Ann. Sci. Math. Québec **35**, No 2, (2011), 153–174

ON THE EQUATION $Y^2 = X^6 + k$

ANDREW BREMNER AND NIKOS TZANAKIS

Dedicated with respect and admiration to Professor Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. Nous trouvons explicitement toutes les solutions rationelles de l'équation du titre pour tous les entiers k avec $|k| \leq 50$, sauf pour les valeurs $k = -47, -39$. Pour la résolution, nous appliquons diverses méthodes qui, selon k, varient des méthodes élémentaires, telles que la divisibilité ou des considérations de congruences, jusqu'aux techniques dites « elliptiques à la Chabauty » et des calculs hautement complexes dans des corps des nombres, ou des combinaisons de ces méthodes. Pour certains ensembles de valeurs de k, nous pouvons proposer une méthode de résolution plus ou moins uniforme, qui pourrait être appliquée avec succès pour un ensemble important de valeurs de k, même au-delà des valeurs ci-dessus. Cependant, il s'avère que six valeurs parmi celles que nous considérons nous mettent vraiment au défi, à savoir $k = 15, 43, -11, -15, -39, -47$. Plus de la moitié de l'article traite de la résolution de l'équation du titre pour les quatre premières valeurs. Pour les deux dernières valeurs, la résolution de l'équation a résisté à tous nos efforts. La présence de ces six valeurs de k est une indication qu'on ne peut pas espérer une méthode générale de résolution applicable, même en principe, pour *toutes* les valeurs de k.

ABSTRACT. We find explicitly all rational solutions of the title equation for all integers k in the range $|k| \leq 50$ except for $k = -47, -39$. For the solution, a variety of methods are applied, which, depending on k, may range from elementary, such as divisibility and congruence considerations, to elliptic Chabauty techniques and highly technical computations in algebraic number fields, or a combination thereof. For certain sets of values of k we can propose a more or less uniform method of solution, which might be applied successfully for quite a number of cases of k, even beyond the above range. It turns out, however, that in the range considered, six really challenging cases have to be dealt with individually, namely $k = 15, 43, -11, -15, -39, -47$. More than half of the paper is devoted to the solution of the title equation for the first four of these values. For the last two values the solution of the equation, at present, has resisted all our efforts. The case with these six values of k shows that one cannot expect a general method of solution which could be applied, even in principle, for *every* value of k.

1. Introduction

For a fixed integer k, there is a vast literature devoted to the integer solutions of the Diophantine equation $Y^2 = X^3 + k$ (Mordell's equation). It is well known that the

Reçu le 20 février 2009 et, sous forme définitive, le 29 août 2009.

equation has only finitely many integer solutions, and many individuals over the years investigated this problem, starting with solving the equation for particular values of k. There now exists a very satisfactory uniform method (the elliptic logarithm method, developed independently by Stroeker and Tzanakis [13] and Gebel, Pethő, Zimmer [11]) for explicitly computing all integer solutions on elliptic curves. See Gebel, Pethő, Zimmer [12] for a very successful application of this method to computing all integer points on Mordell's equation for a given k. When we consider *rational* solutions to Mordell's equation, then the whole theory of elliptic curves comes into play, and many questions remain unresolved, which is not however the focus here. In this paper we shall study rational solutions of the naturally arising Diophantine equation

$$C_k : Y^2 = X^6 + k \tag{1}$$

for a fixed integer $k \neq 0$, free of sixth powers. There are two rational points at infinity on C_k corresponding to $Y = \pm X^3$, and henceforth we shall consider only finite rational points. Since C_k represents a curve of genus 2, Faltings's theorem ("Mordell's Conjecture") [9], shows that $C_k(\mathbb{Q})$ is finite. It is well known that both Falting's proof and the subsequent one by P. Vojta [14] are non-effective (though an effectively computable bound for the number of rational points is accomplished), hence they cannot provide us with a practical method for the explicit determination of all rational points on C_k. Thus determination of rational points on C_k is a good challenge. We attack this challenge by a series of approaches that start with elementary ideas and progress to being more technical; we illustrate the ideas by applying them to k in the range $|k| \leq 50$.

