JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

BENJAMIN M. M. DE WEGER

S-integral solutions to a Weierstrass equation

Journal de Théorie des Nombres de Bordeaux, tome 9, nº 2 (1997), p. 281-301

<http://www.numdam.org/item?id=JTNB_1997__9_2_281_0>

Journal de Théorie des Nombres
de Bordeaux **9** *(1997), 281–301*

S-integral solutions to a Weierstrass equation

par Benjamin M.M. de WEGER

Résumé. On détermine les solutions rationnelles de l'équation diophantienne $y^2 = x^3 - 228x + 848$ dont les dénominateurs sont des puissances de 2. On applique une idée de Yuri Bilu, qui évite le recours à des équations de Thue et de Thue-Mahler, et qui permet d'obtenir des équations aux (S-) unités à quatre termes dotées de propriétés spéciales, que l'on résout par la théorie des formes linéaires en logarithmes réels et p-adiques.

Abstract. The rational solutions with as denominators powers of 2 to the elliptic diophantine equation $y^2 = x^3 - 228x + 848$ are determined. An idea of Yuri Bilu is applied, which avoids Thue and Thue-Mahler equations, and deduces four-term (S-) unit equations with special properties, that are solved by linear forms in real and p-adic logarithms.

1. Introduction

In a recent paper [SW1], my colleague R.J. Stroeker and I determined the complete set of solutions in rational integers to the diophantine equation

$$3(y^2 - 1) = 2x^2(x^2 - 1). \tag{Q}$$

The quartic diophantine equation (Q) can be seen as a model of an elliptic curve. In our solution methods we did not use that viewpoint, but rather worked algebraically. Recently N. Tzanakis [T] has shown how the elliptic logarithms method of Stroeker and Tzanakis [ST], originally designed for Weierstrass models of elliptic curves only, can be adapted to the situation of a quartic model for an elliptic curve, and in fact he chose equation (Q) as one of the examples to illustrate his ideas.

We stress that the problem of integral points on elliptic curves is not a well defined problem, in contrast to the problem of rational points. Birational transformations between different models of the same curve do respect the concept of rational point, but not that of integral point, in an

This research was supported by the Netherlands Mathematical Research Foundation SWON with financial aid from the Netherlands Organization for Scientific Research NWO.
Manuscrit reçu le 18 mars 1997.

essential way. Therefore one should speak of integral solutions to elliptic equations, rather than of integral points on elliptic curves.

When Stroeker and I worked on equation (Q), we also computed (as kind of a standard procedure when dealing with an elliptic curve) the Weierstrass equation of the elliptic curve it represents, being

$$\text{(W)} \qquad y^2 = x^3 - 228x + 848.$$

We did a limited search for integral solutions, and found that there is a large, but of course finite, number of them. Thus we found it a natural question to ask for all the integral solutions to equation (W), and the remarks in the previous paragraph show that this problem is entirely different from that of solving equation (Q). This paper solves this problem, and indeed a bit more, since it turned out to be not too much additional work to determine the complete set of rational solutions to (W) with only powers of 2 in the denominators, i.e. the S-integral solutions for the prime 2.

For determining the integral solutions the method of elliptic logarithms [ST] (see also [GPZ1], [S]) is efficient, if a basis for the free part of the Mordell-Weil group is known. However, a general method for this latter problem has not yet been found. Moreover, a p-adic analogue of this method, that would be needed for the S-integer solutions, is not yet fully available, mainly due to the fact that there is not yet a fully explicit theory of linear forms in p-adic elliptic logarithms, analogous to the excellent work of S. David [D]. For the rank 1 case however this has recently been done [RU]. When a lower bound for p-adic elliptic logarithms can be calculated and the Mordell-Weil basis is known, then it is known how to proceed, see Smart [S], and Gebel, Pethő and Zimmer [GPZ2].

As we have a rank 2 curve here, for the S-integral solutions we have to apply more or less classical ideas. One method would be to translate the problem into Thue- and Thue-Mahler equations, and treating those with diophantine approximation methods, such as in [TW1], [TW2]. An alternative approach here is to use a new idea of Yuri Bilu [B], [BH], which uses 'ordinary' (non-elliptic) linear forms in logarithms, but bypasses the Thue (-Mahler) equations. This last method is practical in our case, due to the nice factorization over $\mathbb{Q}$ of the cubic polynomial in (W), and it is this method we use in this paper. This seems to be the first time such a method is used for S-integral solutions.

We did work out the details for the other methods (elliptic logarithms for the integral solutions and Thue-Mahler equations for the S-integral solutions) too, but as this yields only routine proofs of the same results, we omit details of these proofs.

As a general conclusion of this paper we might state that Bilu's method can be practical and efficient, also p-adically, but only in special cases.

All the computations reported in this paper have been done on a 486 personal computer. We used our own multi-precision routines; for the algebraic number field data we used Pari 1.38.

We now state our main result.

THEOREM 1. *The only rational solutions to the Weierstrass-equation*

$$\text{(W)} \qquad y^2 = x^3 - 228x + 848$$

of which the denominators of x and y are powers of 2, *are the following* 43:

x	$\pm y$
$-16\,439/2^{10}$	$631\,035/2^{15}$
-16	20
-14	36
-11	45
-2	36
$1/2^2$	$225/2^3$
2	20
$49/2^4$	$855/2^6$
4	0
13	9
14	20
16	36
$97/2^2$	$783/2^3$
34	180
52	360
53	371
94	900
196	2 736
$857/2^2$	$25\,027/2^3$
754	20 700
814	23 220
534 256	390 502 764

2. Preliminaries

We rewrite the problem of rational solutions to (W) with powers of 2 as denominators to the equation

$$\text{(W}'\text{)} \qquad y^2 = (x - 2^{2k+2})(x^2 + 2^{2k+2}x - 53 \cdot 2^{4k+2}),$$

where $x, y \in \mathbb{Z}$ and $k \in \mathbb{Z}_{\geq 0}$. We may assume that

$$(1) \qquad k = 0 \quad \text{or} \quad \mathrm{ord}_2(x) \leq 1,$$

since if (x, y, k) is a solution with $4|x$ and $k \geq 1$, then also $(\frac{1}{4}x, \frac{1}{8}y, k-1)$ is a solution.

The right hand side of (W′) being a square, thus being ≥ 0, implies

$$-(2 + 6\sqrt{6})2^{2k} < x \leq 2^{2k+2} \quad \text{or} \quad x > (-2 + 6\sqrt{6})2^{2k}.$$

Let d be the squarefree part of $x - 2^{2k+2}$ such that the sign of d equals the sign of $x - 2^{2k+2}$. Then d is also the squarefree part of $x^2 + 2^{2k+2}x - 53 \cdot 2^{4k+2}$, and it has the same sign. Now, by (W′) we can write

$$\begin{cases} x - 2^{2k+2} & = du^2, \\ x^2 + 2^{2k+2}x - 53 \cdot 2^{4k+2} & = dv^2 \end{cases}$$

for some $u, v \in \mathbb{Z}_{\geq 0}$. Further, $d | (x - 2^{2k+3})(x - 2^{2k+2}) - (x^2 + 2^{2k+2}x - 53 \cdot 2^{4k+2}) = 45 \cdot 2^{2k+2}$, hence $\pm d \in \{1, 2, 3, 5, 6, 10, 15, 30\}$. Substituting the first equation into the second we find

$$(3 \cdot 2^{2k+1} + du^2)^2 - 6(3 \cdot 2^{2k+1})^2 = dv^2. \tag{2}$$

Equation (2) is of the type $X^2 - 6Y^2 = dZ^2$.
If $d \in \{-30, -10, -3, -1, 2, 5, 6, 15\}$, then this equation has no solutions, as is easily shown.

If $d < 0$ and $k = 0$ then $-(2 + 6\sqrt{6}) < x \leq 4$, which only leaves the solutions with $x = -16, -14, -11, -2, 2, 4$. It follows that if $k = 0$ then we may assume that $x \geq \lceil -2 + 6\sqrt{6} \rceil = 13$.

