	π_{83}	$=$	$9+\sqrt{-2}$	9	1
86	$\pi_2\bar{\pi}_{43}$	$=$	$6+5\sqrt{-2}$	6	5

In equation (2) we put $\beta = E + F\sqrt{-2}$ with $E, F \in \mathbb{Z}$. Then comparing imaginary parts we find the Thue equation

$$bE^4 + 4aE^3F - 12bE^2F^2 - 8aEF^3 + 4bF^4 = \pm 1. \tag{3}$$

Looking at this equation modulo 4 we find that the right hand side is 1 if $b \equiv 1 \pmod 4$, and -1 if $b \equiv -1 \pmod 4$. Looking modulo 8 we see that there are no solutions when a is even and $b \equiv 3, 5 \pmod 8$. Looking modulo 3 we see that there are no solutions when $a \equiv 1 \pmod 3$ and $b \equiv 5 \pmod{12}$. Thus only eleven cases remain: $b = 1$ with $a \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and $b = 3$ with $a \in \{5, 7\}$, corresponding to $D \in \{3, 6, 11, 18, 27, 38, 51, 66, 83\}$ and $D \in \{43, 67\}$. It will now be clear that Theorem 1 follows from the following result.

THEOREM 2. *Equation* (3) *with* $b = 1$ *and* $a \in \{1, 3, 4, 5, 6, 7, 8, 9\}$ *has only the solutions* $(E, F) = \pm(1, 0)$.

Equation (3) *with* $b = 1$ *and* $a = 2$ *has only the solutions* $(E, F) = \pm(1, 0), \pm(1, -1)$.

Equation (3) *with* $b = 3$ *and* $a = 5$ *has only the solutions* $(E, F) = \pm(1, -1)$.

Equation (3) *with* $b = 3$ *and* $a = 7$ *has no solutions.*

Notice that with $b = 1$ the solutions $(E, F) = \pm(1, 0)$ lead to $(x, y) = (\pm a, \pm 1)$ for equation (1), that with $b = 1$, $a = 2$ the solutions $(E, F) = \pm(1, -1)$ lead to $(x, y) = (\pm 22, \pm 3)$ for equation (1), and that with $b = 3$, $a = 5$ the solutions $(E, F) = \pm(1, -1)$ lead to $(x, y) = (\pm 59, \pm 3)$ for equation (1).

At this point we note that for each D equation (1) defines an elliptic curve. The rank of this curve is 1 if $D \in \{3, 6, 11, 18, 27, 38, 43, 51, 67, 83\}$, and the rank is 2 if $D = 66$. We checked this because by the theory of elliptic curves equation (1) is trivial if the rank is 0.

In solving the equations (3) we could make it easy for ourselves, and use the software package KANT, which contains a program that solves Thue equations in an automated way. This program works essentially in the same way as our arguments below, and on referring to the program we could at this point end the paper in a few lines. We chose not to do so for two reasons. The first reason is didactical: we want to give the reader insight in what is going on in our proof, and hence what goes on inside a program like KANT. The second reason is more mathematical: we will see below that in our specific situation we can make improvements on the general method, so that we obtain smaller upper bounds and a faster reduction procedure. However, we encourage those readers who are only interested in the truth of results and not in their proofs to stop reading here and invoke the KANT program to prove our Theorem 2. Note that KANT is available by anonymous ftp from **ftp.math.tu-berlin.de.**

3. Quartic fields. We need some information on the quartic fields associated to the binary forms in equation (3). We computed the data below by Pari-1.39.03 on a personal computer. We let (a,b) be one of the pairs treated in Theorem 2, and let $D = a^2 + 2b^2$.

Let θ be a root of $t^4 - 2Dt^2 + 2b^2D$, and let $\mathbb{K} = \mathbb{Q}(\theta)$. Note that this field is totally real, and of degree 4. Put

$$\xi = \frac{1}{ab^2}(\theta + b)(\theta^2 - 2(a^2 + b^2)).$$

Then ξ is a root of $bx^4 + 4ax^3 - 12bx^2 - 8ax + 4b$, so that equation (3) can be written as $bN(E - F\xi) = \pm 1$, when N denotes the norm function of $\mathbb{K}$ over $\mathbb{Q}$. It will be clear why ξ is of interest to us. Pari helped us to find θ, defining the same field $\mathbb{K}$ over $\mathbb{Q}$ as ξ does, but more convenient to work with. We denote conjugates by lower indices, and number them as follows:

$$\theta_1 = \sqrt{D + a\sqrt{D}}, \qquad \theta_2 = \sqrt{D - a\sqrt{D}}, \qquad \theta_3 = -\theta_1, \qquad \theta_4 = -\theta_2.$$

We also write $\mathbb{K}_i = \mathbb{Q}(\theta_i)$. Let σ be the notrivial $\mathbb{Q}$-automorphism of $\mathbb{K}$ sending θ to $-\theta$, thus sending θ_i to θ_{i+2}, indices taken modulo 4. Thus note that $\mathbb{K}_i = \mathbb{K}_{i+2}$.