If the rank of the Jacobian J_k of C_k is at most equal to 1, then there are effective "Chabauty" techniques that allow (at least in principle, but not provably) determination of $C_k(\mathbb{Q})$. However, the Jacobian J_k is isogenous to the product of the two elliptic curves

$$\mathcal{E}_1 : Y_1^2 = X_1^3 + k, \qquad \mathcal{E}_2 : Y_2^2 = X_2^3 + k^2, \tag{2}$$

with maps from C_k to $\mathcal{E}_i$, $i = 1, 2$, given by

$$(X_1, Y_1) = (X^2, Y), \qquad (X_2, Y_2) = \left(\frac{k}{X^2}, \frac{kY}{X^3}\right).$$

Thus the rank of J_k is the sum of the ranks of $\mathcal{E}_1$ and $\mathcal{E}_2$. If J_k has rank at most 1, then there is no need to use Chabauty techniques, for in such a case the rank of $\mathcal{E}_1$ or $\mathcal{E}_2$ is 0, and either there are no finite rational points on (1), or there are only the obvious ones arising from non-zero torsion points on $\mathcal{E}_i$ (which occur for k a perfect square or perfect cube).

The interesting cases therefore arise when both $\mathcal{E}_1$ and $\mathcal{E}_2$ have positive ranks. We know of only one example in the literature where the set of rational points is determined upon such a curve: Coombes and Grant [6] in an example show that the only rational points on the curve $y^2 = x^6 - 972$ (with covering elliptic curves both of rank 1) are the points at infinity. This will also follow from the elementary arguments of section 2.2 below.

To deal with (1), we shall construct maps to C_k from curves having ternary equations of type $ax^6 + by^6 = cz^3$. This is the particular form of a very natural generalized

Fermat curve. Several important papers recently have been devoted to generalized Fermat equations, and papers of Bennett and Skinner [2] and Darmon and Granville [7] seem applicable when at least one of the exponents in the equation is large. However, the specific equations $ax^6 + by^6 = cz^3$ (and $ax^6 + by^6 = cz^2$) seem poorly treated, indeed, essentially absent, in the literature. We can find one paper by Dem'yanenko [8], who *inter alia* discusses the equations $x^6 + y^6 = az^2$ and $x^6 + y^6 = az^3$. This dearth is curious. For several decades in the early twentieth century, number theorists were attracted to showing the impossibility of specific Diophantine equations by elementary methods; we have here a class of such equations where impossibility may often be shown by an argument involving an elliptic curve of rank 0, in other words, by a classical elementary infinite descent argument. This class of equations seems to have been overlooked by earlier researchers. In any event, for a certain class of k's, these curves $ax^6 + by^6 = cz^3$ of genus 4 may be shown by elementary means to have no non-trivial rational points. This furnishes explicitly all solutions to (1) for the corresponding k's; see section 2. Within this class, there are values of k for which the descent argument, while elementary, is not straightforward, and hence deserves some discussion; see section 2.2.1. Some values of k may also be eliminated using the alternative elementary ideas of section 2.2.2.

For many values of k, the above descent is inconclusive, and we turn to working over $K = \mathbb{Q}(\theta)$, with $\theta^3 = k$. There arises the problem of solving a number of Diophantine problems of the following type: for a certain elliptic curve E defined over K such that the rank of $E(K)$ is at most 2, explicitly determine those points $(x, y) \in E(K)$ satisfying a certain "rationality condition" $q(x, y) \in \mathbb{Q}$ where $q(X, Y) \in K(X, Y)$. Problems of this type are amenable to the elliptic Chabauty method as implemented in a number of routines in Magma [4]. But we should stress that the application of Magma is in general not a matter of button pushing, and is sometimes far from automatic; we note later some of the problems that can arise. For a certain class of k's, the elliptic Chabauty method applies more or less directly; and we consider the corresponding equation (1) to be interesting but whose solution is "relatively standard". So few details are given; see section 3.

