Solving Elliptic Diophantine Equations Avoiding Thue Equations and Elliptic Logarithms

Benjamin M. M. de Weger

CONTENTS

This research was supported by the Netherlands Mathematical Research Foundation SWON with financial aid from the Netherlands Organization for Scientific Research NWO.

We determine the solutions in integers of the equation $y^2 = (x + p)(x^2 + p^2)$ for p = 167, 223, 337, 1201. The method used was suggested to us by Yu. Bilu, and is shown to be in some cases more efficient than other general purpose methods for solving such equations, namely the elliptic logarithms method and the use of Thue equations.

1. INTRODUCTION

In this paper we study, as typical examples from the class of elliptic equations, for a few given primes p, the diophantine equation

$$y^2 = (x+p)(x^2+p^2) \tag{1–1}$$

in $x, y \in \mathbb{Z}$. The elliptic curves defined by these equations have been studied by Stroeker and Top [1994], who proved inter alia upper bounds for the ranks of these curves. In the cases $p = 2$ and $p \equiv \pm 3 \pmod 8$ they showed that the rank is 0, so that the only solution of equation (1–1) is $(x, y) = (-p, 0)$, and in the case $p = 337$ (with rank 3) all the solutions of equation (1–1) have been determined by Stroeker and Tzanakis [1994]. The results of [Stroeker and Top 1994] on the Selmer groups and ranks of (1–1) have been generalized by Schmitt [1997] to composite p.

In the present paper we will solve (1–1) for the cases $p = 167$, $p = 223$, $p = 337$ and $p = 1201$, thus redoing and extending the work of Stroeker and Tzanakis, but the method we use differs from theirs. Notice that in these cases the ranks of the elliptic curves are 1, 1, 3, and 3 respectively; see [Stroeker and Top 1994]. We will prove:

1058-6458/1998 $0.50 per page

Theorem 1. *The diophantine equation*

$$y^2 = (x+167)(x^2+167^2)$$

has only the solution $(x,y) = (-167,0)$.

Theorem 2. *The diophantine equation*

$$y^2 = (x+223)(x^2+223^2)$$

has only the solution $(x,y) = (-223,0)$.

Theorem 3 [Stroeker and Tzanakis 1994]. *The diophantine equation*

$$y^2 = (x+337)(x^2+337^2)$$

has only these solutions:

x	y
-337	0
-287	± 3130
2113	± 105910
56784	± 13571615

Theorem 4. *The diophantine equation*

$$y^2 = (x+1201)(x^2+1201^2)$$

has only these solutions:

x	y
-1201	0
599	± 56940
1999	± 131920
58849	± 14424010

Three methods of a more or less general nature exist for solving elliptic diophantine equations, which we will call the "elliptic logarithms method", the "Thue approach", and the "alternative approach". The two latter methods use linear forms in logarithms of algebraic numbers, all three methods lead to rather large upper bounds, that are subsequently reduced by computational diophantine approximation techniques.

The method of elliptic logarithms was developed independently by Stroeker and Tzanakis [1994], by Gebel, Pethő and Zimmer [Gebel et al. 1994], and by Smart [1994]. It was used by Stroeker and Tzanakis for solving equation (1–1) in the case $p = 337$. It is applicable in general, if one has explicit knowledge of a full set of generators for the group of rational points on the curve, modulo torsion. Algorithms for finding such generators can be found in [Cremona 1992; Gebel and Zimmer 1994], but are not guaranteed to produce an answer, and sometimes rely on the Birch–Swinnerton-Dyer Conjecture. Cremona has implemented his ideas in a program called `mwrank`, and the computer algebra system `Simath` contains an implementation of the algorithm of [Gebel and Zimmer 1994]. I am grateful to the referee for pointing out to me that the `Simath` system could verify our results for $p = 223$, 337 and 1201, but not for $p = 167$, due to the large height of the generator of the Mordell–Weil group in this (rank 1) case.

The Thue approach is the most classical; examples in the literature are [Ellison et al. 1972; Tzanakis and de Weger 1989]. Several factorizations over appropriate number fields, where one sometimes has to distinguish between many cases, lead to a finite number of Thue equations, and each Thue equation leads to a finite number of three-term unit equations. These can be solved in practice, if in certain fields the generators of unit groups and decompositions into prime ideals can be found. Algorithms for such problems have been developed by many mathematicians; see, for example, [Pohst and Zassenhaus 1989; Cohen 1993].

The alternative approach is the most recent to have been applied in practice. It was used in [Mignotte and Pethő 1995]; a general description of its application to superelliptic equations is given by Bilu [1994]. The method (including a p-adic variant) was also used in [de Weger 1997]. In this method one does factorizations in a somewhat different way than in the Thue approach, also leading to a subdivision in several cases, but ending in a number of four-term unit equations with special properties. The route to this unit equation seems to be shorter in general than the Thue approach requires for reaching the three-term unit equations, the fields one encounters usually have more nonreal embeddings into $\mathbb{C}$ and hence are easier to treat, and also it is our impression that the number of cases to be distinguished is in general less than the Thue approach leads to, at least in the few cases we studied in some detail. However, in the alternative approach it might easily happen that one has to factor over larger degree fields, which means that one faces larger unit ranks, and more complicated fields.

We feel that it is not possible to give a general statement on the superiority of one method over any other. This will depend very much on the particular elliptic equation one wants to solve. For example, in [Stroeker and de Weger 1994] it is shown that the elliptic logarithms method may succeed when the Thue approach fails (certainly also the alternative approach will fail there). The choice of examples $p = 167$ and $p = 223$ in this paper is motivated by the fact that equation (1–1) is more difficult to solve by the elliptic logarithms method than by the Thue and alternative approaches. This is because the group of rational points of the elliptic curve modulo torsion, which has rank 1 in these cases, has a generator of extremely large height [Stroeker and Top 1994], whereas the generators of the unit groups occurring in the Thue and alternative approaches are much easier to determine. Further, we chose the cases $p = 337$ and $p = 1201$ as examples because they are the smallest two primes for which the rank of the elliptic curve is 3, and because in these cases the Thue approach seems more complicated than the alternative approach. However, note that in these two cases the elliptic logarithms method of [Stroeker and Tzanakis 1994] is to be preferred.

Since generators of the group of rational points of the elliptic curve modulo torsion are known for the cases $p = 167$, 223 and 1201 [Stroeker and Top 1994], the elliptic logarithms method should be very efficient in solving (1–1), just like the situation turned out to be in [Stroeker and Tzanakis 1994] for the case $p = 337$. We did not try this out. Our point here is that especially in the cases $p = 167$ and $p = 223$ these generators were hard to find, and that therefore the Thue or alternative approaches are to be preferred. Further, our point with the cases $p = 337$ and $p = 1201$ is that the alternative approach is superior to the Thue approach.

We remark that our equation (1–1) is only an example, but that the alternative method works in principle for any equation of the type $y^n = f(x)$, with $n \geq 2$, and f a polynomial with integral coefficients and with at least three distinct linear factors over $\mathbb{C}$. In practice it works whenever the fields one encounters are not too complicated, i.e. when n is not too large, the polynomial f has enough factors of low degree, and fundamental units can be found.

2. SOME WORDS ON THE THUE APPROACH

Throughout this paper, p is a fixed prime number congruent to $\pm 1 \pmod 8$.

Although we intend to prove Theorems 1 to 4 by the alternative approach, we will give some details of the Thue approach too, so that we can indicate how easy or difficult this approach might be.