We have computed the discriminant Δ, a basis $\{1, \theta, \omega_1, \omega_2\}$ for the ring of integers of $\mathbb{K}$, a set of fundamental units $\epsilon_1, \epsilon_2, \epsilon_3$, the regulator R, the class number h, and the galois group of the field $\mathbb{K}$. In the cases where $b > 1$ we also need information on the prime ideals dividing b.

If $D \in \{3, 6, 11, 38, 51, 66, 83\}$ we have $\epsilon_1 = 1 + \theta$, $\epsilon_3 = \sigma(\epsilon_1) = 1 - \theta$, and the galois group is the dihedral group of order 8. Further we have data as given below.

D	Δ	ω_1	ω_2	ϵ_2	R	h
3	$2^9\ 3^3$	θ^2	θ^3	$5 + 2\theta - 2\theta^2$	10.1286...	1
6	$2^{10}\ 3^3$	$\frac{1}{2}\theta^2$	$\frac{1}{2}\theta + \frac{1}{4}\theta^3$	$2 - \theta - \frac{1}{2}\theta^2$	17.6308...	1
11	$2^9\ 11^3$	$\frac{1}{3} + \frac{1}{3}\theta^2$	$\frac{1}{3}\theta + \frac{1}{3}\theta^3$	$21 - 6\theta - 18\theta^2 + 4\theta^3$	84.7640...	1
38	$2^{10}\ 19^3$	$\frac{1}{3} - \frac{1}{6}\theta^2$	$\frac{1}{6}\theta - \frac{1}{12}\theta^3$	$818 - 93\theta - \frac{1611}{2}\theta^2 + 93\theta^3$	287.6381...	1
51	$2^9\ 3^3\ 17^3$	$\frac{2}{7} - \frac{1}{7}\theta^2$	$\frac{2}{7}\theta - \frac{1}{7}\theta^3$	$\frac{763055}{7} - \frac{75932}{7}\theta - \frac{755492}{7}\theta^2 + \frac{75178}{7}\theta^3$	466.0410...	4
66	$2^6\ 3^3\ 11^3$	$\frac{1}{8} - \frac{1}{2}\theta - \frac{1}{16}\theta^2$	$\frac{1}{2} - \frac{1}{16}\theta + \frac{1}{32}\theta^3$	$1 - \frac{3}{2}\theta - 3\theta^2 - \frac{1}{4}\theta^3$	201.8533...	2
83	$2^9\ 83^3$	$\frac{2}{9} - \frac{1}{9}\theta^2$	$\frac{2}{9}\theta - \frac{1}{9}\theta^3$	$577232987550887 - \frac{134815072558468}{3}\theta$	1318.1875...	1
				$-573734476516164\theta^2 - \frac{133997981316014}{3}\theta^3$		

If $D=18$ then we have $\Delta = 2^8\,3^2$, $\omega_1 = \frac{1}{4}+\frac{1}{2}\theta+\frac{1}{24}\theta^2$, $\omega_2 = \frac{1}{4}\theta+\frac{1}{24}\theta^3$, $\epsilon_1 = \frac{3}{4}-\frac{5}{4}\theta-\frac{1}{24}\theta^2+\frac{1}{24}\theta^3$, $\epsilon_2 = \frac{3}{2}-\frac{7}{4}\theta-\frac{1}{12}\theta^2+\frac{1}{24}\theta^3$, $\epsilon_3 = \frac{1}{2}-\frac{1}{12}\theta^2$, with $\sigma(\epsilon_3)=\epsilon_3$, $R=2.6608\ldots$, $h=1$, and the galois group is the Klein group of order 4, so the field is galois in this case. Further we note that $1+\theta = -\epsilon_1^{-2}\epsilon_2^{-1}\epsilon_3^2$ and $1-\theta = \epsilon_1^2\epsilon_2\epsilon_3^2$, and that $\epsilon_{1,1} = -\epsilon_{1,2} = -\epsilon_{1,3}^{-1} = \epsilon_{1,4}^{-1}$, and $\epsilon_{2,1} = \epsilon_{2,2}^{-1} = -\epsilon_{2,3}^{-1} = -\epsilon_{2,4}$.

If $D=27$ then $\mathbb{K}$ is the same field as the one for $D=3$. Note that $\theta_{D=27} = 9\theta_{D=3}-2\theta_{D=3}^3$.