For several values of k in our considered range, the elliptic Chabauty method as applied above does not succeed, as we explain in the first paragraph of section 4. This happens for $k = -47, -39, -15, -11, 15, 43$. We surmounted obstacles that arise by means of an alternative approach for the four cases $k = 15, 43, -11, -15$ (given in decreasing order of difficulty, the first two being roughly comparable). We give details on solving (1) for $k = 15$ in section 4.1, with brief details for $k = 43$ in section 4.2; and for $k = -11, -15$ in sections 4.3, 4.4. These are the most technical sections of the paper. We have been unable to develop a uniform method for the k's of this section, though believe the ideas will be useful for solving (1) for other specific "difficult" values of k.

The remaining values $k = -47, -39$ in our range have resisted all our attacks. These values give no indication of the difficulties that arise when trying to solve (1), difficulties that may not be foreseen until after many hours of work. Finding all rational points on (1) for these intractable values of k is indeed a challenging Diophantine problem.

2. General discussion

In this section we give some general discussion, the emphasis being on elementary arguments which often suffice to provide the complete solution of equation (1). Our arguments will then be applied to solve a good number of equations (1) in the range $|k| \leq 50$. Of course, as one should expect, the equation (1) is not susceptible to elementary treatment for all k, not even within the small range we consider. More technical approaches are given in sections 3, 4, and 5 of this paper.

2.1. When at least one $\mathcal{E}_i$ has zero rank

If either of the curves $\mathcal{E}_1$ or $\mathcal{E}_2$ in (2) has rank zero, then the determination of rational points on C_k is trivial. For if $\mathcal{E}_1$ has rank 0, the only possible rational points on $\mathcal{E}_1$ are torsion points, and using, for example, Cassels [5, Theorem page 52], we have on $\mathcal{E}_1$ for $k = -432$ the points $(12, \pm 36)$; for $k = 1$ the points $(2, \pm 3)$, $(0, \pm 1)$, $(-1, 0)$; for $k = D^3$, $D \neq 1$, the point $(-D, 0)$; and for $k = B^2$, $B \neq 1$, the points $(0, \pm B)$. In other cases, the torsion group is trivial. It follows that the only (finite) points on C_k occur when $k = -1$, with points $(\pm 1, 0)$; and when $k = B^2$, with points $(0, \pm B)$. Similarly, if $\mathcal{E}_2$ has rank 0, the same Theorem shows that no (finite) points arise on C_k. In the range $|k| \leq 50$ at least one curve $\mathcal{E}_i$ has rank 0 when

$$\begin{aligned} k = &\pm 1, \pm 2, -3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8, \pm 9, -10, \pm 12, 13, \pm 14, \pm 16, -17, \\ &\pm 18, \pm 19, \pm 20, 21, \pm 22, \pm 23, -24, 25, \pm 26, \pm 27, 29, \pm 30, -31, \pm 32, \\ &\pm 33, \pm 34, -36, \pm 37, \pm 38, \pm 40, \pm 41, \pm 42, \pm 44, 45, -46, 49, \pm 50\,. \end{aligned}$$

So, for the above k's equation (1) is immediately solved.

2.2. Elementary arguments

Henceforth we shall assume that the ranks of both $\mathcal{E}_1$ and $\mathcal{E}_2$ are positive. In the range $|k| \leq 50$, this is the case for for the following values:

$$\begin{aligned} k = &-49, -48, -47, -45, -43, -39, -35, -29, -28, -25, -21, -15, \\ &-13, -11, 3, 10, 11, 15, 17, 24, 28, 31, 35, 36, 39, 43, 46, 47, 48\,. \end{aligned} \tag{3}$$

Now, finding all finite points on (1) is equivalent to solving

$$x^6 + ky^6 = z^2, \quad x, y, z \in \mathbb{Z},\ y \neq 0,\ (x, y) = 1, \tag{4}$$

where $X = x/y$ and $Y = z/y^3$. The factorization $(z + x^3)(z - x^3) = ky^6$ of (4) is easily seen to lead to a number of equations of type

$$Ay_1^6 + By_2^6 = y_3^3, \quad A, B \in \mathbb{Z}\,. \tag{5}$$

The curve (5) has maps to elliptic curves as follows, where the notation

$$E := \left[\, a, b, c, d, e \,\right]$$

means that E is the elliptic curve with Weierstrass coefficients a, b, c, d, e:

$$\left(\frac{Ay_3}{y_2^2}, \frac{A^2 y_1^3}{y_2^3}\right) \text{ on } E_1 := \left[\, 0, 0, 0, 0, -A^3 B \,\right], \tag{6}$$

$$\left(\frac{By_3}{y_1^2}, \frac{B^2 y_2^3}{y_1^3}\right) \text{ on } E_2 := \left[\, 0, 0, 0, 0, -AB^3 \,\right];$$

and

$$(7)\quad \left(\frac{y_3^6 - ABy_1^6y_2^6}{y_1^4y_2^4y_3^2}, \frac{(Ay_1^6 - By_2^6)(2Ay_1^6 + By_2^6)(Ay_1^6 + 2By_2^6)}{2y_1^6y_2^6y_3^3}\right)$$

$$\text{on}\ \ E_3 := \left[0,0,0,0,-\tfrac{27}{4}A^2B^2\right].$$

If the rank of E_1 or E_2 is 0, then the solution of (5) is immediate. (The curve E_3 is in fact 3-isogenous to the curve $\mathcal{E}_2$, so by previous assumption has positive rank).

According as to the possibilities for $k \pmod 4$, four distinct types of equation (5) arise, which we denote by Types I, II, III, IV, as follows.

- Cases where $k \equiv 1 \pmod 2$.

$$\mathrm{I}:\quad 2x^3 = \delta_1y_1^6 + \delta_2y_2^6 \quad y_1y_2 \neq 0\,, \qquad (A,B) = (4\delta_1, 4\delta_2)\,,$$

$$\begin{cases} y = y_1y_2, \quad \delta_1\delta_2 = -k,\ \delta_2 > 0, \\ \left(\dfrac{\delta_1}{\delta}y_1, \dfrac{\delta_2}{\delta}y_2\right) = 1,\ \delta = (\delta_1,\delta_2), \quad (2x, y_1y_2) = 1\,. \end{cases}$$

$$\mathrm{II}:\quad x^3 = 16\delta_1y_1^6 + \delta_2y_2^6 \quad y_1y_2 \neq 0\,, \qquad (A,B) = (16\delta_1, \delta_2)\,,$$

$$\begin{cases} y = 2y_1y_2, \quad \delta_1\delta_2 = -k,\ \delta_2 > 0, \\ \left(\dfrac{2\delta_1}{\delta}y_1, \dfrac{\delta_2}{\delta}y_2\right) = 1,\ \delta = (\delta_1,\delta_2), \quad (x, 2y_1y_2) = 1\,. \end{cases}$$

- Case where $k \equiv 0 \pmod 4$.

$$\mathrm{III}:\quad x^3 = \delta_1y_1^6 + \delta_2y_2^6 \quad y_1y_2 \neq 0\,, \qquad (A,B) = (\delta_1, \delta_2)\,,$$

$$\begin{cases} y = y_1y_2, \quad \delta_1\delta_2 = -\frac{k}{4},\ \delta_2 > 0, \\ \left(\dfrac{\delta_1}{\delta}y_1, \dfrac{\delta_2}{\delta}y_2\right) = 1,\ \delta = (\delta_1,\delta_2), \quad (x, y_1y_2) = 1\,. \end{cases}$$

- Case where $k \equiv 2 \pmod 4$.

$$\mathrm{IV}:\quad x^3 = 32\delta_1y_1^6 + \delta_2y_2^6 \quad y_1y_2 \neq 0\,, \qquad (A,B) = (32\delta_1, \delta_2)\,,$$

$$\begin{cases} y = 2y_1y_2, \quad \delta_1\delta_2 = -\frac{k}{2},\ \delta_2 > 0, \\ \left(\dfrac{2\delta_1}{\delta}y_1, \dfrac{\delta_2}{\delta}y_2\right) = 1,\ \delta = (\delta_1,\delta_2), \quad (x, 2y_1y_2) = 1\,. \end{cases}$$

Equation (4) is thus reduced to a set $\mathcal{S}(k)$ of equations of type I, II, III, IV. For the following values of k at (3), all equations in $\mathcal{S}(k)$ are either impossible or have only the obvious solutions:

$$k = -49, -48, -45, -13, 11, 28, 36, 39, 46, 47\,.$$

This is proved by showing that each equation in $\mathcal{S}(k)$ either is impossible modulo m, where $m \in \{7, 8, 9, 13\}$, or corresponds to a curve E_i at (6) with zero rank for either $i = 1$ or $i = 2$.