If $d \in \{-6, -2, 10, 30\}$ and $k \geq 1$ then $x - 2^{2k+2} = du^2$ and (1) imply that u is odd. It follows that $\mathrm{ord}_2(3 \cdot 2^{2k+1} + du^2) = 1$, hence the left hand side of (2) has 2-adic order equal to 2. But $\mathrm{ord}_2(dv^2)$ is odd, which is contradictory.

If $d = -5$ and $k \geq 1$ then we find from (2) that $25u^4 \equiv -5v^2 \pmod{16}$. Since -5 is not a quadratic residue (mod 16), this implies $2|u$ and $4|v$, leading to a contradiction with (1).

If $d = 3$ and $k \geq 1$ then clearly $3|v$, hence put $v = 3w$. Then (2) leads to $(2^{2k+1} + u^2)^2 - 6(2^{2k+1})^2 = 3w^2$. By (1) we infer that u is odd, and then we see that $1 \equiv 3w^2 \pmod{8}$, which is impossible.

Finally, if $d = 1$ then we derive from (2) that

$$\begin{cases} 3 \cdot 2^{2k+1} + u^2 + v &= 2^a 3^b, \\ 3 \cdot 2^{2k+1} + u^2 - v &= 2^{4k+3-a} 3^{3-b}, \end{cases}$$

where $a, b \in \mathbb{Z}$ with $0 \leq a \leq 4k+3$ and $0 \leq b \leq 3$. This system is equivalent to

$$\begin{cases} 3 \cdot 2^{2k+1} + u^2 &= 2^{a-1} 3^b + 2^{4k+2-a} 3^{3-b}, \\ v &= 2^{a-1} 3^b - 2^{4k+2-a} 3^{3-b}. \end{cases}$$

This immediately shows that $1 \leq a \leq 4k + 2$.

If $2 \leq a \leq 4k + 1$ then u is even, hence $4|x$, which contradicts (1). If $a = 1$ then $0 \leq v = 3^b - 2^{4k+1} 3^{3-b}$, which implies $2^{4k+1} \leq 3^{2b-3} \leq 27$, and thus $k = 0$. Clearly the only solution in this case is $(u, v) = (3, 3)$, leading to the solution with $x = 13$. Hence we may assume that $a = 4k + 2$, and thus

$$3 \cdot 2^{2k+1} + u^2 = 2^{4k+1} 3^b + 3^{3-b}.$$

If $b = 0$ then $u^2 \equiv 2 \pmod{3}$, which is impossible.

If $b = 2$ then $3|u$, so put $u = 3t$, Then we obtain $2^{2k+1} + 3t^2 = 3 \cdot 2^{4k+1} + 1$, which is impossible (mod 3).

If $b = 1$ then again $3|u$, so we put $u = 3t$, leading to $3(t^2 - 1) = 2^{2k+1}(2^{2k} - 1)$, and it follows that $2^{2k+1} | (t + 1)(t - 1)$. By $t > 0$ there is an integer $\alpha > 0$ such that $t = \pm 1 + \alpha 2^{2k}$. This implies $2^{2k-1} = \frac{\mp 3\alpha - 1}{3\alpha^2 - 2}$, which is easily seen to have only one solution: $\alpha = 1, k = 1$, leading to $t = 3$, so that $(u, v) = (9, 87)$, leading to $x = 97/2^2$.

If $b = 3$ then we have $u^2 - 1 = 3 \cdot 2^{2k+1}(9 \cdot 2^{2k} - 1)$, and it follows that $2^{2k+1} | (u+1)(u-1)$. By $u > 0$ there is an integer $\alpha > 0$ such that $u = \pm 1 + \alpha 2^{2k}$, and this implies $2^{2k-1} = \frac{\mp \alpha - 3}{\alpha^2 - 54}$, which is easily seen to have only three solutions: $\alpha = 6, k = 0$ and $\alpha = 8, k = 0$, both implying $(u, v) = (7, 53)$, and leading to the solution with $x = 53$, and $\alpha = 7, k = 1$, implying $(u, v) = (29, 863)$, leading to the solution with $x = 857/2^2$.

This completes the treatment of the case $d = 1$.

3. Bilu's idea

We now have the following situation:

$$\begin{aligned} x - 2^{2k+2} &= du^2, && (3) \\ x^2 + 2^{2k+2}x - 53 \cdot 2^{4k+2} &= dv^2 && (4) \end{aligned}$$

for some $u, v \in \mathbb{Z}_{\geq 0}$, and with either $k = 0$, $d \in \{3, 10, 30\}$, $x \geq 13$, or $k \geq 1$, $d = -15$, $-(2 + 6\sqrt{6})2^{2k} < x \leq 2^{2k+2}$. We factor equation (4) over $\mathbb{Q}(\xi)$ for ξ a root of $x^2 = 6$, and one of its factors can be written as

$$x + 2^{2k+1} + 2^{2k+1}3\xi = \alpha\beta^2, \tag{5}$$

where α is squarefree, d is the squarefree part of $N\alpha$, and α is determined up to squares of the fundamental unit $5 + 2\xi$. Thus there are only a few possibilities for α, and we have to find them all.

In $\mathbb{Q}(\xi)$ we denote conjugation by a bar, so $\overline{\xi} = -\xi$. We have the following decompositions:

$$\begin{aligned} &1 = (5 + 2\xi)(5 - 2\xi), \quad 2 = (2 + \xi)^2(5 + 2\xi)^{-1}, && (6) \\ &3 = (3 + \xi)^2(5 + 2\xi)^{-1}, \quad 5 = -(1 + \xi)(1 - \xi), \end{aligned}$$

with $2 + \xi$, $3 + \xi$, $1 + \xi$ and $1 - \xi$ being non-associated primes.

Let π be a prime dividing α. If it divides also $\overline{\alpha}$, then it divides $\alpha\beta^2 - \overline{\alpha}\overline{\beta}^2 = 2^{2k+2}3\xi$, so $\pi = 2 + \xi$ or $\pi = 3 + \xi$. If π does not divide $\overline{\alpha}$, then by $dv^2 = \alpha\overline{\alpha}(\beta\overline{\beta})^2$ we see that $\mathrm{ord}_\pi(d)$ has the same parity as $\mathrm{ord}_\pi(\alpha)$, which is 1, since α is squarefree. Thus π divides d. Hence we find, using also that $\alpha > 0$, that

$$\alpha = (5 + 2\xi)^p(2 + \xi)^q(3 + \xi)^r(1 + \xi)^s(-1 + \xi)^t$$

for $p, q, r, s, t \in \{0, 1\}$, with $(s, t) \neq (1, 1)$. Since d is the squarefree part of $N\alpha = 2^q 3^r(-5)^{s+t}$, we find that actually $d = N\alpha$. This leaves the following possibilities (where we sometimes take the freedom of adding a multiple of 2 to p):

d	p	q	r	s	t	α
3	0	0	1	0	0	$3+\xi$
	−1	0	1	0	0	$3-\xi$
10	0	1	0	1	0	$8+3\xi$
	−1	1	0	1	0	$4-\xi$
	0	1	0	0	1	$4+\xi$
	−1	1	0	0	1	$8-3\xi$

d	p	q	r	s	t	α
30	−2	1	1	1	0	$18-7\xi$
	−1	1	1	1	0	$6+\xi$
	0	1	1	0	1	$18+7\xi$
	−1	1	1	0	1	$6-\xi$
−15	0	0	1	1	0	$9+4\xi$
	−1	0	1	1	0	$-3+2\xi$
	0	0	1	0	1	$3+2\xi$
	−1	0	1	0	1	$-9+4\xi$

We get rid of the cases $\alpha = 8 \pm 3\xi$, $\alpha = 18 \pm 7\xi$, $\alpha = \pm 3 + 2\xi$, by noting that the quadratic equation obtained from comparing the coefficients of ξ in $x + 2^{2k+1} + 2^{2k+1}3\xi = \alpha(A + B\xi)^2$ (from inserting $\beta = A + B\xi$ in (5)) is impossible (mod 5). For example, in the case $\alpha = \pm 3 + 2\xi$ this equation is $2A^2 + 6AB + 12B^2 = 2^{2k+1}3$, which is equivalent to $(2A + 3B)^2 + 15B^2 = 2^{2k+2}3$, which is impossible modulo 5.