If $D \in \{43, 67\}$ then we have $\Delta = 2^9 D^3$, $\epsilon_3 = \sigma(\epsilon_1)$, $h=1$, and the galois group is the dihedral group of order 8. We have $3 = \rho\sigma(\rho)\tau$ for primes ρ,τ of norm -3 and 9 respectively. Here ρ is the denominator of ξ. Further we have data as given below.

D	ω_1	ω_2	ϵ_1	ϵ_2	R	ρ
43	$\frac{2}{5}+\frac{1}{5}\theta^2$	$\frac{7}{15}\theta+\frac{1}{15}\theta^3$	$1-\frac{151}{5}\theta+\frac{2}{5}\theta^3$	$\frac{56669}{5}+\frac{17732}{5}\theta$ $-\frac{748}{5}\theta^2-\frac{234}{5}\theta^3$	$895.5544\ldots$	$\frac{29}{5}-\frac{8}{15}\theta$ $-\frac{3}{5}\theta^2+\frac{1}{15}\theta^3$
67	$\frac{3}{7}+\frac{1}{7}\theta^2$	$\frac{10}{21}\theta+\frac{1}{21}\theta^3$	$1+\frac{269}{7}\theta$ $-16\theta^2+\frac{8}{7}\theta^3$	$\frac{9655}{7}-\frac{3237}{7}\theta$ $-\frac{67}{7}\theta^2+\frac{27}{7}\theta^3$	$3205.2540\ldots$	$\frac{79}{7}-\frac{127}{21}\theta$ $+\frac{3}{7}\theta^2+\frac{2}{21}\theta^3$

4. Linear forms in logarithms. Equation (3) leads to

$$E - F\xi = \pm\mu\epsilon_1^{a_1}\epsilon_2^{a_2}\epsilon_3^{a_3} \tag{4}$$

for some $a_1, a_2, a_3 \in \mathbb{Z}$, with $\mu = 1$ if $b=1$, and $\mu = \rho^{-1}$ in the cases with $b=3$. As the sign of (E,F) is irrelevant, we may disregard the ± sign in front of the μ. Since the differences of the four numbers $E-F\xi_j$ are of the size of $|F|$, these four numbers are far apart when $|F|$ is large. But their product equals $N(E-F\xi) = \frac{1}{b}$, so it must be the case that three of them are also of the size of $|F|$, and one of them is extremely small, of the size of $|F|^{-3}$. Let $i \in \{1,2,3,4\}$, depending on E,F (thus not known in advance), be such that $|E-F\xi_i| = \min_{j=1,2,3,4} |E-F\xi_j|$. Then this is the extremely small one.

We consider three conjugates of equation (4), with indices i, j, k, where j, k are taken as follows:

$$\begin{array}{lll} j=2,\ k=4 & \text{if} & i=1 \text{ or } i=3. \\ j=1,\ k=3 & \text{if} & i=2 \text{ or } i=4. \end{array}$$

Although we could have made other choices, we will see below that this particular choice turns out to be convenient.

The following identity is sometimes called Siegel's identity, and follows by eliminating E,F from the three conjugates of $E-F\xi$. It reads.

$$(\xi_i-\xi_j)(E-F\xi_k)+(\xi_j-\xi_k)(E-F\xi_i)+(\xi_k-\xi_i)(E-F\xi_j) = 0, \tag{5}$$

and together with (4) this leads to

$$\frac{\xi_i-\xi_j}{\xi_i-\xi_k}\frac{\mu_k}{\mu_j}\left(\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right)^{a_1}\left(\frac{\epsilon_{2,k}}{\epsilon_{2,j}}\right)^{a_2}\left(\frac{\epsilon_{3,k}}{\epsilon_{3,j}}\right)^{a_3}-1=\frac{\xi_j-\xi_k}{\xi_k-\xi_i}\frac{E-F\xi_i}{E-F\xi_j}. \tag{6}$$

In this formula the right-hand side is in absolute value very small, in fact of the size of $|F|^{-4}$, by the definition of i. Put

$$\Lambda_i=\log\left|\frac{\xi_i-\xi_j}{\xi_i-\xi_k}\frac{\mu_k}{\mu_j}\right|+a_1\log\left|\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right|+a_2\log\left|\frac{\epsilon_{2,k}}{\epsilon_{2,j}}\right|+a_3\log\left|\frac{\epsilon_{3,k}}{\epsilon_{3,j}}\right|,$$

so that the left hand side of (6) equals $e^{\pm\Lambda_i}-1$. Then also $|\Lambda_i|$ is extremly small, of the size of $|F|^{-4}$.