Let D be the squarefree part of $x + p$. By (1–1), it is also the squarefree part of $x^2 + p^2$. Then

$$D \mid (x^2 + p^2) - (x - p)(x + p) = 2p^2,$$

so $D \in \{1, 2, p, 2p\}$. Note that $x + p > 0$ unless $(x, y) = (-p, 0)$. There exist $U, V \in \mathbb{Z}$ such that

$$x + p = DU^2, \quad x^2 + p^2 = DV^2. \qquad (2\text{–}1)$$

The Case D = 1

We start with the case $D = 1$. If $p \mid x$ then $p \mid V$, hence (2–1) implies $(x/p)^2 + 1 = (V/p)^2$ in integers x/p, V/p, from which it follows that $x = 0$, $V = p$. This contradicts $x + p = U^2$. Hence $(x, p) = 1$, and by $x^2 + p^2 = V^2$ there exist $m, n \in \mathbb{Z}$ with $(m, n) = 1$ and $m > n > 0$ such that

$$x = \pm 2mn, \quad p = m^2 - n^2, \quad V = m^2 + n^2.$$

Since p is prime this implies that $m - n = 1$ and $m + n = p$; hence

$$x = \pm \tfrac{1}{2}(p^2 - 1), \quad V = \tfrac{1}{2}(p^2 + 1),$$

k	p
3	337
20	3493720040136817
23	691738922446276321
36	6195980350983582340001417521
99	10515898470487430435963999984709018013664104902926438406050690509523838430417

TABLE 1. Cases where solutions with $D = 1$ exist.

from which we derive by $U^2 = x + p$ that

$$U^2 = \tfrac{1}{2}(p+1)^2 - 1 \quad \text{or} \quad U^2 = -\tfrac{1}{2}(p-1)^2 + 1.$$

It is immediate that the first case holds, and clearly this can happen only when $p \equiv 1 \pmod 8$. The theory of Pell equations tells us that

$$p = \frac{1}{\sqrt{2}}\big((1+\sqrt{2})^{2k+1} - (1-\sqrt{2})^{2k+1}\big) - 1$$

for some $k \in \mathbb{Z}$, $k \geq 0$. Given p, it is easy to determine whether it is of the above form. In fact, the above expression on the right hand side yields a prime number for only a few $k \leq 100$, listed in Table 1 (we used the `isprime` functions of Maple V.3 and Pari 1.38 as primality tests).

For our favourite p's thus only $p = 337$ admits solutions of (1–1) with $D = 1$, namely $(x, y) = (56784, \pm 13571615)$. Note that no $p \leq 3.57 \times 10^{77}$ other than those in Table 1 admit solutions of (1–1) with $D = 1$.

This concludes our treatment of the case $D = 1$.

The Case D = 2

We write the second equation of (2–1) as $p^2 - 2V^2 = -x^2$, and factor it over $\mathbb{Q}(\sqrt{2})$. Standard arguments yield that we may write

$$p + V\sqrt{2} = (1+\sqrt{2})p^a(A + B\sqrt{2})^2$$

for an $a \in \{0, 1\}$, and with unknowns $A, B \in \mathbb{Z}$. Comparing coefficients we find

$$p^{1-a} = A^2 + 4AB + 2B^2 = (A+2B)^2 - 2B^2, \tag{2–2}$$

and taking norms we find $-x^2 = -p^{2a}(A^2 - 2B^2)^2$, so that by the first equation of (2–1)

$$2U^2 - p = x = \pm p^a(A^2 - 2B^2). \tag{2–3}$$

If $a = 0$ we add (2–2) to (2–3). If in (2–3) the $+$ holds, we find $U^2 = A(A+2B)$. Equation (2–2) implies that A and B are coprime and that A is odd. Hence A and $A + 2B$ are coprime, and there must exist $E, F \in \mathbb{Z}$ such that $A = F^2$ and $A+2B = E^2$. We substitute this into equation (2–2), and thus obtain a Thue equation

$$E^4 + 2E^2F^2 - F^4 = 2p. \tag{2–4}$$

Notice that $B = \frac{1}{2}(E^2 - F^2)$, and this is even. So (2–2) shows that $p \equiv 1 \pmod 8$.

If in (2–3) the $-$ holds, we find $U^2 = 2(A+B)B$. If $p \equiv 1 \pmod 8$ then B is even, and we find $A + B = E^2$ and $B = 2F^2$, leading by (2–2) to the Thue equation

$$E^4 + 4E^2F^2 - 4F^4 = p. \tag{2–5}$$

If $p \equiv -1 \pmod 8$ then B is odd, and we find $A + B = 2F^2$ and $B = E^2$, leading by (2–2) to the Thue equation

$$E^4 - 4E^2F^2 - 4F^4 = -p. \tag{2–6}$$

If $a = 1$ then it follows that $p \mid U$, so let us write $U = pU_1$. Then (2–3) yields

$$2pU_1^2 - 1 = \frac{x}{p} = \pm(A^2 - 2B^2). \tag{2–7}$$

We add (2–2) to (2–7), and if in (2–7) the $+$ holds, we find $pU_1^2 = A(A + 2B)$. Now note that A is odd, hence so is U_1. If $p \equiv -1 \pmod 8$ then (2–7) is impossible $\pmod 8$, hence $p \equiv 1 \pmod 8$. In the case $p \mid A$ we find $A = pF^2$, $A + 2B = E^2$, leading by (2–2) to the Thue equation

$$E^4 + 2pE^2F^2 - p^2F^4 = 2. \tag{2–8}$$

And in the case $p \mid A+2B$ we find $A = E^2$, $A + 2B = pF^2$, leading by (2–2) to the Thue equation

$$E^4 - 2pE^2F^2 - p^2F^4 = -2. \tag{2–9}$$

If in (2–7) the $-$ holds, we find $pU_1^2 = 2(A+B)B$. Now note that A is odd, and U_1 and B are even. If $p \mid A+B$ then (2–7) is impossible $\pmod p$, hence $p \mid B$, and we find $A + B = E^2$ and $B = 2pF^2$, leading by (2–2) to the Thue equation

$$E^4 + 4pE^2F^2 - 4p^2F^4 = 1. \tag{2–10}$$

So we end up with a number of quartic Thue equations (2–4), (2–5), (2–6), (2–8), (2–9), (2–10), which one can try to solve explicitly by the method described in [Tzanakis and de Weger 1989].

The Cases D = p **and** D = 2p

In the cases $D = p$ and $D = 2p$ we write $D = pD_1$, $x = pz$, $V = pW$, and find from (2–1)

$$z + 1 = D_1U^2, \quad z^2 + 1 = D_1pW^2. \tag{2–11}$$

Now -1 is a quadratic residue $\pmod p$, so this shows that $p \equiv 1 \pmod 8$, i.e. these cases do not occur when $p \equiv -1 \pmod 8$. It is easiest to factor the second equation of (2–11) over $\mathbb{Q}(i)$. Let $a_0, b_0 \in \mathbb{Z}$ be such that $a_0 > b_0 > 0$ and $p = a_0^2 + b_0^2$. A prime dividing both $z + i$ and $z - i$ must be $1 + i$, so we find that there are $a, b, c, d \in \{0, 1\}$ and $A, B \in \mathbb{Z}$ such that

$$z + i = i^a(1+i)^b(a_0 + b_0i)^c(a_0 - b_0i)^d(A + Bi)^2.$$

Taking the norm we find

$$D_1pW^2 = z^2 + 1 = 2^bp^{c+d}(A^2 + B^2)^2,$$

and it follows that $2^b = D_1$ and $(c, d) = (1, 0)$ or $(0, 1)$. We write

$$i^a(1+i)^b(a_0 + b_0i)^c(a_0 - b_0)^d = r + si,$$

so a priori we have eight cases: $(r, s) = (a_0, \pm b_0)$, $(\pm b_0, a_0)$, $(a_0 \pm b_0, a_0 \mp b_0)$, $(-a_0 \pm b_0, a_0 \pm b_0)$. We always have $r^2 + s^2 = D_1p$.

So we find

$$z + i = (r + si)(A + Bi)^2$$

for unknown $A, B \in \mathbb{Z}$, and comparing imaginary parts leads to

$$1 = sA^2 + 2rAB - sB^2. \tag{2–12}$$

Further, $W^2 = (A^2 + B^2)^2$, so we find

$$\begin{aligned} z^2 &= D_1pW^2 - 1^2 \\ &= (r^2+s^2)(A^2+B^2)^2 - (sA^2+2rAB-sB^2)^2 \\ &= (rA^2 - 2sAB - rB^2)^2, \end{aligned}$$

hence

$$D_1U^2 - 1 = z = \pm(rA^2 - 2sAB - rB^2). \tag{2–13}$$

We add (2–12) to (2–13), and in the case of $+$ in equation (2–13) we obtain

$$\begin{aligned} D_1U^2 &= (r+s)A^2 + 2(r-s)AB - (r+s)B^2 \\ &= \frac{1}{r+s}\big(((r+s)A + (r-s)B)^2 - 2D_1pB^2\big). \end{aligned} \tag{2–14}$$

In the left and right-hand sides there are three quadratic terms here, and there are three ways of putting two of them on one side of the equality sign. Hence we can factor in three ways, namely over $\mathbb{Q}\big(\sqrt{(2/D_1)p}\big)$, over $\mathbb{Q}(D_1(r+s))$, or over $\mathbb{Q}(-2p(r+s))$. Any of these factorizations will yield quadratic form expressions for A and B, whose substitution into (2–12) gives a few Thue equations, difficult to describe in general but easy to find for each particular value of p.