For $\alpha = 3 - \xi, 4 + \xi, 6 - \xi, 9 - 4\xi$ we take in (5) the conjugate in $\mathbb{Q}(\xi)$. Then we have to replace β by $\overline{\beta}$ (which is allowed because it is a variable), and replace the parameters α and ξ by their conjugates $\overline{\alpha}$ and $-\xi$.

Thus we are left with only four values for α, namely $\alpha = 3 + \xi, 4 - \xi, 6 + \xi, 9 + 4\xi$, and for each of them we have the case of ξ remaining as it is, and the case of ξ replaced by $-\xi$.

Now we eliminate x from (3) and (5), and we find

$$du^2 - \alpha\beta^2 = -2^{2k+1}3(1 \pm \xi), \tag{7}$$

the ± corresponding to the cases as described in the preceding paragraph. Bilu's idea (cf. [B], [BH]) now is that this equation, multiplied by d, factors over the quartic field $\mathbb{K} = \mathbb{Q}(\psi)$, where ψ satisfies $\psi^2 = d\alpha$. Then from the four different conjugates of these factors we can eliminate the variables $u \in \mathbb{Z}$ and $\beta \in \mathbb{Q}(\xi)$, and obtain a four-term (S-) unit equation with special properties.

4. The quartic field for $d = 3$

Let θ be a root of $x^4 - 6x^2 + 3 = 0$. Then $\psi = -6\theta + \theta^3$, $\xi = 3 - \theta^2$ satisfy $\psi^2 = 3\alpha = 3(3 - \xi)$, $\xi^2 = 6$. The field $\mathbb{K} = \mathbb{Q}(\psi) = \mathbb{Q}(\theta)$ has discriminant $27648 = 2^{10}\,3^3$, integral basis $\{1, \theta, \theta^2, \theta^3\}$, trivial class group, Galois group $\mathbb{D}_4$, a set of fundamental units is

$$\epsilon = 4 - 5\theta - \theta^2 + \theta^3, \quad \eta = -1 - \theta + 2\theta^2 + \theta^3, \quad \chi = 1 - \theta - 2\theta^2 + \theta^3,$$

and $\eta^{-1}\chi^{-1} = 5+2\xi$ is the fundamental unit of the quadratic subfield $\mathbb{Q}(\xi)$. We have the following relevant decompositions into primes:

$$\begin{array}{rcll} 2+\xi & = & p^2\epsilon\eta^{-1}\chi^{-1}, & \text{with } p = 1+\theta, \\ 3+\xi & = & q^2\eta^{-1}\chi^{-1}, & \text{with } q = \theta, \\ 1+\xi & = & r_1 r_2, & \text{with } r_1 = 2-\theta, \quad r_2 = 2+\theta, \\ 1-\xi & = & -r_3, & \text{with } r_3 = 2-\theta^2. \end{array}$$

There is a nontrivial $\mathbb{Q}(\xi)$-automorphism σ of $\mathbb{K}$, defined by $\sigma\theta = -\theta$. It acts as follows on the numbers defined above:

$$\sigma\psi = -\psi, \quad \sigma\epsilon = \epsilon^{-1}, \quad \sigma\eta = -\chi, \quad \sigma\chi = -\eta,$$

$$\sigma p = p\epsilon, \quad \sigma q = -q, \quad \sigma r_1 = r_2, \quad \sigma r_2 = r_1, \quad \sigma r_3 = r_3.$$

From (7) with $1-\xi$ in the right hand side we find, by (6) and $k = 0$, that

$$(3u)^2 - \psi^2\beta^2 = -18(1-\xi) = p^4 q^8 r_3 \epsilon^2 \eta^{-3}\chi^{-3},$$

and hence we find for its two factors

$$3u + \psi\beta = \pm p^a q^b r_3^c \epsilon^l \eta^m \chi^n,$$

$$3u - \psi\beta = \sigma(3u+\psi\beta) = \pm(-1)^{b+m+n} p^a q^b r_3^c \epsilon^{a-l} \eta^n \chi^m$$

for some $a, b, c \in \mathbb{Z}_{\geq 0}, l, m, n \in \mathbb{Z}$. On multiplying it follows at once that $2c = 1$, which is impossible.

From (7) with $1+\xi$ in the right hand side we find, by (6) and $k = 0$, that

$$(3u)^2 - \psi^2\beta^2 = -18(1+\xi) = -p^4 q^8 r_1 r_2 \epsilon^2 \eta^{-3}\chi^{-3},$$

and hence

$$3u + \psi\beta = \pm p^a q^b r_1^c r_2^d \epsilon^l \eta^m \chi^n,$$

$$3u - \psi\beta = \sigma(3u+\psi\beta) = \pm(-1)^{b+m+n} p^a q^b r_1^d r_2^c \epsilon^{a-l} \eta^n \chi^m$$

for some $a, b, c, d \in \mathbb{Z}_{\geq 0}, l, m, n \in \mathbb{Z}$. It follows at once that $a = 2$, $b = 4$, $(c, d) = (1, 0)$ or $(0, 1)$, $n = -m-3$. Because of symmetry we may disregard without loss of generality one of the cases for (c, d). So we take $c = 1, d = 0$, and hence we obtain

$$3u + \psi\beta = \pm\gamma\epsilon^l(\eta/\chi)^m, \tag{8}$$

where $\gamma = p^2 q^4 r_1 \chi^{-3} = 48+9\theta-96\theta^2-39\theta^3$, and $\eta/\chi = -1-2\theta+4\theta^2+2\theta^3$. Notice that we intend to show that there are only the following solutions to (8):

x	u	β	l	m	$\pm$
16	2	ξ	1	-1	+
52	4	$-6+\xi$	0	-1	−
196	8	$6-5\xi$	0	-2	−
534256	422	$-336+265\xi$	3	1	+

5. The quartic field for $d = 10$

Let θ be a root of $x^4 - 8x^2 + 10 = 0$. Then $\psi = -8\theta + \theta^3$, $\xi = -4 + \theta^2$ satisfy $\psi^2 = 10\alpha = 10(4-\xi)$, $\xi^2 = 6$. The field $\mathbb{K} = \mathbb{Q}(\psi) = \mathbb{Q}(\theta)$ has discriminant $92160 = 2^{11}3^2 5$, integral basis $\{1, \theta, \theta^2, \theta^3\}$, trivial class group, Galois group $\mathbb{D}_4$, a set of fundamental units is

$$\epsilon = 7 - 6\theta - \theta^2 + \theta^3, \quad \eta = -3 + 2\theta^2, \quad \chi = -3 + 3\theta^2 + \theta^3,$$

and $\eta = 5 + 2\xi$ is the fundamental unit of the quadratic subfield $\mathbb{Q}(\xi)$. We have the following relevant decompositions into primes:

$$\begin{array}{rcll} 2+\xi & = & p^2\epsilon\eta\chi, & \text{with } p = -4-\theta+\theta^2, \\ 3+\xi & = & -q_1q_2, & \text{with } q_1 = -1-\theta, \quad q_2 = -1+\theta, \\ 1+\xi & = & -r_1, & \text{with } r_1 = 3-\theta^2, \\ 1-\xi & = & -r_2^2\epsilon^{-1}\eta^{-1}\chi^{-1} & \text{with } r_2 = 5+\theta-3\theta^2-\theta^3. \end{array}$$

There is a nontrivial $\mathbb{Q}(\xi)$-automorphism σ of $\mathbb{K}$, defined by $\sigma\theta = -\theta$. It acts as follows on the numbers defined above:

$$\sigma\psi = -\psi, \quad \sigma\epsilon = -\epsilon^{-1}, \quad \sigma\eta = \eta, \quad \sigma\chi = -\chi^{-1},$$

$$\sigma p = -p\epsilon\chi, \quad \sigma q_1 = q_2, \quad \sigma q_2 = q_1, \quad \sigma r_1 = r_1, \quad \sigma r_2 = r_2\epsilon^{-1}\chi^{-1}.$$

From (7) with $1-\xi$ in the right hand side we find, by (6) and $k = 0$, that

$$(10u)^2 - \psi^2\beta^2 = -60(1-\xi) = -p^8q_1^2q_2^2r_1r_2^4\epsilon^2\eta^{-1}\chi^2,$$

and hence

$$(9) \quad \begin{cases} 10u + \psi\beta = \pm p^a q_1^b q_2^c r_1^d r_2^e \epsilon^l \eta^m \chi^n, \\ 10u - \psi\beta = \sigma(10u+\psi\beta) = \pm(-1)^{a+l+n} p^a q_1^c q_2^b r_1^d r_2^e \epsilon^{a-e-l} \eta^m \chi^{a-e-n}, \end{cases}$$

for some $a, b, c, d, e \in \mathbb{Z}_{\geq 0}, l, m, n \in \mathbb{Z}$. It follows at once that $2d = 1$, which is impossible.