Put

$$A=\max\{|a_1|,|a_2|,|a_3|\}.$$

Equation (4) suggests that $|F|$ is of the size of e^A, so that in fact $|\Lambda_i|$ is exponentially small in terms of A. Indeed, following the details of [TW], one finds

$$\text{if } |F|\geq F_0 \text{ then } |\Lambda_i|<C_1e^{-C_2A}, \tag{7}$$

with F_o, C_1, C_2 as below.

D	F_0	C_1	C_2
3	3	2.86921×10^4	3.01818
6	3	1.01488×10^5	4.12666
11	3	2.98502×10^5	5.01267
18	3	7.24331×10^5	2.63391
27	3	1.20295×10^5	3.01818
38	3	2.85210×10^6	6.87134

D	F_0	C_1	C_2
43	12	8.78250×10^{11}	12.9731
51	3	4.93434×10^6	7.26100
66	3	8.00597×10^6	7.59225
67	1100	1.37917×10^{13}	21.1564
83	3	1.23426×10^7	7.93874

Heuristically speaking, this is extraordinary for a linear form with coefficients of the size of A, which generically will be only polynomially small in terms of A. We will exploit this heuristic argument below.

5. Simplification Following the general theory as outlined in [**8**] would mean that one now has to proceed with four-term linear forms Λ_i. The number of terms in the linear forms is very important for the efficiency of the method. The upper bounds to be derived for A grow more than exponentially in terms of this number, and also the complexity of the reduction procedure to be performed depends very much on it. Although with the present state of the art a four-term linear form is very well doable in general, it's to the author's taste a matter of elegance to use a method as efficient as possible, by using properties special to the particular case, taking the shortcuts this suggests, rather than to follow blindly the longer route set out by the general theory.

We note that in our specific situations the linear forms Λ_i can be simplified considerably. Namely, due to our special choice of j,k, we have in the cases with $D \neq 18$ that $\epsilon_3 = \sigma(\epsilon_1)$, so $\epsilon_{3,j} = \sigma(\epsilon_{1,j}) = \epsilon_{1,k}$ and $\epsilon_{3,k} = \sigma(\epsilon_{1,k}) = \epsilon_{1,j}$, so that

$$\Lambda_i = \log\left|\frac{\xi_i - \xi_j}{\xi_i - \xi_k}\frac{\mu_k}{\mu_j}\right| + (a_1 - a_3)\log\left|\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right| + a_2 \log\left|\frac{\epsilon_{2,k}}{\epsilon_{2,j}}\right|,$$

and if $D = 18$ then we have $\sigma(\epsilon_3) = \epsilon_3$, so $\epsilon_{3,k} = \epsilon_{3,j}$, so that

$$\Lambda_i = \log\left|\frac{\xi_i - \xi_j}{\xi_i - \xi_k}\frac{\mu_k}{\mu_j}\right| + a_1 \log\left|\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right| + a_2 \log\left|\frac{\epsilon_{2,k}}{\epsilon_{2,j}}\right|.$$

This already is an important simplification.

Moreover, we can get rid of the first term. Namely, we note that

$$(\xi_1 - \xi_2)(\xi_3 - \xi_4) = (\xi_1 - \xi_4)(\xi_2 - \xi_3) = \frac{-4}{b}\sqrt{2D}, \qquad (\xi_1 - \xi_3)(\xi_2 - \xi_4) = \frac{-8}{b}\sqrt{2D}.$$

It follows that

$$\frac{\xi_i - \xi_j}{\xi_i - \xi_k} = \frac{(\xi_i - \xi_j)(\xi_j - \xi_\ell)}{(\xi_i - \xi_k)(\xi_j - \xi_\ell)} = \frac{b}{4\sqrt{2D}}(\xi_j^2 - (\xi_i + \xi_\ell)\xi_j + \xi_i\xi_\ell),$$

where ℓ is taken such that $\{i, j, k, \ell\} = \{1, 2, 3, 4\}$. If $D = 18$ then everything is in $\mathbb{K}_j$, since this field is galois. If $D \neq 18$ then everything is in the splitting field of $t^4 - 2Dt^2 + 2b^2D$, which is a quadratic extension of $\mathbb{K}_j$. Indeed, since $\sqrt{2D} \notin \mathbb{K}_j$, this splitting field is $\mathbb{K}_j(\sqrt{2D})$. However, notice that $\xi_i + \xi_\ell = \frac{-4a}{b} - \xi_j - \sigma(\xi_j) \in \mathbb{K}_j$ and $\xi_i\xi_\ell = 4/(\xi_j\sigma(\xi_j)) \in \mathbb{K}_j$. Indeed, we find

$$\sqrt{2D}\,\frac{\xi_i - \xi_j}{\xi_i - \xi_k} = \frac{1}{b^2}(b + \theta_j)(2D - \theta_j^2),$$

which is also true if $D = 18$. It follows that $\left(\frac{\xi_i - \xi_j}{\xi_i - \xi_k}\right)^2 \in \mathbb{K}_j$, in fact,

$$\left(\frac{\xi_i - \xi_j}{\xi_i - \xi_k}\right)^2 = \frac{4a^2 + 7b^2}{b^2} + \frac{4a^2 + 6b^2}{b^3}\theta_j - \frac{2}{b^2}\theta_j^2 - \frac{2}{b^3}\theta_j^3.$$