For the following values of k all equations in $\mathcal{S}(k)$ are also impossible; however, for at least one element of $\mathcal{S}(k)$, more refined but still elementary arguments are required:

$$k = -43, -35, -29, -25, -21, 31\,.$$

We choose to give in the following subsection some details of the proposed elementary method when $k = -35$ which is a most characteristic case. Here, $\mathcal{S}(-35)$ consists of two equations of type I and four equations of type II. Five out of the six equations are impossible as congruences modulo 7 or 8 and only the equation (of type II)

$$16 \cdot 35 y_1^6 + y_2^6 = x^3, \quad y_1 y_2 \neq 0\,, \tag{8}$$

remains. This belongs to the more general class of equations

$$DY_1^6 + Y_2^6 = X^3, \quad Y_1 \neq 0,\ (DY_1, Y_2) = 1\,, \tag{9}$$

where D is a sixth power free non-zero integer.

It is worth noting that for a number of D's, equations (9) can be treated by quite elementary means.

2.2.1. An approach to (9) with application to $k = -43, -35, -21, 31$

We distinguish two cases, depending on the divisibility of $X - Y_2^2$ by 3.

Case (i): $X - Y_2^2 \not\equiv 0 \pmod 3$. In this case $(X - Y_2^2, X^2 + XY_2^2 + Y_2^4) = 1$, $DY_1 \not\equiv 0 \pmod 3$ and

$$X - Y_2^2 = d_1 Y_3^6\,, \quad X^2 + XY_2^2 + Y_2^4 = d_2 Y_4^6\,,$$

where

$$d_1 d_2 = D,\ d_2 > 0,\ (2d_1Y_3, d_2Y_4) = 1,$$
$$Y_1 = Y_3Y_4 \not\equiv 0 \pmod 3),\ (X, Y_2Y_3Y_4) = 1,\ (Y_2, d_2) = 1\,.$$

Substitution of X from the first equation into the second gives

$$3Y_2^4 + 3d_1Y_2^2Y_3^6 + d_1^2Y_3^{12} = d_2Y_4^6\,. \tag{10}$$

Observe first that the following conditions are necessary for (10) to be solvable:

(a) $(d_2, d_1) \equiv (1,1), (1,7), (1,8), (4,2), (4,4), (4,7), (7,1), (7,4), (7,5) \pmod 9$,

(b) $\left(\dfrac{3d_2}{p}\right) = 1$, for every odd prime divisor p of d_1,

(c) $p \equiv 1 \pmod 3$ for every odd prime divisor p of d_2.

Note that in our example with $k = -35$, only equation (8) is left to treat, and accordingly we take $D = 16 \cdot 35$. It is straightforward to check that the first condition above is satisfied for no pair (d_2, d_1) which means that (8) is impossible whenever $x \not\equiv y_2^2 \pmod 3$.

Case (ii): $X - Y_2^2 \equiv 0 \pmod 3$. In this case let

$$3^\tau || D \quad \text{and} \quad \nu = \begin{cases} 5 & \text{if } \tau = 0, \\ 6 & \text{if } \tau = 1, \\ \tau - 1 & \text{if } \tau \geq 2. \end{cases}$$

It is easy to see that

$$X - Y_2^2 = 3^\nu d_1 Y_3^6, \quad X^2 + XY_2^2 + Y_2^4 = 3d_2 Y_4^6$$

with

$$d_1 d_2 = 3^{-\tau} D, \quad d_2 > 0, \quad Y_1 = 3^{\frac{\nu+1-\tau}{6}} Y_3 Y_4,$$

and where

$$(2d_1 Y_3, d_2 Y_4) = 1, \quad (X, 3^{\nu+1-\tau} Y_2 Y_3 Y_4) = 1, \quad (Y_2, d_2) = 1\,.$$

Substitution of X from the first equation into the second gives

$$Y_2^4 + 3^\nu d_1 Y_2^2 Y_3^6 + 3^{2\nu-1} d_1^2 Y_3^{12} = d_2 Y_4^6\,. \tag{11}$$

Necessary conditions for the solvability of (11) are the following:

(a) $\left(\dfrac{d_2}{p}\right) = 1$ for every odd prime divisor p of d_1,

(b) $p \equiv 1 \pmod 3$ for every odd prime divisor p of d_2.