From (7) with $1+\xi$ in the right hand side we find, by (6) and $k = 0$, that

$$(10u)^2 - \psi^2\beta^2 = -60(1+\xi) = -p^8q_1^2q_2^2r_1^2r_2^2\epsilon^3\chi^3,$$

and hence we find again (9) for some $a, b, c, d, e \in \mathbb{Z}_{\geq 0}, l, m, n \in \mathbb{Z}$. Now it follows at once that $a = 4$, $(b, c) = (2, 0)$ or $(1, 1)$ or $(0, 2)$, $d = 1$, $e = 1$, $m = 0$, $l + n \equiv 1 \pmod 2$. Because of symmetry we may disregard without loss of generality one of the cases $(2,0),(0,2)$ for (b,c). So we take either $b=2, c=0$ or $b=1, c=1$, and hence we obtain

$$10u + \psi\beta = \pm\gamma\epsilon^l\chi^n, \tag{10}$$

where γ equals $\gamma_1 = p^4q_1^2r_1r_2 = -710 - 82\theta + 310\theta^2 - 66\theta^3$ or $\gamma_2 = p^4q_1q_2r_1r_2 = 970 - 342\theta - 610\theta^2 + 234\theta^3$. Notice that we intend to show that there are only the following solutions to (10):

x	u	β	γ	l	n	$\pm$
14	1	$2+\xi$	γ_1	2	1	$-$
94	3	$6+\xi$	γ_2	2	1	$+$
94	3	$-6-\xi$	γ_2	1	2	$-$
814	9	$6+7\xi$	γ_2	0	1	$+$
814	9	$-6-7\xi$	γ_2	3	2	$-$

Solutions for $\gamma = \gamma_2$ occur in pairs, because $\sigma\gamma_2 = \gamma_2\epsilon^3\chi^3$, so if (l,n) is a solution, then so is $(3-l, 3-n)$.

6. The quartic field for $d = 30$

Let θ be a root of $x^4 - 12x^2 + 30 = 0$. Then $\psi = -12\theta + \theta^3$, $\xi = 6 - \theta^2$ satisfy $\psi^2 = 30\alpha = 30(6+\xi)$, $\xi^2 = 6$. The field $\mathbb{K} = \mathbb{Q}(\psi) = \mathbb{Q}(\theta)$ has discriminant $276480 = 2^{11}3^35$, integral basis $\{1, \theta, \theta^2, \theta^3\}$, trivial class group, Galois group $\mathbb{D}_4$, a set of fundamental units is

$$\epsilon = -11 + 2\theta + 2\theta^2, \quad \eta = -7 + 2\theta^2, \quad \chi = 31 - 16\theta - 4\theta^2 + 2\theta^3,$$

and $\eta^{-1} = 5 + 2\xi$ is the fundamental unit of the quadratic subfield $\mathbb{Q}(\xi)$. We have the following relevant decompositions into primes:

$$\begin{array}{rcll} 2+\xi & = & p^2\eta^{-1}\chi, & \text{with } p = 2+\theta, \\ 3+\xi & = & -q^2\epsilon\chi^{-1}, & \text{with } q = -3+\theta, \\ 1+\xi & = & r_1, & \text{with } r_1 = 7-\theta^2, \\ 1-\xi & = & -r_2^2\epsilon^{-1}, & \text{with } r_2 = -5+\theta+\theta^2. \end{array}$$

There is a nontrivial $\mathbb{Q}(\xi)$-automorphism σ of $\mathbb{K}$, defined by $\sigma\theta = -\theta$. It acts as follows on the numbers defined above:

$$\sigma\psi = -\psi, \quad \sigma\epsilon = \epsilon^{-1}, \quad \sigma\eta = \eta, \quad \sigma\chi = \chi^{-1},$$

$$\sigma p = p\chi, \quad \sigma q = -q\epsilon\chi^{-1}, \quad \sigma r_1 = r_1, \quad \sigma r_2 = r_2\epsilon^{-1}.$$

From (7) with $1-\xi$ in the right hand side we find, by (6) and $k = 0$, that

$$(30u)^2 - \psi^2\beta^2 = -180(1-\xi) = -p^8q^8r_1r_2^4\epsilon^2,$$

and hence

$$(11)\quad \begin{cases} 30u + \psi\beta = \pm p^a q^b r_1^c r_2^d \epsilon^l \eta^m \chi^n, \\ 30u - \psi\beta = \sigma(30u + \psi\beta) = \pm(-1)^b p^a q^b r_1^c r_2^d \epsilon^{b-d-l} \eta^m \chi^{a-b-n}, \end{cases}$$

for some $a, b, c, d \in \mathbb{Z}_{\geq 0}, l, m, n \in \mathbb{Z}$. It follows at once that $2c = 1$, which is impossible.

From (7) with $1 + \xi$ in the right hand side we find, by (6) and $k = 0$, that

$$(30u)^2 - \psi^2\beta^2 = -180(1 + \xi) = p^8 q^8 r_1^2 r_2^2 \epsilon^3,$$

and hence we find again (11) for some $a, b, c, d \in \mathbb{Z}_{\geq 0}, l, m, n \in \mathbb{Z}$. It follows at once that $a = 4$, $b = 4$, $c = 1$, $d = 1$, $m = 0$. Hence we obtain

$$(12)\qquad 30u + \psi\beta = \pm\gamma\epsilon^l\chi^n,$$

where $\gamma = p^4 q^4 r_1 r_2 = 690 + 162\theta - 120\theta^2 - 6\theta^3$. Notice that we intend to show that there are only the following solutions to (12):

x	u	β	l	n	$\pm$
34	1	ξ	2	0	$-$
34	1	$-\xi$	1	0	$-$
754	5	$-12 + \xi$	2	-1	$+$
754	5	$12 - \xi$	1	1	$+$

Solutions occur in pairs, because $\sigma\gamma = \gamma\epsilon^3$, so if (l, n) is a solution, then so is $(3 - l, -n)$.

7. The quartic field for $d = -15$

Let θ be a root of $x^4 - 2x^3 - 3x^2 + 4x - 2 = 0$. Then $\psi = -17 + 30\theta + 12\theta^2 - 8\theta^3$, $\xi = 2 + \theta - \theta^2$ satisfy $\psi^2 = -15\alpha = -15(9 + 4\xi)$, $\xi^2 = 6$. The field $\mathbb{K} = \mathbb{Q}(\psi) = \mathbb{Q}(\theta)$ has discriminant $-8640 = -2^6 3^3 5$, integral basis $\{1, \theta, \theta^2, \theta^3\}$, trivial class group, Galois group $\mathbb{D}_4$, a set of fundamental units is

$$\epsilon = 1 - 2\theta + 2\theta^2, \quad \eta = -1 + \theta + \theta^2,$$

and $\epsilon^{-1} = 5 + 2\xi$ is the fundamental unit of the quadratic subfield $\mathbb{Q}(\xi)$. We have the following relevant decompositions into primes:

$$\begin{array}{rcll} 2 + \xi & = & p_1 p_2 \epsilon^{-1}, & \text{with } p_1 = 1 - \theta, \quad p_2 = \theta, \\ 3 + \xi & = & q^2 \eta^{-1}, & \text{with } q = -1 + 4\theta + \theta^2 - \theta^3, \\ 1 + \xi & = & -r_1, & \text{with } r_1 = -3 - \theta + \theta^2, \\ 1 - \xi & = & r_2^2 \epsilon \eta^{-1} & \text{with } r_2 = -5 + 3\theta + 2\theta^2 - \theta^3. \end{array}$$