This shows that in the cases with $b = 1$ indeed $\left(\frac{\xi_i - \xi_j}{\xi_i - \xi_k}\right)^2$ is integral, and since its norm equals 1, it even is a unit. Furthermore, in these cases where $b = 1$ we also have $\mu = 1$, so that we have

$$\left(\frac{\xi_i - \xi_j}{\xi_i - \xi_k}\frac{\mu_k}{\mu_j}\right)^2 = -\frac{1 + \theta_j}{1 - \theta_j} = \begin{cases} -\left(\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right)^{-1} & \text{if } \; D \in \{3, 6, 11, 38, 51, 66, 83\}, \\ -\left(\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right)^2\left(\frac{\epsilon_{2,k}}{\epsilon_{2,j}}\right) & \text{if } \; D = 18 \\ -\left(\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right)\left(\frac{\epsilon_{2,k}}{\epsilon_{2,j}}\right)^{-1} & \text{if } \; D = 27. \end{cases}$$

In the cases with $b = 3$ we have $\mu = \rho^{-1}$, and then we happen to find that

$$\left(\frac{\xi_i - \xi_j\,\mu_k}{\xi_i - \xi_k\,\mu_j}\right)^2 = \begin{cases} -\left(\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right) & \text{if} \quad D = 43, \\ -\left(\frac{\epsilon_{2,k}}{\epsilon_{2,j}}\right)^{-1} & \text{if} \quad D = 67. \end{cases}$$

Now we put

$$b_1 = \begin{cases} 2a_1 - 2a_3 - 1 & \text{if} \quad D \in \{3, 6, 11, 27, 38, 51, 66, 83\}, \\ 2a_1 + 2 & \text{if} \quad D = 18, \\ 2a_1 - 2a_3 + 1 & \text{if} \quad D \in \{27, 43\}, \\ 2a_1 - 2a_3 & \text{if} \quad D = 67; \end{cases}$$

$$b_2 = \begin{cases} 2a_2 & \text{if} \quad D \in \{3, 6, 11, 38, 43, 51, 66, 83\}, \\ 2a_2 + 1 & \text{if} \quad D = 18, \\ 2a_2 - 1 & \text{if} \quad D \in \{27, 67\}. \end{cases}$$

Then we can write

$$2\Lambda_i = b_1 \log\left|\frac{\epsilon_{1,k}}{\epsilon_{1,j}}\right| + b_2 \log\left|\frac{\epsilon_{2,k}}{\epsilon_{2,j}}\right|, \tag{8}$$

and this is a linear form in only two logarithms with integer coefficients, which is very convenient to work with. Moreover, the number of linear forms itself has been halved, as we observe that $2\Lambda_1 = 2\Lambda_3$ and $2\Lambda_2 = 2\Lambda_4$.

We put

$$B = \max\{|b_1|, |b_2|\},$$

then we have (unless $a_1 = a_2 = a_3 = 0$ in the case $D = 67$)

$$B \le \begin{cases} 4A + 1 & \text{if} \quad D \in \{3, 6, 11, 27, 38, 43, 51, 66, 83\}, \\ 2A + 2 & \text{if} \quad D = 18, \\ 4A & \text{if} \quad D = 67. \end{cases} \tag{9}$$

6. Large upper bonds. We now apply a result from the theory of linear forms in logarithms of algebraic numbers, stating that such a linear form cannot be too small. The nice fact that now every linear form in logarithms $2\Lambda_i$ has only two terms (see (8)) means that we can use the very good result of Laurent, Mignotte and Nesterenko [**5**]. Note that for a linear form with three terms the best result today probably is that of Voutier [**9**], and for linear forms with more than three terms one can use the result of Baker and Wustholz [**1**].