In the case $k = -35$, $D = 16 \cdot 35$, we have $\tau = 0$, $\nu = 5$, and the conditions above are satisfied by no pair (d_2, d_1) except for $(d_2, d_1) = (1, 16 \cdot 35)$, for which equation (11) has an obvious solution and hence cannot be excluded by congruence considerations.

To proceed further, however, we factor (11) over $\mathbb{Q}(\omega)$, where $\omega^2 + \omega + 1 = 0$, obtaining (for all values of k):

$$Y_2^2 + 3^{\nu-1} d_1 (2 + \omega) Y_3^6 = (m + n\omega)(a + b\omega)^6, \quad m, n, a, b \in \mathbb{Z}, \tag{12}$$

where

$$m^2 - mn + n^2 = d_2\,, \quad a^2 - ab + b^2 = |Y_4|\,,\ (a, b) = 1\,.$$

Moreover, if $\tau \neq 2$ we can assume without loss of generality that

$$m \not\equiv 0,\ n \equiv 0 \pmod 3 \quad \text{and} \quad ab \text{ is odd with } a + b \not\equiv 0 \pmod 3\,.$$

From (12), on equating coefficients of ω, 1, we obtain

$$\begin{aligned} F_1(a, b) &= 3^{\nu-1} d_1 Y_3^6, \\ F_2(a, b) &= Y_2^2, \end{aligned} \tag{13}$$

where

$$\begin{aligned} F_1(a, b) = {} & na^6 + 6(m - n)a^5 b - 15ma^4 b^2 + 20na^3 b^3 \\ & + 15(m - n)a^2 b^4 - 6mab^5 + nb^6, \\ F_2(a, b) = {} & (m - 2n)a^6 - 6(2m - n)a^5 b + 15(m + n)a^4 b^2 + 20(m - 2n)a^3 b^3 \\ & - 15(2m - n)a^2 b^4 + 6(m + n)ab^5 + (m - 2n)b^6\,. \end{aligned}$$

In our case $k = -35$, we have $d_2 = 1$, so $n = 0$, and equation (13) becomes

$$\frac{ab(a-b)}{2}\,\frac{(a+b)(2a-b)(a-2b)}{2} = \pm 2^2 \cdot 3^3 \cdot 35 Y_3^6$$

where the two factors on the left-hand side are relatively prime. Putting $a/b = u \in \mathbb{Q}$ we obtain

(14) $$u(u-1) = 2c_1 w_1^3\,, \quad (u+1)(2u-1)(u-2) = 2c_2 w_2^3\,, \quad w_1, w_2 \in \mathbb{Q}\,,$$

where c_1, c_2 are relatively prime positive integers with $c_1c_2 = 140$. It is easily checked that for every such pair (c_1, c_2) at least one of the elliptic curves at (14) is of zero rank, from which we easily conclude that equation (8) is impossible in case (ii).

Mutatis mutandis, for the remaining values of k of this subsection, namely

$$k = -43, -21, 31$$

(as well as for $k = -972$, the example considered by Coombes and Grant [6]), the set $\mathcal{S}(k)$ contains equations that are either impossible or possess only trivial solutions.

2.2.2. Congruences on elliptic curves with application to $k = -29, -25$

If an equation in the set $\mathcal{S}(k)$ is everywhere locally solvable, yet is suspected of having no rational solution, we can in some instances still prove impossibility by elementary means using the following trick involving congruences with points on elliptic curves. For the remaining values of k in the range $|k| \le 50$, this applies to $k = -29, -25$ (see also $k = -15$ in section 4.4).