There is a nontrivial $\mathbb{Q}(\xi)$-automorphism σ of $\mathbb{K}$, defined by $\sigma\theta = 1-\theta$. It acts as follows on the numbers defined above:

$$\sigma\psi = -\psi, \quad \sigma\epsilon = \epsilon, \quad \sigma\eta = \eta^{-1},$$

$$\sigma p_1 = p_2, \quad \sigma p_2 = p_1, \quad \sigma q = q\eta^{-1}, \quad \sigma r_1 = r_1, \quad \sigma r_2 = -r_2\eta^{-1}.$$

From (7) with $1-\xi$ in the right hand side we find, by (6), that

$$(15u)^2 - \psi^2\beta^2 = 90(1-\xi) = p_1^{4k+2}p_2^{4k+2}q^8 r_1 r_2^4 \epsilon^{-2k+3}\eta^{-6},$$

and hence we find

$$(13) \quad \begin{cases} 15u + \psi\beta = \pm p_1^a p_2^b q^c r_1^d r_2^e \epsilon^m \eta^n, \\ 15u - \psi\beta = \sigma(15u+\psi\beta) = \pm(-1)^e p_1^b p_2^a q^c r_1^d r_2^e \epsilon^m \eta^{-c-e-n}, \end{cases}$$

for some $a, b, c, d, e \in \mathbb{Z}_{\geq 0}, m, n \in \mathbb{Z}$. It follows at once that $2d = 1$, which is impossible.

From (7) with $1+\xi$ in the right hand side we find, by (6), that

$$(15u)^2 - \psi^2\beta^2 = 90(1+\xi) = -p_1^{4k+2}p_2^{4k+2}q^8 r_1^2 r_2^2 \epsilon^{-2k+2}\eta^{-5},$$

and hence we find again (13) for some $a, b, c, d, e \in \mathbb{Z}_{\geq 0}, m, n \in \mathbb{Z}$. It follows at once that $a+b = 4k+2$, $c = 4$, $d = 1$, $e = 1$, $m = -k+1$. Because of symmetry we may assume $a \leq b$. Note that

$$\pm 30u = p_1^a p_2^b q^4 r_1 r_2 \epsilon^{-k+1}\eta^n - p_1^b p_2^a q^4 r_1 r_2 \epsilon^{-k+1}\eta^{-5-n},$$

and that u is odd (because of (1) and (3)), and $a+b \geq 6$ (because $k \geq 1$). Comparing p_1-adic values, noting that $\mathrm{ord}_{p_1}(30) = 2$, it follows that $a = 2, b = 4k$. Hence we obtain

$$(14) \qquad 15u + \psi\beta = \pm\gamma\pi^k\eta^n,$$

with $\gamma = p_1^2 q^4 r_1 r_2 \epsilon = -81 + 120\theta - 39\theta^2 - 84\theta^3$, and $\pi = p_2^4\epsilon^{-1} = -2+\theta^2$, satisfying $\pi\sigma\pi = 4$. Notice that we intend to show that there are only the following solutions to (14):

x	u	k	β	n	$\pm$
1	1	1	$3-2\xi$	-3	$+$
49	1	2	$-9+2\xi$	-3	$-$
-16439	37	5	$99-38\xi$	-5	$+$

8. Linear forms in real logarithms

In the cases $d = 3, 10, 30$ we need only 'real' arguments. We treat equations (8), (10) and (12) as follows. Write them as

$$du + \psi\beta = \pm\gamma\epsilon^l\zeta^h, \tag{15}$$

where $\zeta = \eta/\chi, h = m$ if $d = 3$, and $\zeta = \chi, h = n$ if $d = 10, 30$. We apply the $\mathbb{Q}(\xi)$-automorphism σ to (15), using $d, u \in \mathbb{Z}, \beta \in \mathbb{Q}(\xi)$, so that $\sigma d = d, \sigma u = u, \sigma\beta = \beta$. On further noting that $\sigma\psi = -\psi, \sigma\epsilon = s\epsilon^{-1}, \sigma\zeta = s\zeta^{-1}$, where $s = 1$ if $d = 3, 30$ and $s = -1$ if $d = 10$, and writing $\delta = \sigma\gamma$, we obtain

$$du - \psi\beta = \pm s^{l+h}\delta\epsilon^{-l}\zeta^{-h}. \tag{16}$$

Adding (15) to (16), using that $l + h$ is always odd in the case $d = 10$ and $s = 1$ in the cases $d = 3, 30$, so that $s^{l+h} = s$, we find

$$\pm\, du = \gamma\epsilon^l\zeta^h + s\delta\epsilon^{-l}\zeta^{-h}, \tag{17}$$

and thus we have eliminated the unknown β.

Now we notice that the quartic field $\mathbb{K}$ is totally real. We choose two embeddings of $\mathbb{K}$ into $\mathbb{R}$, denoting elements in one of these embeddings without primes, and in the other one with primes, such that $0 < \theta < \theta'$. Note that by $\sigma : \theta \to -\theta$ this determines all four embeddings, and also note that now an embedding of $\mathbb{Q}(\xi)$ into $\mathbb{R}$ has been fixed.

We thus have two different manifestations in $\mathbb{R}$ of equation (17), one written again exactly as (17), and the other one being

$$\pm\, du = \gamma'\epsilon'^l\zeta'^h + s\delta'\epsilon'^{-l}\zeta'^{-h}. \tag{18}$$

Hence now we can eliminate the unknown u from (17) and (18), and thus get

$$\gamma\epsilon^l\zeta^h + s\delta\epsilon^{-l}\zeta^{-h} = \gamma'\epsilon'^l\zeta'^h + s\delta'\epsilon'^{-l}\zeta'^{-h}. \tag{19}$$

For convenience we write this four term unit equation as $I + II = III + IV$.

Now an important observation is that $I \times II = s\gamma\delta$ and $III \times IV = s\gamma'\delta'$ are constant. Bilu's original idea is to solve I from the quadratic equation $I^2 - (III + IV)I + \gamma\delta = 0$. We use a somewhat simpler idea, and work directly with (19). Namely, of the pair I, II only one can be large in absolute value, and the same holds for the pair III, IV. So we either have two of the four terms being large and two small, in which case we can apply the theory of linear forms in logarithms, or all four terms are bounded, in which case we can easily determine the solutions by hand.

In each of the cases we look carefully at the signs of I, II, III, IV, and thus determine which one is the largest in absolute value. We find:

case				signs				largest
$d=3$		l odd		$I<0$	$II>0$	$III>0$	$IV>0$	$\|II\|$
$d=3$		l even		$I<0$	$II>0$	$III<0$	$IV<0$	$\|I\|$
$d=10$	$\gamma=\gamma_1$	l odd		$I>0$	$II>0$	$III>0$	$IV<0$	$\|III\|$
$d=10$	$\gamma=\gamma_1$	l even		$I<0$	$II<0$	$III>0$	$IV<0$	$\|IV\|$
$d=10$	$\gamma=\gamma_2$	l odd		$I<0$	$II<0$	$III<0$	$IV>0$	$\|III\|$
$d=10$	$\gamma=\gamma_2$	l even		$I>0$	$II>0$	$III<0$	$IV>0$	$\|IV\|$
$d=30$		l odd	n odd	$I<0$	$II>0$	$III>0$	$IV>0$	$\|II\|$
$d=30$		l odd	n even	$I<0$	$II>0$	$III<0$	$IV<0$	$\|I\|$
$d=30$		l even	n odd	$I>0$	$II<0$	$III>0$	$IV>0$	$\|I\|$
$d=30$		l even	n even	$I>0$	$II<0$	$III<0$	$IV<0$	$\|II\|$

In each case we distinguish four subcases:

subcase 1: $|I|>|II|$ and $|III|>|IV|$,
subcase 2: $|I|>|II|$ and $|III|<|IV|$,
subcase 3: $|I|<|II|$ and $|III|>|IV|$,
subcase 4: $|I|<|II|$ and $|III|<|IV|$.

Note that half of the subcases lead to contradictions, e.g. if $d=3, l$ odd, then $|II|>|I|$, so then only subcases 3 and 4 occur.