In the case of $-$ in equation (2–13) we obtain

$$\begin{aligned} D_1U^2 &= (s-r)A^2 + 2(r+s)AB - (s-r)B^2 \\ &= \frac{1}{s-r}\big(((s-r)A + (r+s)B)^2 - 2D_1pB^2\big), \end{aligned} \tag{2–15}$$

which again can be factored in three ways, namely over $\mathbb{Q}\big(\sqrt{(2/D_1)p}\big)$, over $\mathbb{Q}(D_1(s-r))$, or over $\mathbb{Q}(-2p(s-r))$. As above this leads to a few Thue equations.

The quartic Thue equations thus found can in principle be solved following the method outlined in [Tzanakis and de Weger 1989].

Some Details for p = 167, 223, 337, 1201

When $p = 167$ or $p = 223$ we only have to look at the Thue equations (2–6) and (2–10). The only bottlenecks in the Thue approach are the determination of fundamental units in the quartic field associated to the binary form of the Thue equation, and the determination of the primes in this field lying above the primes in the constant term of the Thue equation. In the case of equation (2–6) we have for each p the same quartic field, namely the one generated by a root of x^4-4x^2-4, which is an easy field, of discriminant only -2^{10}.

In the case of equation (2–10) we have for $p = 167$ a quartic field with discriminant $-2^{10}167^2$, generated by a root θ of $x^4+334x^2-27889$. The class number is 2, the regulator is $135.05459\ldots$, and fundamental units are $\frac{1}{167}\theta^2$ and one with coefficients over 30 digits long. This is a bit awesome, but still workable. For $p = 223$ the situation with equation (2–10) is much better, mainly because of the large class number, which keeps the fundamental units small (notice that the class group itself is irrelevant to solving Thue equations with constant term equal to 1). Indeed, we have a quartic field with discriminant $-2^{10}223^2$, generated by a root θ of $x^4+446x^2-49729$. The class number is 20, the regulator is $14.81172\ldots$, and fundamental units are $\frac{1}{223}\theta^2$ and $1903-198\theta+\frac{788}{223}\theta^2-\frac{82}{223}\theta^3$, which is very well workable.

These remarks show that the Thue approach is practically possible for $p = 167$ and $p = 223$, although a bit more difficult for $p = 167$. We will not work out details, as it is a matter of routine only, following the arguments outlined in [Tzanakis and de Weger 1989].

When $p = 337$ or $p = 1201$ we have to solve the equations (2–4), (2–5), (2–8), (2–9) and (2–10), and to work further with equations (2–14) and (2–15). Equations (2–4) and (2–5) are easy, as they give rise to the quartic field of discriminant -2^{10} studied above. Equations (2–8) and (2–9) are trivial in the cases $p = 337$ and $p = 1201$, because in the quartic fields the only prime ideal of norm 2 is nonprincipal, so there exist no algebraic integers with norm 2 in these fields. Equation (2–10) is still doable, although for $p = 1201$ we get a fundamental unit with about 10 digit coefficients.

The real problems start when we treat (2–14) and (2–15). For example, the solution $x = 58849$ of (1–1) with $p = 1201$ (here $a_0 = 25$, $b_0 = 24$) comes from the solution $A = 1$, $B = 0$, $U = 5$ of equation (2–14) in the case $(r,s) = (49,1)$. This equation reads $25A^2 + 48AB - 25B^2 = U^2$, and the left-hand side factors over $\mathbb{Q}(\sqrt{1201})$. This quadratic field is quite unpleasant, since its fundamental unit is

$$\omega = 241828415471370634067447 + 14370833712188846154770\,\frac{1+\sqrt{1201}}{2}. \qquad (2\text{–}16)$$

The above solution comes from the factorization

$$25A+24B+B\sqrt{1201} = \left(E+F\frac{1+\sqrt{1201}}{2}\right)^2,$$

which gives $A = \frac{1}{25}E^2-\frac{23}{25}EF+\frac{577}{50}F^2$ and $B = EF+\frac{1}{2}F^2$. This substituted into (2–12) yields the Thue equation

$$2E^4+4808E^3F-109288E^2F^2+1329508EF^3+872977F^4 = 1250,$$

which obviously has the solution $E = 5, F = 0$. The quartic field related to the binary form of this equation is generated by a root of x^4-98x^2-1, and so the Thue equation is relatively easy to solve.

But we must also study, among others, the case of

$$25A+24B+B\sqrt{1201} = \omega\left(E+F\frac{1+\sqrt{1201}}{2}\right)^2,$$

for ω as in (2–16), which leads as above to

$$A = \frac{765638277811989032875 92}{25}E^2 + \frac{2729917496091439647751009}{25}EF + \frac{4866821416481078162030620 9}{50}F^2$$

and

$$B = 7185416856094423077385E^2 + 25619924918355948022221 7EF + \frac{4567449362840213326653217}{2}F^2.$$

This, substituted into (2–12), yields the horrible Thue equation shown at the top of the next page — and this is only one of a number of such equations to be solved.

$$\begin{aligned}&2642887061864282492960123394168352279287578443678e^4\\&\quad + 188466638606297413117337095284836231611892932710912e^3 f\\&\quad + 503989666926515460700422775243028845013548059780686 8e^2 f^2\\&\quad + 598999226947326603398706137537377284503248668785182 12 e f^3\\&\quad + 266969814136940895435179041059948854619355246603967953 f^4 = 1250,\end{aligned}$$

A typical Thue equation occurring for $p = 1201$ (see end of preceding page).

We can try to avoid such complicated equations by writing (2–14) as $(25A + 24B)^2 = 25U^2 + 1201B^2$, and factoring over $\mathbb{Q}(\sqrt{-1201})$, which is a much nicer field from the point of view of units. Let's see what this leads to. The field $\mathbb{Q}(\sqrt{-1201})$ has a cyclic class group of order 16, the prime 2 ramifies, and the prime 5 splits. From this it's easy to conclude that there is an integral ideal $\mathfrak{a}$ such that $(5U + B\sqrt{-1201}) = (5)^a\mathfrak{a}^2$, where $a \in \{0, 1\}$. If $\mathfrak{p}$ is the ideal of norm 2, which is nonprincipal, then either $\mathfrak{a}$ or $\mathfrak{pa}$ is principal, written as $(E + F\sqrt{-1201})$, because $\mathfrak{a}^2$ and $\mathfrak{p}^2$ are principal. From this it follows that $U = \frac{d}{5}(E^2 - 1201F^2)$, $B = 2dEF$, and $A = \frac{d}{25}(E^2 \pm 48EF + 1201F^2)$, where $d \in \{1, \frac{1}{2}, 5, \frac{5}{2}\}$. We substitute this into $A^2 + 98AB - B^2 = 1$, and thus find the Thue equations

$$E^4 \pm 4804E^3F - 232944E^2F^2 \pm 5769604EF^3 + 1442401F^4 = 25, 100, 625, 2500.$$

The quartic field we meet here is generated by a root of $x^4 - 98x^2 - 1$, and is friendly enough to admit an efficient solution. However, we have treated only one case of (r, s), so that the number of Thue equations to be solved will be much larger, although probably not as large as when factoring over $\mathbb{Q}(\sqrt{1201})$.

Our conclusion is that the Thue approach is efficient for $p = 167$ and $p = 223$, and, when factoring in the right way, might be doable for $p = 337$ and $p = 1201$, although a large number of cases have to be distinguished.

3. THE ALTERNATIVE APPROACH

Deriving a Four-Term Unit Equation

We start off as in the Thue approach, so our starting point now is the system (2–1) of Section 2. We have seen that we only have to look at the cases $D = 2, p, 2p$, and if $p \equiv -1 \pmod 8$ we may even restrict ourselves to $D = 2$.

From now on we will concentrate only on our four favourite values for p, namely 167, 223, 337 and 1201. However, we stress that for any reasonable value of p one should be able to carry out the method as easily as in the cases worked out below.