The set $\mathcal{S}(-25)$ comprises two equations of type I and two equations of type II. Three out of the four equations correspond to a zero rank elliptic curve E_i at (6) for either $i = 1$ or $i = 2$. Only the equation $5y_1^6 + 5y_2^6 = 2x^3$ remains. It is not difficult to prove that this equation is everywhere locally solvable. However, according to our general discussion at the beginning of section 2, a solution (x, y_1, y_2) $(y_1y_2 \neq 0)$ gives rise to a point $Q_1 = (10x/y_1^2, 50y_1^3/y_2^3)$ on $E_1 := \left[\,0,0,0,0,-4\cdot 5^4\,\right]$. This elliptic curve has rank 1, with $E_1(\mathbb{Q})$ generated by the point $P = (50, 350)$ of infinite order. Let $Q_1 = n \cdot P$. It is easily checked that

$$n \cdot P \equiv \mathcal{O}, (7, \pm 6), (42, \pm 6), (37, \pm 6) \pmod{43}\,.$$

Since the second coordinate of Q_1 equals $50y_1^3/y_2^3$, and the congruence

$$50Y^3 \equiv \pm 6 \pmod{43}$$

is impossible, we conclude that the only possibility is $Q_1 \equiv \mathcal{O} \pmod{43}$. This means that y_2 is divisible by 43, and consequently

$$5y_1^6 \equiv 2x^3 \pmod{43},$$

which is possible only if y_1 is divisible by 43; this contradicts the fact that y_1, y_2 are relatively prime.

The case $k = -29$ can be treated in complete analogy. The set $\mathcal{S}(-29)$ contains exactly three equations, two of which furnish a zero rank elliptic curve E_i. Only the equation $16y_1^6 + 29y_2^6 = x^3$ remains, which is everywhere locally solvable. A solution (x, y_1, y_2) gives a point Q_2 on $E_2 := \left[\,0,0,0,0,-16\cdot 29^3\,\right]$ of rank one and generator

$$P = (33085897/606^2, 129969272827/606^3)\,.$$

The relation $Q_2 = (29x/y_1^2, 29y_2^3/y_1^3) = n \cdot P$ is proven impossible as above, working modulo 19.

3. Application of elliptic Chabauty

In the range $|k| \leq 50$ we are left with the following values

$$k = -47, -39, -28, -15, -11, 3, 10, 15, 17, 24, 35, 43, 48\,. \tag{15}$$

A natural approach to equation (4) is to factorize it over the field $K = \mathbb{Q}(\theta)$, where $\theta^3 = k$. The maximal order $\mathcal{O}_K$ of K has one fundamental unit $\epsilon(\theta)$ which we normalize by sign to satisfy $\epsilon(k^{1/3}) > 0$ for the real cube root $k^{1/3}$ of k. For $k \not\equiv \pm 1 \pmod 9$, the ideal $\langle 3 \rangle$ factors as $\langle 3 \rangle = \mathfrak{p}_3^3$; and when $k \equiv \pm 1 \pmod 9$, then $\langle 3 \rangle = \mathfrak{p}_3 \mathfrak{p}_3'^2$. We deduce from (4) the following ideal equations

$$\langle x^4 - \theta x^2 y^2 + \theta^2 y^4 \rangle = \mathfrak{c}\mathfrak{a}^2, \quad \langle x^2 + \theta y^2 \rangle = \mathfrak{c}\mathfrak{b}^2, \quad \langle z \rangle = \mathfrak{c}\mathfrak{a}\mathfrak{b} \tag{16}$$

for ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ of $\mathcal{O}_K$, where

$$\mathfrak{c} = \langle x^4 - \theta x^2 y^2 + \theta^2 y^4\,,\, x^2 + \theta y^2 \rangle = \langle x^2 + \theta y^2\,,\, 3\theta^2 \rangle\,.$$

If the highest power of every rational prime dividing k is odd, then

$$\mathfrak{c} = \begin{cases} \mathcal{O}_K & \text{if } k \not\equiv 8 \pmod 9, \\ \mathfrak{p}_3 \mathfrak{p}_3' & \text{if } k \equiv 8 \pmod 9. \end{cases}$$

If there exist rational primes whose highest power dividing k is 2 or 4, then $\mathfrak{c}$ is as before, times an ideal $\mathfrak{c}_0$ which is divisible only by prime ideals over such rational primes with exponents bounded by a small explicit integer.