Put $c_1=|\gamma\delta|+|\gamma'\delta'|$. In subcase 1 we now have

$$|I-III|=|IV-II|\le|II|+|IV|=\frac{|\gamma\delta|}{|I|}+\frac{|\gamma'\delta'|}{|III|}.$$

Then we find

$$\text{(20)}\qquad \text{if}\quad |I|>|III|\quad\text{then}\quad |III/I-1|\le c_1|I|^{-1}|III|^{-1},$$

$$\text{(21)}\qquad \text{if}\quad |I|<|III|\quad\text{then}\quad |I/III-1|\le c_1|I|^{-1}|III|^{-1}.$$

Analogously, in subcase 2 we find

$$\text{(22)}\qquad \text{if}\quad |I|>|IV|\quad\text{then}\quad |IV/I-1|\le c_1|I|^{-1}|IV|^{-1},$$

$$\text{(23)}\qquad \text{if}\quad |I|<|IV|\quad\text{then}\quad |I/IV-1|\le c_1|I|^{-1}|IV|^{-1}.$$

And in subcase 3 we find

$$\text{(24)}\qquad \text{if}\quad |II|>|III|\quad\text{then}\quad |III/II-1|\le c_1|II|^{-1}|III|^{-1},$$

$$\text{(25)}\qquad \text{if}\quad |II|<|III|\quad\text{then}\quad |II/III-1|\le c_1|II|^{-1}|III|^{-1}.$$

Finally, in subcase 4 we find

$$\text{(26)}\qquad \text{if}\quad |II|>|IV|\quad\text{then}\quad |IV/II-1|\le c_1|II|^{-1}|IV|^{-1},$$

$$\text{(27)}\qquad \text{if}\quad |II|<|IV|\quad\text{then}\quad |II/IV-1|\le c_1|II|^{-1}|IV|^{-1}.$$

The left hand side of each of these inequalities (20) - (27) is of the form $|e^{\Lambda}-1| \leq \cdots$, where Λ is a linear form in logarithms of algebraic numbers, namely

in case (20):	$\Lambda = \log|\gamma'/\gamma| - \Lambda_1$,	in case (24):	$\Lambda = \log|\gamma'/\delta| + \Lambda_2$,
in case (21):	$\Lambda = \log|\gamma/\gamma'| + \Lambda_1$,	in case (25):	$\Lambda = \log|\delta/\gamma'| - \Lambda_2$,
in case (22):	$\Lambda = \log|\delta'/\gamma| - \Lambda_2$,	in case (26):	$\Lambda = \log|\delta'/\gamma| + \Lambda_1$,
in case (23):	$\Lambda = \log|\gamma/\delta'| + \Lambda_2$,	in case (27):	$\Lambda = \log|\gamma/\delta'| - \Lambda_1$,

where $\Lambda_1 = l\log|\epsilon/\epsilon'| + h\log|\zeta/\zeta'|$, $\Lambda_2 = l\log|\epsilon\epsilon'| + h\log|\zeta\zeta'|$. Put $N = \max\{|l|,|h|\}$. The theorem of [BW] implies the existence of an absolute constant C such that

$$|\Lambda| > \exp(-C\log N). \tag{28}$$

We will show that combining this with the appropriate equation from (20) - (27) leads to an absolute upper bound for N. For example, if $d=3$, subcase 1, then l is even, and we have $|I| > |III| > |IV|$. From these inequalities it follows at once that there are only finitely many solutions with $l \geq -4$, and if $l \leq -5$, then $N=-l$, and $c_1|I|^{-1}|III|^{-1} < 0.5$. This last inequality implies $|\Lambda| < 1.39|e^{\Lambda}-1| \leq 1.39c_1|I|^{-1}|III|^{-1}$, so (20) and (28) imply

$$\log|I||III| \leq \log(1.39c_1) + C\log N. \tag{29}$$

Using $|III| > |IV|$ and $N=-l$ we compute constants c_2, c_3' such that

$$\log|I||III| > c_2N - c_3'. \tag{30}$$

In general, for each of the inequalities (20) - (27) we find by (29) and (30), for large enough N, that

$$|\Lambda| < 1.39|e^{\Lambda}-1| < \exp(c_3 - c_2N), \tag{31}$$

with $c_3 = c_3' + \log(1.39c_1)$. Hence we obtain by (28)

$$c_2N < c_3 + C\log N, \tag{32}$$

which at once implies an absolute upper bound for N.

A similar procedure works in all cases. We give some details for each case below. We give in each case a condition to ensure that the right hand side of the appropriate inequality from (20) - (27) is < 0.5, which fails for only finitely many easily determined l,h. Sometimes we have to make a further distinction between $N=|l|$ and $N=|h|$. In the column marked 'inequ.' we indicate which inequality we used to derive $\log|X||Y| > c_2N - c_3'$ for $X = I, II$, $Y = III, IV$. The constant C is computed directly from [BW], noting that we have linear forms in 3 logarithms of algebraic numbers in a field of degree 8. The constant N_0 is the upper bound for N following from (32).

d	γ	subcase	condition	N	inequ.	$C <$	$c_1 <$	$c_2 >$	$c_3 <$	N_0
3		1	$l \leq -5$	$-l$	$\|III\| > \|IV\|$	2.5154×10^{18}	88.182	2.0633	−0.34522	5.5423×10^{19}
3		2	$l \leq -23$	$-l$	$\|III\| < \|IV\|$	2.5154×10^{18}	88.182	2.0633	−0.34522	5.5423×10^{19}
3		3	$l \geq 6$	l	$\|III\| > \|IV\|$	2.5154×10^{18}	88.182	2.0633	2.5725	5.5423×10^{19}
3		4	$l \leq 1$	l	$\|III\| < \|IV\|$	2.5154×10^{18}	88.182	2.0633	2.5725	5.5423×10^{19}
10	γ_1	1	$h \geq 4$	h	$\|I\| > \|II\|$	3.6254×10^{18}	293.94	3.7681	5.4475	4.3507×10^{19}
10	γ_1	2	$h \leq -3$	$-h$	$\|I\| > \|II\|$	3.6254×10^{18}	293.94	3.7681	−3.2202	4.3507×10^{19}
10	γ_1	2	$l \leq -2$	$-l$	$h \leq l/3$	3.6254×10^{18}	293.94	3.6603	−7.9711	4.4818×10^{19}
10	γ_1	3	$h \geq 4$	h	$\|I\| < \|II\|$	3.6254×10^{18}	293.94	3.7681	5.4475	4.3507×10^{19}
10	γ_1	3	$l \geq 3$	l	$h \geq l/3$	3.6254×10^{18}	293.94	3.6603	10.199	4.4818×10^{19}
10	γ_1	4	$h \leq -14$	$-h$	$\|I\| < \|II\|$	3.6254×10^{18}	293.94	3.7681	−3.2202	4.3507×10^{19}
10	γ_2	1	$h \geq 3$	h	$\|I\| > \|II\|$	3.4101×10^{18}	293.94	3.7681	6.7659	4.0867×10^{19}
10	γ_2	2	$h \leq -3$	$-h$	$\|I\| > \|II\|$	3.4101×10^{18}	293.94	3.7681	−4.5386	4.0867×10^{19}
10	γ_2	2	$l \leq -3$	$-l$	$h \leq l/3$	3.4101×10^{18}	293.94	3.6603	−6.5891	4.2098×10^{19}
10	γ_2	3	$h \geq 2$	h	$\|I\| < \|II\|$	3.4101×10^{18}	293.94	3.7681	6.7659	4.0867×10^{19}
10	γ_2	3	$l \geq 2$	l	$h \geq l/3$	3.4101×10^{18}	293.94	3.6603	8.8164	4.2098×10^{19}
10	γ_2	4	$h \leq -12$	$-h$	$\|I\| < \|II\|$	3.4101×10^{18}	293.94	3.7681	−4.5386	4.0867×10^{19}
30		1	$h \leq -3$	$-h$	$\|III\| > \|IV\|$	5.6210×10^{18}	881.82	4.9112	1.1137	5.1959×10^{19}
30		2	$h \leq -3$	$-h$	$\|III\| < \|IV\|$	5.6210×10^{18}	881.82	4.9112	1.1137	5.1959×10^{19}
30		2	$l \leq -2$	$-l$	$h \leq l/13$	5.6210×10^{18}	881.82	4.6380	−5.6328	5.5090×10^{19}
30		3	$h \geq 5$	h	$\|III\| > \|IV\|$	5.6210×10^{18}	881.82	4.9112	1.1137	5.1959×10^{19}
30		3	$l \geq 2$	l	$h \geq l/13$	5.6210×10^{18}	881.82	4.6380	7.8601	5.5090×10^{19}
30		4	$l \leq 5$	h	$\|III\| < \|IV\|$	5.6210×10^{18}	881.82	4.9112	1.1137	5.1959×10^{19}