We factor the quadratic equation in (2–1) over $\mathbb{Q}(i)$. Let δ be the squarefree part of $x + pi$. We can write

$$x + pi = \delta\kappa^2$$

for an algebraic integer $\kappa \in \mathbb{Q}(i)$. If π is a prime element in $\mathbb{Q}(i)$ dividing δ but not D, then it divides also $x - pi$, hence it must divide $(x + pi) - (x - pi) = 2pi$. This shows that we can take

$$\delta = i^a(1 + i)^b(\alpha + \beta i)^c(\alpha - \beta i)^d$$

for $a, b, c, d \in \{0, 1\}$, where we take

$$\begin{array}{lll}\alpha = p, & \beta = d = 0 & \text{if} \quad p = 167 \text{ or } 223,\\ \alpha = 9, & \beta = 16 & \text{if} \quad p = 337,\\ \alpha = 24, & \beta = 25 & \text{if} \quad p = 1201,\end{array}$$

so that $\alpha + \beta i$ is a prime element dividing p. Notice that D is the squarefree part of $N(\delta) = 2^b p^{c+d}$.

We now have the cases given in Table 2. Note that sometimes we took $a = -1$ in stead of $a = 1$, which is not an essential change.

Let's pause for a moment and see what happens to the known solutions, listed in Theorems 1 to 4 in Section 1. For any p there is the solution $x = -p$, which occurs in case II, with $\delta = p - pi$, and $\kappa = i$. For $p = 167$ and $p = 223$ there are no other solutions. For $p = 337$ and $p = 1201$ we give data in Table 3 (neglecting the solution $x = 56784$ for $p = 337$, since that one has $D = 1$).

case	a	b	(c,d)	δ	D
I	$0,-1$	1	$(0,0)$	$1\pm i$	2
II	$0,-1$	1	$\begin{cases}(1,1) & \text{if } p\equiv 1 \pmod 8\\ (1,0) & \text{if } p\equiv -1 \pmod 8\end{cases}$	$p\pm pi$	2
III	0	0	$(1,0),(0,1)$	$\alpha\pm\beta i$	p
IV	±1	0	$(1,0),(0,1)$	$\beta\pm\alpha i$	p
V	$0,-1$	1	$(1,0),(0,1)$	$(\alpha+\beta)\pm(\alpha-\beta)i$	$2p$
VI	$0,-1$	1	$(1,0),(0,1)$	$(\alpha-\beta)\pm(\alpha+\beta)i$	$2p$

TABLE 2. Possibilities for δ.

p	x	case	δ	κ
337	-287	I	$1+i$	$13+12i$
337	2113	I	$1+i$	$37-12i$
1201	599	I	$1-i$	$18+25i$
1201	1999	I	$1-i$	$32+25i$
1201	58849	VI	$-1-49i$	$24+25i$

TABLE 3. Tracing the known solutions.

We continue our general discussion. We eliminate x from $x+p=DU^2$ and $x+pi=\delta\kappa^2$, multiply by D, and thus find

$$Dp(1-i)=(DU)^2-D\delta\kappa^2.$$

We factorize this equation over the field $\mathbb{K}=\mathbb{Q}(\theta)$, where $\theta^2=D\delta$. This is a totally complex quartic field, a quadratic extension of $\mathbb{Q}(i)$. Let ε be a fundamental unit in $\mathbb{K}$. Then there exists a finite set of $\gamma\in\mathbb{K}$ such that

$$DU+\theta\kappa=\gamma\varepsilon^a, \tag{3–1}$$

for some $a\in\mathbb{Z}$. In the Appendix to this paper we will determine complete sets of nonassociated γ's for each δ, and we present the necessary data on the number fields $\mathbb{K}$.

Let σ be the nontrivial $\mathbb{Q}(i)$-automorphism of $\mathbb{K}$ that sends θ to $-\theta$. Then

$$\varepsilon\sigma(\varepsilon)=\zeta$$

for a fourth root of unity ζ, so we find from (3–1)

$$DU-\theta\kappa=\sigma(\gamma)\sigma(\varepsilon)^a=\zeta^a\sigma(\gamma)\varepsilon^{-a}. \tag{3–2}$$

Now we apply complex conjugation to (3–1) and (3–2), and obtain

$$DU+\overline{\theta}\overline{\kappa}=\overline{\gamma}\,\overline{\varepsilon}^a, \tag{3–3}$$

$$DU-\overline{\theta}\overline{\kappa}=\overline{\zeta}^a\overline{\sigma(\gamma)}\,\overline{\varepsilon}^{-a}. \tag{3–4}$$

From the four equations (3–1) – (3–4) we eliminate the variables U,κ, which is simply done by noting that in the left-hand sides

$$(3\text{–}1)+(3\text{–}2)=(3\text{–}3)+(3\text{–}4).$$

In the right-hand sides this gives a four-term unit equation:

$$\gamma\varepsilon^a+\zeta^a\sigma(\gamma)\varepsilon^{-a}=\overline{\gamma}\,\overline{\varepsilon}^a+\overline{\zeta}^a\,\overline{\sigma(\gamma)}\,\overline{\varepsilon}^{-a}. \tag{3–5}$$

Here only the variable $a\in\mathbb{Z}$ remains.

Deriving an Upper Bound

We take an embedding of $\mathbb{K}$ into $\mathbb{C}$ such that $|\varepsilon|>1$. Put $a^*\equiv a \pmod 4$ with $a^*\in\{-1,0,1,2\}$. We rewrite equation (3–5) as

$$\gamma\varepsilon^a-\overline{\gamma}\,\overline{\varepsilon}^a=\overline{\zeta}^{a^*}\overline{\sigma(\gamma)}\,\overline{\varepsilon}^{-a}-\zeta^{a^*}\sigma(\gamma)\,\varepsilon^{-a},$$

and deduce from this, for the case $a\geq 0$ the inequality

$$\left|\frac{\gamma}{\overline{\gamma}}\left(\frac{\varepsilon}{\overline{\varepsilon}}\right)^a-1\right|\leq 2\frac{|\sigma(\gamma)|}{|\gamma|}|\varepsilon|^{-2a}, \tag{3–6}$$

and for the case $a\leq 0$ the inequality

$$\left|\left(\frac{\zeta}{\overline{\zeta}}\right)^{a^*}\frac{\sigma(\gamma)}{\overline{\sigma(\gamma)}}\left(\frac{\varepsilon}{\overline{\varepsilon}}\right)^{-a}-1\right|\leq 2\,\frac{|\gamma|}{|\sigma(\gamma)|}\,|\varepsilon|^{2a}. \tag{3–7}$$

Notice that by $\gamma\sigma(\gamma) = \pm Dp(1 \pm i)$ we have

$$\frac{\sigma(\gamma)}{\overline{\sigma(\gamma)}} = \eta^{b^*} \left(\frac{\gamma}{\overline{\gamma}}\right)^{-1}$$

for a $b^* \in \{-1, 1\}$ (here η is a generator of the torsion unit group, i.e. $\eta = \pm i$). Further, notice that we always have $\gamma = \pm\eta^k\gamma_j$ or $\gamma = \pm\eta^k\sigma(\gamma_j)$, where the numbers γ_j for j in a subset of $\{1, 2, 3\}$ are given in the Appendix. In what follows, each different γ_j is treated separately.

Now define $\alpha_0, \alpha_1, \alpha_2 \in (-\pi, \pi]$ by

$$e^{i\alpha_0} = \frac{\gamma_j}{\overline{\gamma_j}}, \quad e^{i\alpha_1} = \frac{\varepsilon}{\overline{\varepsilon}}, \quad e^{i\alpha_2} = i,$$

so $\alpha_2 = \pi/2$. Inequality (3–6) now reads

$$|e^{i(\pm(\alpha_0 - l\alpha_2) + a\alpha_1)} - 1| \le 2\,\frac{|\sigma(\gamma)|}{|\gamma|}\,|\varepsilon|^{-2a}$$

for an $l \in \mathbb{Z}$, that is determined modulo 4 only, and similarly inequality (3–7) becomes

$$\left|e^{i(\pm(\alpha_0 - l\alpha_2) - a\alpha_1)} - 1\right| \le 2\,\frac{|\gamma|}{|\sigma(\gamma)|}\,|\varepsilon|^{2a}.$$

So we now put

$$\Lambda = \alpha_0 + A\alpha_1 - l\alpha_2$$

where $A = a$ or $A = -a$ such that the left-hand sides of (3–6) and (3–7) become $|e^{\pm i\Lambda} - 1|$, and where we take l so that $|\Lambda| \le \pi$. This choice of l ensures that

$$B = \max\{|A|, |l|\} \le 4 + 2\,|A|. \tag{3–8}$$

Then, by (3–6) and (3–7), the following inequality holds in all cases:

$$|\Lambda| \le K|\varepsilon|^{-2|A|}. \tag{3–9}$$

where

$$K = 2\pi \max\left\{\frac{|\sigma(\gamma)|}{|\gamma|},\ \frac{|\gamma|}{|\sigma(\gamma)|}\right\}.$$

In the Appendix we give the values of K and $\log|\varepsilon|$ in all our cases.