We apply Corollaire 2 of [**5**] to the linear form $2\Lambda_i$, as given in (8). Note that the algebraic numbers inside the logarithms are multiplicatively independent elements of the quartic field $\mathbb{K}_j$. So, noting that $h(\frac{\alpha}{\beta}) \le h(\alpha) + h(\beta)$ for any α, β, we define A_j for $j = 1, 2$ by

$$\log A_j = \max\left\{2h(\epsilon_j), \frac{1}{4}\left|\log\left|\frac{\epsilon_{j,4}}{\epsilon_{j,2}}\right|\right|, \frac{1}{4}\left|\log\left|\frac{\epsilon_{j,3}}{\epsilon_{j,1}}\right|\right|, \frac{1}{4}\right\}.$$

We put

$$b' = \frac{1}{4}\left(\frac{|b_1|}{\log A_2} + \frac{|b_2|}{\log A_1}\right),$$

so that

$$b' \leq \frac{1}{4}\left(\frac{1}{\log A_1} + \frac{1}{\log A_2}\right)B.$$

And we put

$$L = \max\left\{\log b' + 0.14, \frac{21}{4}\right\}, \qquad C_3 = 6231.04 \log A_1 \log A_2.$$

Then Corollaire 2 of [5] tells us that

$$|2\Lambda_i| \leq e^{-C_3 L^2} \tag{11}$$

If

$$B \leq \exp\left(5.11 - \log\frac{1}{4}\left(\frac{1}{\log A_1} + \frac{1}{\log A_2}\right)\right)$$

then (10) implies $L = \frac{21}{4}$, and we find from (7) (assuming that $|F| \leq F_0$) that $A \leq B_1$, where

$$B_1 = \left\lfloor \frac{1}{C_2}\log(2C_1) + \frac{441}{16}\frac{C_3}{C_2} \right\rfloor.$$

Otherwise, we have $L = \log B + 0.14 + \log\frac{1}{4}\left(\frac{1}{\log A_1} + \frac{1}{\log A_2}\right)$, and then we find from (7) (assuming that $|F| \geq F_0$) and (11) that

$$A < \frac{1}{C_2}\log(2C_1) + \frac{C_3}{C_2}\left(\log B + 0.14 + \log\frac{1}{4}\left(\frac{1}{\log A_1} + \frac{1}{\log A_2}\right)\right)^2.$$

With (9) this gives an upper bound $A \leq B_2$ since A is less than a quadratic function of $\log A$. Hence we obtain

$$\text{if } |F| \geq F_0 \text{ then } A \leq \max\{B_1, B_2\}.$$

We computed the following numerical values for C_3, B_1, B_2

D	C_3	B_1	B_2
3	1.20264×10^4	109830	796051
6	1.32480×10^4	88487	609302
11	4.57474×10^4	251547	1880541
18	4.70294×10^3	49219	337082
27	1.20264×10^4	109830	796052
38	9.92799×10^4	398236	3028667
43	1.77433×10^5	376992	2665865
51	1.41947×10^5	538826	4218038
66	6.92735×10^4	251488	1800899
67	4.67517×10^5	609078	4299201
83	3.80034×10^5	1319441	11438210

In all cases we have $B_1 < B_2$, so $|F| \leq F_0 - 1$ or $A \leq B_2$.

7. Reduction of the upper bound. Although the upper bounds B$_2$ are so small that enumeration of all possibilities for d and e is practically possible, a much more efficient search can be done as follows. The basic idea is to use the heuristic argument mentioned above, that the linear forms Λ_i should behave generically, i.e. should be not essentially smaller than diophantine approximation theory suggests, namely linear in A^{-1}. As we now have an upper bound $A \leq B_2 \approx 10^7$, we have a good idea how small the linear forms can be, namely of the size of A^{-1}, which is at worst $\approx 10^{-7}$. If we can check that indeed for all coefficients below these bounds the linear forms are larger than $\approx 10^{-7}$, we can use (8) to obtain a reduced upper bound for A.

In practice it works as follows. Fix a linear form Λ_i, and let (d,e) be a solution of (7). Note that $\Lambda_1 = \Lambda_3$ and $\Lambda_2 = \Lambda_4$, so that we only have to look at $i = 1$ and $i = 2$, and if $D = 18$ then the relations $\epsilon_{1,1} = -\epsilon_{1,2} = -\epsilon_{1,3}^{-1} = \epsilon_{1,4}^{-1}$, and $\epsilon_{2,1} = \epsilon_{2,2}^{-1} = -\epsilon_{2,3}^{-1} = -\epsilon_{2,4}$ imply that Λ_1 and Λ_2 are the same, when the sign of b_2 is changed. So if $D = 18$ we only have to consider $i = 1$.