9. Real reduction

To reduce the upper bound N_0 for N we use computational diophantine approximation techniques, as in previous sections. Let us write the linear form Λ as $\Lambda = \phi_0 + l\phi_1 + h\phi_2$. We take $C = 10^{44}$, which is a bit larger than N_0^2. We introduce the lattice $\Gamma = \{\mathcal{A}\boldsymbol{z} | \boldsymbol{z} \in \mathbb{Z}^2\}$ and the point $\boldsymbol{y}$ given by

$$\mathcal{A} = \begin{pmatrix} 1 & 0 \\ [C\phi_1] & [C\phi_2] \end{pmatrix}, \qquad \boldsymbol{y} = \begin{pmatrix} 0 \\ -[C\phi_0] \end{pmatrix}.$$

Here $[\cdot]$ stands for rounding to an integer. Then we define $\lambda \in \mathbb{Z}$ by

$$\mathcal{A}\begin{pmatrix} l \\ h \end{pmatrix} - \boldsymbol{y} = \begin{pmatrix} l \\ \lambda \end{pmatrix}.$$

We computed ϕ_0, ϕ_1, ϕ_2 to sufficient precision. To 10 decimal places they are:

d	i	ϕ_1	ϕ_2
3	1,4	−0.9938638120	−4.3528545224
3	2,3	−2.8254730309	3.1019926241
10	1,4	−2.9229106733	−2.2122333004
10	2,3	−1.8710556827	4.7641977272
30	1,4	−4.4976592439	−1.8250625868
30	2,3	0.4236678296	−5.2019722206

i	$d = 3$	$d = 10, \gamma = \gamma_1$	$d = 10, \gamma = \gamma_2$	$d = 30$
1	4.2104911458	−8.6512061735	−7.2692085973	−7.1799962291
2	−6.2414274406	1.7262293534	4.7732204299	0.2019943812
3	−5.3744127141	0.8592146269	3.9062057034	1.0690091077
4	5.0775058723	−9.5182209000	−8.1362233238	−6.3129815026

Note that for the 16 different linear forms there are only 6 different lattices.

Using the Euclidean algorithm we can easily compute a lower bound for the distance $d(\Gamma, \boldsymbol{y})$ from $\boldsymbol{y}$ to the nearest lattice point in Γ. Then we have $|\lambda| \geq \sqrt{d(\Gamma, \boldsymbol{y})^2 - N_0^2}$. Further, notice that

$$|\lambda - C\Lambda| \leq |[C\phi_0] - C\phi_0| + |l||[C\phi_1] - C\phi_1| + |h||[C\phi_2] - C\phi_2| \leq 1 + 2N_0,$$

so that

$$|\Lambda| \geq \frac{1}{C}\left(\sqrt{d(\Gamma, \boldsymbol{y})^2 - N_0^2} - (1 + 2N_0)\right).$$

If $d(\Gamma, \boldsymbol{y})$ is large enough, this gives an explicit lower bound for $|\Lambda|$, which together with (31) yields a reduced upper bound for N.

The details for each case are as follows.

d	γ	subcase	$d(\Gamma, y) >$	reduced bound
3		1	7.4269×10^{21}	24
3		2	6.2958×10^{21}	24
3		3	1.1698×10^{22}	25
3		4	6.9060×10^{21}	25
10	γ_1	1	4.6601×10^{21}	15
10	γ_1	2	8.2252×10^{21}	13
10	γ_1	3	7.0485×10^{21}	16
10	γ_1	4	2.7660×10^{21}	12
10	γ_2	1	7.7020×10^{21}	15
10	γ_2	2	1.1844×10^{22}	12
10	γ_2	3	1.1844×10^{22}	16
10	γ_2	4	7.7020×10^{21}	12
30		1	1.8954×10^{22}	10
30		2	3.5283×10^{21}	11
30		3	3.5283×10^{21}	12
30		4	1.8954×10^{22}	10

Finally we checked equation (19) directly for all $N \leq 30$. This revealed only the known solutions, listed already in previous sections. This completes the treatment of the cases $d = 3, 10, 30$.

10. Linear forms in p-adic logarithms

In the case $d = -15$ we need almost only 'p-adic' arguments. We start with equation (14), analogous to the beginning of our treatment in the previous sections, as follows. We apply the $\mathbb{Q}(\xi)$-automorphism σ to (14), using $u \in \mathbb{Z}, \beta \in \mathbb{Q}(\xi)$, so that $\sigma u = u, \sigma\beta = \beta$. On further noting that $\sigma\psi = -\psi, \sigma\pi = 4\pi^{-1}, \sigma\eta = \eta^{-1}$, and writing $\delta = \sigma\gamma$, we obtain

$$-15u - \psi\beta = \pm\delta 4^k \pi^{-k} \eta^{-n}. \tag{33}$$

Adding (14) to (33), we find

$$\mp 15u = \gamma\pi^k\eta^n + \delta 4^k \pi^{-k} \eta^{-n}, \tag{34}$$

and thus we have eliminated the unknown β.

At this point the main difference with the previous sections becomes apparent, since now, due to the fact that π is not a unit, the product of the two factors in the right hand side of (34) is not constant, but is a constant times 4^k. The idea now is that, though this is large in the archimedean sense, it is small in the 2-adic sense, so that we can try to transform the arguments of the previous sections from the real to the 2-adic realm.

It is not difficult to show that the Galois closure of the quartic field $\mathbb{K}$ can be embedded into $\mathbb{Q}_2(\xi)$, so that we can embed $\mathbb{K}$ into the field $\mathbb{Q}_2(\xi)$ in two different ways (remember that ξ is defined by $\xi^2 = 6$). We denote elements in one of these embeddings without primes, and in the other one with primes. Then we have two different manifestations in $\mathbb{Q}_2(\xi)$ of equation (34), one written again exactly as (34), and the other one being

$$\mp 15u = \gamma'\pi'^k\eta'^n + \delta' 4^k \pi'^{-k}\eta'^{-n}. \tag{35}$$

Again we can eliminate the unknown u from (34) and (35), and thus get a four term S-unit equation $I + II = III + IV$, namely

$$\gamma\pi^k\eta^n + \delta 4^k\pi^{-k}\eta^{-n} = \gamma'\pi'^k\eta'^n + \delta' 4^k \pi'^{-k}\eta'^{-n}. \tag{36}$$

For the 2-adic number $a_0+a_1 2+a_2 2^2+\ldots$ we use the notation $0.a_0a_1a_2\cdots$. We choose conjugates as follows:

$$\begin{array}{rcl}
\theta & = & 0.1011000000\ldots + 0.1001010000\ldots\xi, \\
\sigma\theta = 1-\theta & = & 0.0010111111\ldots + 0.1110101111\ldots\xi, \\
\theta' & = & 0.1011000000\ldots + 0.1110101111\ldots\xi, \\
\sigma\theta' = 1-\theta' & = & 0.0010111111\ldots + 0.1001010000\ldots\xi.
\end{array}$$

Then the following is true:

x	$\mathrm{ord}_2(x)$	$\mathrm{ord}_2(\sigma x)$	$\mathrm{ord}_2(x')$	$\mathrm{ord}_2(\sigma x')$
γ	1	0	1	0
π	0	2	0	2
η	0	0	0	0

And if $x \in \mathbb{Q}_2(\xi)$ is written as $x = a + b\xi$ for $a, b \in \mathbb{Q}_2$, then $x' = a - b\xi$, so that $x - x' = 2b\xi$, and $\mathrm{ord}_2(x - x') = \mathrm{ord}_2(b) + \frac{3}{2}$. With $x = II, x' = IV$ it follows that $\mathrm{ord}_2(I - III) = \mathrm{ord}_2(IV - II) \geq 2k + \frac{3}{2}$, hence

$$\mathrm{ord}_2(I/III - 1) \geq 2k + k_0, \tag{37}$$

where $k_0 = \frac{3}{2} - \mathrm{ord}_2(\gamma') = \frac{1}{2}$. Notice that here we have a linear form in 2-adic logarithms in disguise. It will be made explicit later on.