Note that $\Lambda = 0$ implies by (3–5), (3–6) and (3–7) that $\gamma\varepsilon^a$ equals its complex conjugate, hence by (3–1) and (3–3) the same is true for $\theta\kappa$. Then by the definition of θ we have that $x + pi = \delta\kappa^2 = (\theta\kappa)^2/D$ equals its complex conjugate, which is obviously false. So $\Lambda \ne 0$, and we are in a position to apply the theory of linear forms in logarithms. The result of [Baker and Wüstholz 1993] is

$$|\Lambda| > e^{-C\log B} \tag{3–10}$$

for a large constant C. In the Appendix we computed C for all cases. Notice that in all cases $\varepsilon/\overline{\varepsilon}$ and $\gamma/\overline{\gamma}$ lie in a field of degree 8 over $\mathbb{Q}$. Further, in case II it appears that the linear form in fact has only two terms, since then it happens that $\alpha_0 = \frac{1}{4}\pi$, so that we can write $\Lambda = A\alpha_1 - L\pi/4$ for an $L \in \mathbb{Z}$, and redefine α_2 as $\frac{1}{4}\pi$, and α_0 as 0.

The lower bound (3–10) for $|\Lambda|$ contradicts the upper bound given by (3–9) if B becomes large enough (and thus, in view of (3–8), $|A|$ too). Precisely, in this way we find by (3–8), (3–9), and (3–10),

$$\begin{aligned} C\log B &> -\log|\Lambda| \ge -\log K + 2|A|\log|\varepsilon| \\ &\ge -\log K - 4\log|\varepsilon| + B\log|\varepsilon|. \end{aligned}$$

From the numerical values of our constants we thus find

$$|A| \le B \le B_0, \tag{3–11}$$

where B_0 is given in the Appendix (and in Table 4 below). In fact, in all cases $B_0 \le 1.65799 \times 10^{20}$.

Reducing the Upper Bound

In reducing the upper bound (3–11) we follow [Tzanakis and de Weger 1989]. Take a constant C_0, somewhat larger that B_0^2. Put

$$\mathcal{A} = \begin{pmatrix} 1 & 0 \\ [C_0\alpha_1] & [C_0\alpha_2] \end{pmatrix}, \quad \boldsymbol{y} = \begin{pmatrix} 0 \\ -[C_0\alpha_0] \end{pmatrix},$$

where $[\,\cdot\,]$ denotes rounding off towards zero. Note that in case II we have $\boldsymbol{y} = \boldsymbol{0}$. Consider the lattice

$$\Gamma = \{\mathcal{A}\boldsymbol{x} : \boldsymbol{x} \in \mathbb{Z}^2\},$$

and put

$$d(\Gamma, \boldsymbol{y}) = \min_{\boldsymbol{u}\in\Gamma, \boldsymbol{u}\ne\boldsymbol{y}} |\boldsymbol{u} - \boldsymbol{y}|.$$

By a variant of the Euclidean algorithm it is easy to compute $d(\Gamma, \boldsymbol{y})$. For a solution (A, l) of (3–9) we define λ by

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

As in [Tzanakis and de Weger 1989] we find $A^2 + \lambda^2 \geq d(\Gamma, \boldsymbol{y})^2$ and $|\lambda - C_0\Lambda| \leq 1 + 2B_0$. Using (3–9), this shows that if $d(\Gamma, \boldsymbol{y}) > \sqrt{5B_0^2 + 4B_0 + 1}$, then

$$|A| < \frac{1}{2\log|\varepsilon|}\Bigl(\log C_0 + \log K - \log\bigl(\sqrt{d(\Gamma,\boldsymbol{y})^2 - B_0^2} - (1+2B_0)\bigr)\Bigr).$$

We did this reduction in each case, using $C_0 = 10^{43}$, and in case I for all p subsequently using $C_0 = 10^5$ and the new B_0 being $4 + 2\times$ the just found reduced upper bound for $|A|$. We present results in Table 4.

Note that the size of the initial upper bound B_0 is determined almost entirely by the number of terms in the linear form in logarithms (2 in case II and 3 in the other cases). Further, the size of the reduced bound is determined almost entirely by the regulator $\log|\varepsilon|$. This becomes apparent in a remarkable way in case II for $p = 167$ and $p = 1201$, where the bound is reduced in one step from 1.04804×10^{15} to 0, even with a far too large C_0, and hence far too large $d(\Gamma, \boldsymbol{y})$.

We thus reach $|A| \leq 7$ in all cases. For the few remaining possibilities we checked equation (3–5), and thus found only the solutions listed in Table 5.

This completes the proof of Theorems 1 to 4. The total computation time is to be measured in minutes only on a 486 personal computer.

case	p	j	C_0	$B_0 \leq$	$d(\Gamma,\boldsymbol{y}) >$	$\lvert A\rvert \leq$
I	167	1	10^{43}	6.57394×10^{19}	4.18793×10^{21}	33
			10^5	70	203.769	6
I	223	1	10^{43}	6.88974×10^{19}	3.96114×10^{21}	33
			10^5	70	288.118	6
I	337	1	10^{43}	7.34120×10^{19}	6.81355×10^{20}	34
			10^5	72	175.413	7
I	337	2	10^{43}	7.34120×10^{19}	3.85752×10^{20}	35
			10^5	74	308.084	5
I	1201	1	10^{43}	8.73426×10^{19}	4.03328×10^{21}	33
			10^5	70	287.868	5
I	1201	2	10^{43}	8.73426×10^{19}	1.12741×10^{21}	34
			10^5	72	177.341	7
II	167	1	10^{43}	1.04804×10^{15}	2.32314×10^{21}	0
II	223	1	10^{43}	1.04804×10^{15}	2.92249×10^{21}	3
II	337	1	10^{43}	1.04804×10^{15}	2.96975×10^{21}	2
II	1201	1	10^{43}	1.04804×10^{15}	2.91083×10^{21}	0
III	337	1	10^{43}	1.29880×10^{20}	1.37682×10^{21}	4
III	337	2	10^{43}	1.29880×10^{20}	8.77527×10^{20}	5
III	337	3	10^{43}	1.29880×10^{20}	3.78415×10^{20}	5
III	1201	1	10^{43}	1.58087×10^{20}	3.07190×10^{21}	3
III	1201	2	10^{43}	1.58087×10^{20}	1.24798×10^{21}	3
IV	337	1	10^{43}	1.29880×10^{20}	1.17413×10^{21}	6
IV	337	2	10^{43}	1.29880×10^{20}	4.12866×10^{21}	7
IV	1201	1	10^{43}	1.58087×10^{20}	5.52862×10^{20}	3
IV	1201	2	10^{43}	1.58087×10^{20}	1.63354×10^{21}	3
IV	1201	3	10^{43}	1.58087×10^{20}	2.30565×10^{21}	3
VI	1201	1	10^{43}	1.65799×10^{20}	2.44886×10^{21}	5
VI	1201	2	10^{43}	1.65799×10^{20}	3.13041×10^{21}	5

TABLE 4. Data of the reduction.

p	case	$\pm\gamma$	a	x
337	I	$\gamma_1,\, \sigma(\gamma_1)$	0	-287
337	I	$\eta\gamma_2$	2	2113
337	I	$\eta\sigma(\gamma_2)$	-2	2113
1201	I	$\eta\gamma_1$	1	1999
1201	I	$\sigma(\gamma_1)$	-1	1999
1201	I	$\eta\gamma_2$	1	599
1201	I	$\sigma(\gamma_2)$	-1	599
167	II	$\gamma_1,\, \sigma(\gamma_1),\, \eta\gamma_1,\, \eta\sigma(\gamma_1)$	0	-167
223	II	$\gamma_1,\, \sigma(\gamma_1),\, \eta\gamma_1,\, \eta\sigma(\gamma_1)$	0	-223
337	II	$\gamma_1,\, \sigma(\gamma_1),\, \eta\gamma_1,\, \eta\sigma(\gamma_1)$	0	-337
1201	II	$\gamma_1,\, \sigma(\gamma_1),\, \eta\gamma_1,\, \eta\sigma(\gamma_1)$	0	-1201
1201	VI	$\eta\gamma_2$	1	58849
1201	VI	$\eta\sigma(\gamma_2)$	-1	58849
1201	VI	$\gamma_2,\, \sigma(\gamma_2)$	0	58849

TABLE 5. The solutions of (3–5).