Pick a convenient large enough constant C$_4$, somewhat larger than the square of the upper bound B$_2$ for A. Define $\lambda \in \mathbb{Z}$, by

$$\begin{pmatrix} 1 & 0 \\ [C_4 \log |\epsilon_{1,k}/\epsilon_{1,j}|] & [C_4 \log |\epsilon_{2,k}/\epsilon_{2,j}|] \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} b_1 \\ \lambda \end{pmatrix},$$

where $[\cdot]$ denotes rounding to an integer. This formula says that the point $(d, \lambda)^{\mathsf{T}}$ is in the lattice spanned by the columns of the above matrix, and because at least one of b_1 and b_2 is odd, this point is not zero. This lattice point is of interest to us, because λ is approximately equal to $2C_4\Lambda_i$ (compare (8)), hence relatively small by (7).

By a variant of the euclidean algorithm (in fact we compute the simple continued fraction expansion of $-\frac{\log |\epsilon_{1,k}/\epsilon_{1,j}|}{\log |\epsilon_{2,k}/\epsilon_{2,j}|}$), we can find the nonzero lattice point closest to zero, and this gives us a lower bound ℓ for the length of the vector $(b_1, \lambda)^{\mathsf{T}}$. We expect that ℓ is of the size of the square root of the volume of a fundamental domain of the lattice, which is approximately C$_4$. So ℓ will be at least of the size of the upper bound B$_2$. Increasing C$_4$ will in general cause an increasing ℓ. On the other hand, the first component of the vector $(b_1, \lambda)^{\mathsf{T}}$ is b_1, which is at most of the size of B_2. Hence the second component, λ, will be large, which is contradictory, as we've just seen that it's small.

To make this reasoning precise, let us put

$$B_3 = \begin{cases} 4B_2 + 1 & \text{if} \quad D \in \{3, 6, 11, 27, 38, 43, 51, 66, 83\}, \\ 2B_2 + 2 & \text{if} \quad D = 18, \\ 4B_2 & \text{if} \quad D = 67. \end{cases}$$

so that (9) implies $B \leq B_3$. Then we have

$$\ell^2 \leq b_1^2 + \lambda^2 \leq B_3^2 + \lambda^2,$$

and λ is defined such that

$$|\lambda - 2C_4\Lambda_i| \leq |b_1| + |b_2| \leq 2B \leq 2B_3.$$

Hence

$$|\Lambda_i| \geq \frac{1}{2C_4}\left(\sqrt{\ell^2 - B_3^2} - 2B_3\right)$$

which is possible only if we have taken C_4 large enough so that $\ell > \sqrt{5}B_3$ (if this is not the case, take a somewhat larger C_4). Then (7) implies (under the assumption $|F| \geq F_0$)

$$A \leq \left\lfloor \frac{1}{C_2}\left(\log(2C_1) + \log C_4 - \log\left(\sqrt{\ell^2 - B_3^2} - 2B_3\right)\right)\right\rfloor.$$

Thus we have found a new upper bound for A, and we can repeat the procedure with B_2 replaced with this new upper bound, and a new C_4, to see if we can get further improvement.

Here are some details of the computations. For C_4 we took the power of 10 for which $\ell > \sqrt{5}C_4$ turned out to be true, and the new upper bound turned out to be the best reachable. In all cases we did two successive reduction steps, and in the case $D = 38$ a third step also yielded a further improvement. The data for the first and second reduction steps are as follows.

	$i=1$		$i=2$		
D	C_4	$\ell >$	C_4	$\ell >$	$A \leq$
3	10^{14}	1.10660×10^7	10^{14}	1.80099×10^7	9
6	10^{14}	1.35144×10^7	10^{14}	1.76093×10^7	6
11	10^{15}	3.24838×10^7	10^{14}	3.22646×10^7	6
18	10^{13}	3.32629×10^6			11
27	10^{14}	1.10660×10^7	10^{14}	1.80099×10^7	9
38	10^{15}	4.13470×10^7	10^{14}	4.24690×10^7	4
43	10^{14}	4.25311×10^7	10^{15}	5.96382×10^7	3
51	10^{17}	1.46002×10^8	10^{14}	4.97647×10^7	5
66	10^{14}	1.61715×10^7	10^{14}	3.03380×10^7	4
67	10^{16}	9.47743×10^7	10^{14}	4.09314×10^7	2
83	10^{17}	4.64362×10^8	10^{15}	2.59490×10^8	4

	$i=1$		$i=2$		
D	C_4	$\ell >$	C_4	$\ell >$	$A \leq$
3	10^4	137.974	10^4	220.102	5
6	10^4	68.5054	10^4	173.611	4
11	10^4	165.027	10^3	96.213	3
18	10^6	1342.82			7
27	10^4	137.974	10^4	220.102	5
38	10^4	91.3892	10^3	110.571	3
43	10^4	239.002	10^3	57.0350	2
51	10^4	57.0087	10^3	178.986	3
66	10^4	159.477	10^3	80.9938	2
67	10^2	18.3847	10^2	35.4683	1
83	10^3	46.0434	10^3	156.003	2

Finally, when $D = 38$ we did a third step, with data as follows.