Now we apply the theory of linear forms in p-adic logarithms of algebraic numbers. In fact, using

$$I/III = \frac{\gamma}{\gamma'}\left(\frac{\pi}{\pi'}\right)^k\left(\frac{\eta}{\eta'}\right)^n,$$

Yu's theorem [Y] implies

$$\mathrm{ord}_2(I/III - 1) < 8.6078 \times 10^{27}\log(8\max\{k, |n|\}) \tag{38}$$

(we omit details, but note that we used the result Yu mentions in his Section 0.1, on page 242 of [Y]).

To obtain an upper bound for the variables k and $|n|$ from (37) and (38), we also need to study the complex embeddings of $\mathbb{K}$. So now we interpret equation (36) as an equation in complex numbers, where we choose conjugates as follows:

$$\begin{array}{rclrcl} \theta & = & 2.6678\ldots, & \sigma\theta = 1-\theta & = & -1.6678\ldots, \\ \theta' & = & \frac{1}{2}+0.4466\ldots i, & \sigma\theta' = \overline{\theta'} = 1-\theta' & = & \frac{1}{2}-0.4466\ldots i. \end{array}$$

So we have $I, II \in \mathbb{R}$, and $III, IV \in \mathbb{C}$ are complex conjugates. Using $|\pi'| = 2, |\eta'| = 1$ we find

$$\left| I - \frac{90(\sqrt{6}-1)}{I} 4^k \right| = |I + II| = |III + IV| \leq 2|III| < 35.240 \cdot 2^k,$$

since $\gamma\delta = -90(\sqrt{6}-1)$. This inequality implies $3.3781 \cdot 2^k < |I| < 38.618 \cdot 2^k$, and we obtain the inequality

$$\log(3.3781) < \log|\gamma| + k \log \pi/2 + n \log \eta < \log(38.618).$$

From $\log \pi/2 = 0.93\ldots, \log \eta = 2.17\ldots, \log(-\gamma) = 7.39\ldots$ we immediately obtain that if $k \geq 6$ then $-k \leq n < 0$, hence $\max\{k, |n|\} = k$.

Inequalities (37) and (38) thus immediately imply

$$(39) \qquad |n| \leq k < 3.0109 \times 10^{29}.$$

11. p-adic reduction

In this final section we reduce the bound (39) by making use of p-adic computational diophantine approximation techniques, applied to inequality (37). Put $\Lambda' = \log_2 I/III$. If $k \geq 1$ then (37) implies

$$(40) \qquad \mathrm{ord}_2(\Lambda') = \mathrm{ord}_2(I/III - 1) \geq 2k + \tfrac{1}{2}.$$

Notice that $\Lambda' = \log_2 \gamma/\gamma' + k \log_2 \pi/\pi' + n \log_2 \eta/\eta'$, where we computed

$$\log_2 \gamma/\gamma' = 0.0100110111\ldots\xi, \quad \log_2 \pi/\pi' = 0.0010001100\ldots\xi,$$

$$\log_2 \eta/\eta' = 0.0111001001\ldots\xi.$$

So if we put $\Lambda = \Lambda'/\log_2 \eta/\eta' = \phi_0 + k\phi_1 + n$ then it happens that ϕ_0, ϕ_1 are in $\mathbb{Q}_2$ and are integral, in fact

$$\phi_0 = 0.1111111101\ldots, \quad \phi_1 = 0.0111001111\ldots.$$

And we obtain from (40) that

$$(41) \qquad \mathrm{ord}_2(\Lambda) = \mathrm{ord}_2(\Lambda') - \frac{3}{2} \geq 2k - 1.$$

For a positive integer μ, let $\phi_*^{(\mu)}$ be the unique rational integer satisfying $0 \le \phi_*^{(\mu)} < 2^\mu$ and $\mathrm{ord}_2(\phi_* - \phi_*^{(\mu)}) \ge \mu$. Consider the lattice $\Gamma = \{\mathcal{A}z | z \in \mathbb{Z}^2\}$ and the point y given by

$$\mathcal{A} = \begin{pmatrix} 1 & 0 \\ \phi_1^{(\mu)} & 2^\mu \end{pmatrix}, \qquad y = \begin{pmatrix} 0 \\ -\phi_0^{(\mu)} \end{pmatrix}.$$

Then it follows that $\mathrm{ord}_2(\Lambda) \ge \mu$ if and only if

$$\begin{pmatrix} k \\ -n \end{pmatrix} = \mathcal{A} \begin{pmatrix} k \\ z \end{pmatrix} - y$$

for a $z \in \mathbb{Z}$. So the distance $d(\Gamma, y)$ from y to the lattice Γ can be at most $\sqrt{k^2 + n^2}$, which is bounded by (39). On the other hand, for each μ this distance can be computed easily by the Euclidean algorithm. In fact, we can reach a contradiction when we choose μ so that 2^μ is of the magnitude of the square of the upper bound.

We took $\mu = 204$, and computed $\sqrt{2}k \ge \sqrt{k^2 + n^2} \ge d(\Gamma, y) > 2.0409 \times 10^{30}$. This contradicts (39), and it follows that $\mathrm{ord}_2(\Lambda) \le \mu - 1 = 203$, which with (41) yields a reduced upper bound, namely $k \le 102$.

Next we took $\mu = 18$, and computed $\sqrt{2}k \ge d(\Gamma, y) > 153.05$, which contradicts $k \le 102$. Hence the upper bound reduces further to $k \le 9$.

Finally it's trivial to determine the solutions with $k \le 9$, and our proof is complete.

REFERENCES

[B] YU. BILU, "Solving superelliptic Diophantine equations by the method of Gelfond-Baker", Preprint 94-09, Mathématiques Stochastiques, Univ. Bordeaux 2 [1994].

[BH] YU. BILU AND G. HANROT, "Solving superelliptic Diophantine equations by Baker's method", *Compos. Math.*, to appear.

[BW] A. BAKER AND G. WÜSTHOLZ, "Logarithmic forms and group varieties", *J. reine angew. Math.* **442** [1993], 19–62.

[D] S. DAVID, *Minorations de formes linéaires de logarithmes elliptiques*, Mém. Soc. Math. de France, Num. 62 [1995].

[GPZ1] J. GEBEL, A. PETHŐ AND H.G. ZIMMER, "Computing integral points on elliptic curves", *Acta Arith.* **68** [1994], 171–192.

[GPZ2] J. GEBEL, A. PETHŐ AND H.G. ZIMMER, "Computing S-integral points on elliptic curves", in: H. COHEN (ED.), *Algorithmic Number Theory*, Proceedings ANTS-II, Lecture Notes in Computer Science VOl. 1122, Springer-Verlag, Berlin [1996], pp. 157–171.

[RU] G. REMOND AND F. URFELS, "Approximation diophantienne de logarithmes elliptiques p-adiques", *J. Number Th.* **57** [1996], 133–169.

[S] N.P. SMART, "S-integral points on elliptic curves", *Math. Proc. Cambridge Phil. Soc.* **116** [1994], 391–399.

[ST] R.J. STROEKER AND N. TZANAKIS, "Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms", *Acta Arith.* **67** [1994], 177-196.

[SW1] R.J. STROEKER AND B.M.M. DE WEGER, "On a quartic diophantine equation", *Proc. Edinburgh Math. Soc.* **39** [1996], 97–115.

[T] N. TZANAKIS, "Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations", *Acta Arith.* **75** [1996], 165–190.

[TW1] N. TZANAKIS AND B.M.M. DE WEGER, "On the practical solution of the Thue equation", *J. Number Th.* **31** [1989], 99-132.

[TW2] N. TZANAKIS AND B.M.M. DE WEGER, "How to explicitly solve a Thue-Mahler equation", *Compos. Math.* **84** [1992], 223-288.

[Y] K.R. YU, "Linear forms in p-adic logarithms III", *Compos. Math.* **91** [1994], 241-276.

Benjamin M.M. DE WEGER
Sportsingel 30
2924 XN Krimpen aan den IJssel
The Netherlands
e-mail: deweger@X54all.nl