APPENDIX

Our main task in this Appendix is to compute all possibilities, up to units modulo torsion, for the parameter γ in equation (3–1). This parameter satisfies

$$N_{\mathbb{K}/\mathbb{Q}(i)}(\gamma) = \gamma\sigma(\gamma) = \pm Dp(1 \pm i), \qquad N_{\mathbb{K}/\mathbb{Q}}(\gamma) = 2D^2p^2. \tag{A–1}$$

case	p	f_θ	f_φ	integral basis	θ	Δ
I	all	x^4-4x^2+8	x^4-2x^2+2	$1,\ \varphi,\ \varphi^2,\ \varphi^3$	$[0,2,0,-1]$	2^9
II	167	$x^4-668x^2+223112$	$x^4-334x^2+55778$	$1,\ \varphi,\ \frac{1}{167}\varphi^2,\ \frac{1}{167}\varphi^3$	$[0,2,0,-1]$	$2^9\cdot 167^2$
II	223	$x^4-892x^2+397832$	$x^4-446x^2+99458$	$1,\ \varphi,\ \frac{1}{223}\varphi^2,\ \frac{1}{223}\varphi^3$	$[0,2,0,-1]$	$2^9\cdot 223^2$
II	337	$x^4-1348x^2+908552$	$x^4-674x^2+227138$	$1,\ \varphi,\ \frac{1}{337}\varphi^2,\ \frac{1}{337}\varphi^3$	$[0,2,0,-1]$	$2^9\cdot 337^2$
II	1201	$x^4-4804x^2+11539208$	$x^4-2402x^2+2884802$	$1,\ \varphi,\ \frac{1}{1201}\varphi^2,\ \frac{1}{1201}\varphi^3$	$[0,2,0,-1]$	$2^9\cdot 1201^2$
III	337	$x^4-6066x^2+38272753$	$x^4-23-3x^2+4x+20$	$1,\ \varphi,\ \frac{2+3\varphi+\varphi^2}{4},\ \frac{2+\varphi+\varphi^3}{4}$	$[25,-2,-48,32]$	$2^4\cdot 337$
III	1201	$x^4-57648x^2+1732323601$	x^4-48x^2+1201	$1,\ \varphi,\ \frac{1+\varphi^2}{25},\ \frac{\varphi+\varphi^3}{25}$	$[0,49,0,-25]$	$2^8\cdot 1201$
IV	337	$x^4-10784x^2+38272753$	x^4-32x^2+337	$1,\ \varphi,\ \frac{2+\varphi^2}{9},\ \frac{2\varphi+\varphi^3}{9}$	$[0,34,0,-9]$	$2^8\cdot 337$
IV	1201	$x^4-60050x^2+1732323601$	$x^4-2x^3-11x^2+12x+72$	$1,\ \varphi,\ \frac{5\varphi+\varphi^2}{6},\ \frac{5\varphi+\varphi^3}{6}$	$[49,-6,-72,48]$	$2^4\cdot 1201$
V	337	$x^4-33700x^2+306182024$	x^4-50x^2+674	$1,\ \varphi,\ \frac{3+\varphi^2}{7},\ \frac{3\varphi+\varphi^3}{7}$	$[0,53,0,-7]$	$2^9\cdot 337$
V	1201	$x^4-235396x^2+13858588808$	x^4-98x^2+2402	$1,\ \varphi,\ \varphi^2,\ \varphi^3$	$[0,98,0,-1]$	$2^9\cdot 1201$
VI	337	$x^4+9436x^2+306182024$	x^4-14x^2+674	$1,\ \varphi,\ \frac{18+\varphi^2}{25},\ \frac{18\varphi+\varphi^3}{25}$	$[0,32,0,-25]$	$2^9\cdot 337$
VI	1201	$x^4+4804x^2+13858588808$	x^4-2x^2+2402	$1,\ \varphi,\ \frac{48+\varphi^2}{49},\ \frac{48\varphi+\varphi^3}{49}$	$[0,48,0,1]$	$2^9\cdot 1201$

case	p	$\sigma(\varphi)$	class group	ε	$\log\lvert\varepsilon\rvert$	η	ζ
I	all	$-\varphi$	trivial	$[1,1,0,0]$	$0.7642854597\ldots$	$[1,0,-1,0]$	η
II	167	$-\varphi$	C_2	$[10274571991916504257638181614625\,43,$ $827414776081310794340980496312 70,$ $-925977270707225969051835703018 25,$ $-288460455029147002276719615762 90]$	$76.6159777243\ldots$	$[1,0,-1,0]$	-1
II	223	$-\varphi$	C_{20}	$[3121,-172,-1337,108]$	$8.4026350290\ldots$	$[1,0,-1,0]$	-1
II	337	$-\varphi$	$C_8\times C_4$	$[31679,2274,10783,-288]$	$11.3807589430\ldots$	$[1,0,-1,0]$	-1
II	1201	$-\varphi$	$C_8\times C_4$	$[870467395091137,\ 18387380204044,$ $-495880468949768,-14594648896220]$	$34.7562401985\ldots$	$[1,0,-1,0]$	1
III	337	$1-\varphi$	trivial	$[115,59,7,-45]$	$5.3601764068\ldots$	$[1,1,-1,0]$	$-\eta$
III	1201	$-\varphi$	C_4	$[9271,1752,-2359,-829]$	$9.5892515738\ldots$	$[1,0,-1,0]$	1
IV	337	$-\varphi$	C_4	$[38,11,-7,-3]$	$3.9116856241\ldots$	$[2,0,-1,0]$	1
IV	1201	$1-\varphi$	trivial	$[2133,881,718,-303]$	$8.7179705990\ldots$	$[1,1,-1,0]$	η
V	337	$-\varphi$	C_4	$[329,41,-128,-20]$	$6.1017599984\ldots$	$[4,0,-1,0]$	$-\eta$
V	1201	$-\varphi$	C_8	$[7,1,0,0]$	$2.6390963699\ldots$	$[49,0,-1,0]$	η
VI	337	$-\varphi$	C_4	$[1,-1,3,0]$	$2.3120607729\ldots$	$[1,0,-1,0]$	η
VI	1201	$-\varphi$	C_8	$[1,-10,49,0]$	$4.9417454873\ldots$	$[1,0,-1,0]$	-1

TABLE 6. Field data. The number θ is defined on page 250. In each case we give the field in terms of a somewhat simpler generator φ. Top: f_θ and f_φ are defining polynomials for θ and φ. The notation $[a,b,c,d]$ is used for an algebraic number to denote its coefficients with respect to the given integral basis. (Note that $\mathbb{K}$ is always a quadratic extension of $\mathbb{Q}(i)$, and is totally complex.) Δ is the field discriminant. Bottom: σ is the nontrivial $\mathbb{Q}(i)$-automorphism, ε is a generator of the group of units modulo torsion, η is a generator of the group of torsion units (hence an embedding into $\mathbb{C}$ sends η to $\pm i$), and $\zeta=\varepsilon\sigma(\varepsilon)$.

We will also compute some other paramaters needed in Section 3. Numerical values of the α_i are given to 50 decimal places, which is sufficient to perform the reduction steps.

We have to study several quartic fields $\mathbb{K} = \mathbb{Q}(\theta)$, which we did using Pari 1.38. (The number θ is defined in Section 3.) The results are presented in Table 6.

Our next task is to compute the decomposition of (2) and (p) into prime ideals, and from this, all possibilities for γ, using (A–1). We always have $\gamma = \pm\eta^k\gamma_j$ or $\gamma = \pm\eta^k\sigma(\gamma_j)$ for $k \in \{0,1\}$, where γ_j is given in Table 8.

Note that in the cases V for both $p = 337$ and $p = 1201$, and in the case VI for $p = 337$ we have found a contradiction: no principal ideal satisfying (A–1) exists.