	$i=1$		$i=2$		
D	C_4	$\ell >$	C_4	$\ell >$	$A \leq$
38	10^3	36.0555	10^3	110.571	2

It is good to realise again what really is going on here, as this reduction of the upper bound from $\approx 10^7$ to only ≈ 10 is dramatic and seems mysterious. In fact, we have shown above that the existence of a solution of (7) with $A \leq B_2$ either has a very small A, or implies the existence of a nonzero lattice point in the given lattice with a distance to zero less than or equal to ℓ. By inspection, after having performed the euclidean algorithm, we know that such lattice points do not exist. We could also have said (in fact, this is equivalent to the above reasoning) that the existence of a solution with large A implies the existence of a large partial quotient in the simple continued fraction expansion of $-\frac{\log|\epsilon_{1,k}/\epsilon_{1,j}|}{\log|\epsilon_{2,k}/\epsilon_{2,j}|}$, in the range where the denominators of the convergents are at most B_3. As we can actually compute these continued fractions, we can simply see that such large partial quotients do not occur. We preferred to give the argument in terms of lattices, because this can be generalised straightaway to linear forms with more than two logarithms, see [**10**].

8. Conclusion. It remains to find the solutions with $A \leq 5, 4, 3, 7, 5, 2, 2, 3, 2, 1, 2$, respectively, in the case $D = 3, 6, 11, 18, 27, 38, 43, 51, 66, 67, 83$, and those with $|F| \leq F_0 - 1$. This can be done easily as follows. For all the remaining possibilities of (a_1, a_2, a_3) with $A = \max\{|a_1|, |a_2|, |a_3|\}$ below the upper bound we check Siegel's identity (5) (single precision suffices). This revealed in all the cases with $b = 1$ the solution $(a_1, a_2, a_3) = (0, 0, 0)$, leading to $(E, F) = \pm(1, 0)$, in the case $D = 6$ also the solution $(a_1, a_2, a_3) = (0, -1, 1)$, leading to $(E, F) = \pm(1, -1)$, and in the case $D = 43$ the solution $(a_1, a_2, a_3) = (0, 0, 0)$, leading to $(E, F) = \pm(1, -1)$, and no other solutions.

The solutions E, F with $2 \leq |F| \leq F_0 - 1$ correspond to convergents $\frac{E}{F}$ of the simple continued fraction expansion of ξ_i (note that $\left|\frac{E}{F} - \xi_i\right|$ is of the size of $|F|^{-4}$, as argued immediately after equation (4); in fact one can prove easily that if $|F| \geq 2$ then $\left|\frac{E}{F} - \xi_i\right| < \frac{1}{2F^2}$, see [8]). Thus only in the cases $D = 43$, and $D = 67$ the continued fractions of $\xi_1, \xi_2, \xi_3, \xi_4$ have to be computed, up to the first convergent with denominator exceeding F_0. This produced no solutions. Finally, the solutions with $|F| \leq 1$ are trivally found.

This completes the proof of Theorem 2, hence also that of Theorem 1. All the computations were performed on a 486/75 notebook PC, using Pari-1.39-03, Maple V.4 and Borland Pascal 7.0 The total computation time was only a few minutes.

REFERENCES

1. A. Baker and G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62.

2. R. Bumby, The diophantine equation $3x^4 - 2y^2 = 1$, *Math. Scand.* **21** (1967), 144–148.

3. J. H. E. Cohn, Eight diophantine equations, *Proc. London Math. Soc. (3)* **16** (1966), 153–166.

4. J. H. E. Cohn, Twelve diophantine equations, *Arch. Math.* (Basel) **65** (1995), 130–133.

5. M. Laurent, M. Mignotte and Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Th.* **55** (1995), 285–321.

6. M. Mignotte and A. Pethő, On the system of diophantine equations $x^2 - 6y^2 = -5$ and $x = 2z^2 - 1$, *Math. Scand.* **76** (1995), 50–60.

7. N. Tzanakis, Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations, *Acta Arith.* **75** (1996). 165–190

8. N. Tzanakis and B. M. M. de Weger, On the practical solution of the Thue equation, *J. Number Th.* **31** (1989), 99–132.

9. P. Voutier, Linear forms in three logarithms, *Canad. J. Math*, (1998), to appear.

10. B. M. M. de Weger, *Algorithms for Diophantine equations* (CWI Tract 65, Centre for Mathematics and Computer Science, Amsterdam, 1989).

Sportsingel 30
2924 XN Krimpen aan den IJssel
The Netherlands
E-mail: dweger@xs4all.nl