We next have to compute heights. We made maybe sometimes rough estimates, but they are sufficient for our purposes. In fact, in any case we have

$$h(\varepsilon/\overline{\varepsilon}) \le 2h(\varepsilon) = \log|\varepsilon|,$$
$$h(\gamma_j/\overline{\gamma_j}) \le 2h(\gamma_j) \le \tfrac{1}{2}\log N_{\mathbb{K}/\mathbb{Q}}(\gamma) = \log\sqrt{2}Dp.$$

Note that in the cases II for all p we find $\gamma_1/\overline{\gamma_1} = e^{3\pi i/4}$, so the linear form Λ can be written as $\Lambda = A\alpha_1 - L\pi/4$. So then we have redefined α_2 as $\pi/4$, and α_0 as 0.

We now have sufficient data to apply the main theorem of Baker and Wüstholz [1993]. Thus we computed the constant C appearing in inequality (3–10) in each case, and we give C, K, B_0 in Table 7.

Finally we present in Table 9 the numerical values of the numbers α_0, α_1 to sufficient precision. They serve as input for the (essentially Euclidean) reduction algorithm.

case	p	j	$K<$	$C<$	$B_0<$
I	167	1	7.34749	1.10106×10^{18}	6.57394×10^{19}
I	223	1	12.76258	1.15277×10^{18}	6.88974×10^{19}
I	337	1	8.13968	1.22660×10^{18}	7.34120×10^{19}
I	337	2	6.95642	1.22660×10^{18}	7.34120×10^{19}
I	1201	1	8.66105	1.45384×10^{18}	8.73426×10^{19}
I	1201	2	8.50634	1.45384×10^{18}	8.73426×10^{19}
II	167	1	6.28319	2.32167×10^{15}	1.04804×10^{15}
II	223	1	6.28319	2.54622×10^{14}	1.04804×10^{15}
II	337	1	6.28319	3.44867×10^{14}	1.04804×10^{15}
II	1201	1	6.28319	1.05321×10^{15}	1.04804×10^{15}
III	337	1	16.03643	1.50320×10^{19}	1.29880×10^{20}
III	337	2	69.08756	1.50320×10^{19}	1.29880×10^{20}
III	337	3	921.72694	1.50320×10^{19}	1.29880×10^{20}
III	1201	1	4205.61076	3.25940×10^{19}	1.58087×10^{20}
III	1201	2	91778.06827	3.25940×10^{19}	1.58087×10^{20}
IV	337	1	23.06428	1.09699×10^{19}	1.29880×10^{20}
IV	337	2	314.05330	1.09699×10^{19}	1.29880×10^{20}
IV	1201	1	4517.81464	2.96325×10^{19}	1.58087×10^{20}
IV	1201	2	141.12712	2.96325×10^{19}	1.58087×10^{20}
IV	1201	3	646.99840	2.96325×10^{19}	1.58087×10^{20}
VI	1201	1	25.90466	1.75984×10^{19}	1.65799×10^{20}
VI	1201	2	879.73661	1.75984×10^{19}	1.65799×10^{20}

TABLE 7. Constants and upper bounds.

REFERENCES

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

[Bilu 1994] Y. Bilu, "Solving superelliptic Diophantine equations by the method of Gelfond–Baker", preprint 94–09, Univ. Bordeaux 2, 1994.

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math. **138**, Springer, Berlin, 1993.

[Cremona 1992] J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, 1992.

[Ellison et al. 1972] W. J. Ellison, F. Ellison, J. Pesek, C. E. Stahl, and D. S. Stall, "The Diophantine equation $y^2 + k = x^3$", *J. Number Theory* **4** (1972), 107–117.

[Gebel and Zimmer 1994] J. Gebel and H. G. Zimmer, "Computing the Mordell-Weil group of an elliptic curve over $\mathbb{Q}$", pp. 61–83 in *Elliptic curves and related topics*, edited by H. Kisilevsky and M. R. Murty, CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence, RI, 1994.

[Gebel et al. 1994] J. Gebel, A. Pethő, and H. G. Zimmer, "Computing integral points on elliptic curves", *Acta Arith.* **68**:2 (1994), 171–192.

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

[Pohst and Zassenhaus 1989] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Encyclopedia of Mathematics and its Applications **30**, Cambridge University Press, Cambridge, 1989.

case	p	decomposition	ideals	(γ)	γ_j
I	all	$(2)=\mathfrak{q}^4$	$\mathfrak{q}=([0,1,0,0])$		
I	167	$(167)=\mathfrak{p}\sigma(\mathfrak{p})$	$\mathfrak{p}=([1,14,-2,-4])$	$\mathfrak{q}^3\mathfrak{p}^m\sigma(\mathfrak{p})^{1-m}$	$\gamma_1=[12,-4,-20,3]$
I	223	$(223)=\mathfrak{p}\sigma(\mathfrak{p})$	$\mathfrak{p}=([9,9,-1,3])$	$\mathfrak{q}^3\mathfrak{p}^m\sigma(\mathfrak{p})^{1-m}$	$\gamma_1=[18,16,6,-9]$
I	337	$(337)=$ $\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2\sigma(\mathfrak{p}_2)$	$\mathfrak{p}_1=([3,1,1,-1])$ $\mathfrak{p}_2=([1,-2,2,2])$	$\mathfrak{q}^3\mathfrak{p}_1^m\sigma(\mathfrak{p}_1)^{1-m}\mathfrak{p}_2^n\sigma(\mathfrak{p}_2)^{1-n}$	$\gamma_1=[10,26,0,-25]$ $\gamma_2=[14,-18,8,17]$
I	1201	$(1201)=$ $\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2\sigma(\mathfrak{p}_2)$	$\mathfrak{p}_1=([3,2,2,-2])$ $\mathfrak{p}_2=([1,5,0,0])$	$\mathfrak{q}^3\mathfrak{p}_1^m\sigma(\mathfrak{p}_1)^{1-m}\mathfrak{p}_2^n\sigma(\mathfrak{p}_2)^{1-n}$	$\gamma_1=[66,-16,-50,-7]$ $\gamma_2=[74,-24,-50,7]$
II	167	$(2)=\mathfrak{q}^4$ $(167)=\mathfrak{p}\sigma(\mathfrak{p})$	$\mathfrak{q}=([32945578597020996,$ $-1592306022993617,$ $-24269413632834339,$ $1675060839211249])$ $\mathfrak{p}=([293555214456623127,$ $-24269413632834339,$ $-13820054308344544,$ $7796624334323841])$	$\mathfrak{q}^3\mathfrak{p}$	$\gamma_1=[0,0,0,1]$
II	223	$(2)=\mathfrak{q}^4$ $(223)=\mathfrak{p}\sigma(\mathfrak{p})$	$\mathfrak{q}=([56,3,-26,-2])$ $\mathfrak{p}=([223,-26,223,-2])$	$\mathfrak{q}^3\mathfrak{p}$	$\gamma_1=[0,0,0,1]$
II	337	$(2)=\mathfrak{q}^4$ $(337)=\mathfrak{p}_1^2\mathfrak{p}_2^2$	$\mathfrak{q}=([240,9,-153,-8])$ $\mathfrak{p}_1,\mathfrak{p}_2$ nonprincipal $\mathfrak{p}_1\mathfrak{p}_2=([3033,87,-2696,120])$	$\mathfrak{q}^3\mathfrak{p}_1\mathfrak{p}_2$	$\gamma_1=[0,0,0,1]$
II	1201	$(2)=\mathfrak{q}^4$ $(1201)=\mathfrak{p}\sigma(\mathfrak{p})$	$\mathfrak{q}$ nonprincipal $\mathfrak{p}_1$ nonprincipal $\mathfrak{q}\mathfrak{p}_1=([-57159144,\ 249799,$ $111027622,1988755])$ $\mathfrak{p}_2=([-111677901,\ 3387622,$ $8233730,-1145122])$	$\mathfrak{q}^3\mathfrak{p}_1\mathfrak{p}_2$	$\gamma_1=[0,0,0,1]$
III	337	$(2)=\mathfrak{q}^2\sigma(\mathfrak{q})^2$ $(337)=\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2^2$	$\mathfrak{q}=([0,0,1,0])$ $\mathfrak{p}_1=([1,-6,4,0])$ $\mathfrak{p}_2=([1,-2,0,0])$	$\mathfrak{q}^m\sigma(\mathfrak{q})^{1-m}\mathfrak{p}_1^l\sigma(\mathfrak{p}_1)^{2-l}\mathfrak{p}_2^2$	$\gamma_1=[624,200,-407,88]$ $\gamma_2=[0,0,337,0]$ $\gamma_3=[3580,3025,-3956,1117]$
III	1201	$(2)=\mathfrak{q}^4$ $(1201)=\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2^2$	$\mathfrak{q}=([23,3,-61,7])$ $\mathfrak{p}_1=([0,1,5,0])$ $\mathfrak{p}_2=([0,1,0,0])$	$\mathfrak{q}\mathfrak{p}_1^l\sigma(\mathfrak{p}_1)^{2-l}\mathfrak{p}_2^2$	$\gamma_1=[6001,-2623,9708,-480]$ $\gamma_2=[27623,3603,-73261,8407]$
IV	337	$(2)=\mathfrak{q}^4$ $(337)=\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2^2$	$\mathfrak{q}=([2,1,1,0])$ $\mathfrak{p}_1=([3,1,-3,0])$ $\mathfrak{p}_2=([0,1,0,0])$	$\mathfrak{q}\mathfrak{p}_1^l\sigma(\mathfrak{p}_1)^{2-l}\mathfrak{p}_2^2$	$\gamma_1=[153,-76,154,5]$ $\gamma_2=[674,337,337,0]$
IV	1201	$(2)=\mathfrak{q}^2\sigma(\mathfrak{q})^2$ $(1201)=\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2^2$	$\mathfrak{q}=([2,-2,1,0])$ $\mathfrak{p}_1=([27,17,-30,7])$ $\mathfrak{p}_2=([1,-2,0,0])$	$\mathfrak{q}^m\sigma(\mathfrak{q})^{1-m}\mathfrak{p}_1^l\sigma(\mathfrak{p}_1)^{2-l}\mathfrak{p}_2^2$	$\gamma_1=[2722,9668,-9940,-2797]$ $\gamma_2=[2402,-2402,1201,0]$ $\gamma_3=[6806,7600,-3635,-2362]$
V	337	$(2)=\mathfrak{q}^4$ $(337)=\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2^2$	$\mathfrak{q},\mathfrak{p}_1,\mathfrak{p}_2\in\mathcal{A}^2$	$\mathfrak{q}^3\mathfrak{p}_1^l\sigma(\mathfrak{p}_1)^{2-l}\mathfrak{p}_2^2$	none
V	1201	$(2)=\mathfrak{q}^4$ $(1201)=\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2^2$	$\mathfrak{q},\mathfrak{p}_1,\mathfrak{p}_2\in\mathcal{A}^4$	$\mathfrak{q}^3\mathfrak{p}_1^l\sigma(\mathfrak{p}_1)^{2-l}\mathfrak{p}_2^2$	none
VI	337	$(2)=\mathfrak{q}^4$ $(337)=\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2^2$	$\mathfrak{q},\mathfrak{p}_1,\mathfrak{p}_2\in\mathcal{A}^4$	$\mathfrak{q}^3\mathfrak{p}_1^l\sigma(\mathfrak{p}_1)^{2-l}\mathfrak{p}_2^2$	none
VI	1201	$(2)=\mathfrak{q}^4$ $(1201)=\mathfrak{p}_1\sigma(\mathfrak{p}_1)\mathfrak{p}_2^2$	$\mathfrak{q}=([10,-1,-5,1])$ $\mathfrak{p}_1=([21,2,-10,-2])$ $\mathfrak{p}_2=([49,-5,-25,5])$	$\mathfrak{q}^3\mathfrak{p}_1^l\sigma(\mathfrak{p}_1)^{2-l}\mathfrak{p}_2^2$	$\gamma_1=[2018,342,392,-199]$ $\gamma_2=[12010,2402,0,-1201]$

TABLE 8. Possibilities for γ_j. In the column (γ) the parameters m,n run through $\{0,1\}$, and l runs through $\{0,1,2\}$. In the column "ideals", $\mathcal{A}$ is an ideal class generating the class group.

case	p	j	
I	all	1	$\alpha_1 = 0.42707858639247612548064688331895685930333615088099\ldots$
I	167	1	$\alpha_0 = 2.04637251790229010116078165540835617879426934709549\ldots$
I	223	1	$\alpha_0 = -0.03925703029925735306974525816603622382406447435049\ldots$
I	337	1	$\alpha_0 = -1.7536062071392217780080203473266603322852108928865\ldots$
I	337	2	$\alpha_0 = 2.2110346230503769489584456131685011650171155930184\ldots$
I	1201	1	$\alpha_0 = 2.9635347463178025795862305781960138740635273317856\ldots$
I	1201	2	$\alpha_0 = -3.0562529567499106804509985762022363119923815077681\ldots$
II	167	1	$\alpha_1 = -0.19745572088331441539615662654250512853642884231739\ldots$
II	223	1	$\alpha_1 = -1.28628443917500963152984929655629236963064676941704\ldots$
II	337	1	$\alpha_1 = 0.49737573080345337189592038689826874911837531477174\ldots$
II	1201	1	$\alpha_1 = -1.8476993632942805074449396893957480676706619129465\ldots$
III	337	1, 2, 3	$\alpha_1 = -1.20991586741567359323493945362902447518715319378315\ldots$
III	337	1	$\alpha_0 = 2.57820224934360735136631263501690544758445762488863\ldots$
III	337	2	$\alpha_0 = 1.11214435505078374419082988153467881138852208272066\ldots$
III	337	3	$\alpha_0 = 0.856002328173633730250286581681476650379739734335857\ldots$
III	1201	1, 2	$\alpha_1 = -0.657789678520481166779189498837670710091210627217237\ldots$
III	1201	1	$\alpha_0 = -2.68071431715477348910516378548331217581427470133947\ldots$
III	1201	2	$\alpha_0 = 2.68508932945258551223657728687846251819348236314000\ldots$
IV	337	1, 2	$\alpha_1 = -0.568018734012102541798376583046650557465258549542252\ldots$
IV	337	1	$\alpha_0 = 1.03045002542603731156213285862393744666379187397820\ldots$
IV	337	2	$\alpha_0 = 0.501388796391397038716472554296550442316663075072650\ldots$
IV	1201	1, 2, 3	$\alpha_1 = 0.172668798235089931546778117445675675351495031660719\ldots$
IV	1201	1	$\alpha_0 = 1.65664292192666408867224763512233981880431662537874\ldots$
IV	1201	2	$\alpha_0 = 0.807704955972425812187470144570839458385135024414367\ldots$
IV	1201	3	$\alpha_0 = -3.01015686533651577121317261181448811087972094426439\ldots$
VI	1201	1, 2	$\alpha_1 = 1.55049299476067579365442935933824729518686421685792\ldots$
VI	1201	1	$\alpha_0 = 1.52323200061915050392055616818253122637170183429667\ldots$
VI	1201	2	$\alpha_0 = 1.58094799281200703201976785779050351555444494110236\ldots$

TABLE 9. The input data for the reduction algorithm.

[Schmitt 1997] S. Schmitt, "Computation of the Selmer groups of certain parameterized elliptic curves", *Acta Arith.* **78**:3 (1997), 241–254.

[Smart 1994] N. P. Smart, "S-integral points on elliptic curves", *Math. Proc. Cambridge Philos. Soc.* **116**:3 (1994), 391–399.

[Stroeker and Top 1994] R. J. Stroeker and J. Top, "On the equation $Y^2 = (X+p)(X^2+p^2)$", *Rocky Mountain J. Math.* **24**:3 (1994), 1135–1161.

[Stroeker and Tzanakis 1994] R. J. Stroeker and N. Tzanakis, "Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms", *Acta Arith.* **67**:2 (1994), 177–196.

[Stroeker and de Weger 1994] R. J. Stroeker and B. M. M. de Weger, "On elliptic Diophantine equations that defy Thue's method: the case of the Ochoa curve", *Experiment. Math.* **3**:3 (1994), 209–220.

[Tzanakis and de Weger 1989] N. Tzanakis and B. M. M. de Weger, "On the practical solution of the Thue equation", *J. Number Theory* **31**:2 (1989), 99–132.

[de Weger 1997] B. M. M. de Weger, "S-integral solutions to a Weierstrass equation", *J. Th. Nombres Bordeaux* **9**:2 (1997), 281–301.

Benjamin M. M. de Weger, Sportsingel 30, 2924 XN Krimpen aan den IJssel, The Netherlands (deweger@xs4all.nl)

Received March 19, 1997; accepted in revised form December 4, 1997