In general, the equations at (16) are equivalent to a system of element equations

$$x^4 - \theta x^2 y^2 + \theta^2 y^4 = cw^2, \quad x^2 + \theta y^2 = cv^2, \quad z = cwv, \tag{17}$$

for finitely many $c \in K$. We focus on the quartic curve C defined by the first equation in (17). If this quartic represents an elliptic curve over K (so in practice, if we can find a solution (x, y, w) in K), then we seek points $(x/y, w/y^2)$ on the curve subject to the rationality condition $x/y \in \mathbb{Q}$. We make extensive use of the Magma routines (*inter alia*) `PseudoMordellWeilGroup`, with parameter `IndexBound:=2`, to compute a subgroup of odd finite index in $C(K)$, and `Chabauty` for computing the K-points on C with prescribed rationality condition.

As a characteristic example, consider $k = -28$. Here, $K = \mathbb{Q}(\theta)$ with $\theta^3 = -28$; the fundamental unit is $\epsilon = (-2 + 2\theta + \theta^2)/6$, the class number of $\mathcal{O}_K$ is 3 and we have four quartics C_i corresponding to $c = 1, \epsilon, 4 + \theta, \epsilon(4 + \theta)$, respectively. Both quartics C_2 and C_4 are unsolvable at the prime ideal $\langle 2, (4 + 2\theta + \theta^2)/6 \rangle$. For C_1, Magma routines show that there are no solutions with $y \neq 0$. As for C_3, it has several points over K, the "simplest" one being

$$(x/y, w/y^2) = (-2, 6/(4 + \theta))\,.$$

`Chabauty` reveals $x/y = \pm 2$ as the only possibility with $y \neq 0$, which returns $(\pm X, \pm Y) = (2, 6)$ as the only finite points on (1). In an analogous manner, we solve equation (4) and hence (1) when $k = 3$, 10, 17, 24, 35, and 48; see the table in section 6. Note that these values of k do not cover the full list (15). Why not? This is discussed in sections 4 and 5.

4. The difficult cases $k = 15, 43, -11, -15$

We were unable to apply directly methods of the previous section for the values $k = -47, -39, -15, -11, 15, 43$. In most cases, for at least one value of c in (17), our machines were unable to compute the relevant Mordell-Weil groups over the cubic number field K. Oftentimes the Selmer bound on the rank was equal to 3, but at most one non-torsion point could be found, indicating the possible presence of a non-trivial Shafarevic-Tate group (of course, if the rank is actually equal to 3, then elliptic Chabauty arguments over a cubic number field must fail). It is possible that a standard descent could be carried out by hand in such cases, but the calculations are rather daunting. Such an example of Selmer rank bound 3 occurs for instance when $k = 15$ with $c = \epsilon = 1 - 30\theta + 12\theta^2$, $\theta^3 = 15$ (ϵ being a fundamental unit in $\mathbb{Q}(\theta)$). In such cases we also investigated the quartic cover obtained by eliminating x at (17), which results in the curve

$$cv^4 - 3\theta v^2 y^2 + \frac{3\theta^2}{c} y^4 = w^2. \tag{18}$$

Here, and in several other cases, the K-rank of the curve (18) could be computed exactly but turned out to equal 3 (and in one case, 4), so not strictly less than the degree of $\mathbb{Q}(\theta)$; hence `Chabauty` is not applicable.

We adopt an alternative approach, which is successful for four of the values, namely $k = 43, 15, -11, -15$. This approach involves factorization over an appropriate *quadratic* number field of the equation of type I, II, III, IV that is causing the difficulty.

4.1. Case $k = 15$

Here, the finite points are $(\pm 1, \pm 4)$, $(\pm 1/2, \pm 31/8)$.

We have to solve the equation $x^6 + 15y^6 = z^2$, and following the approach of section 2.2.1 we are left with solving each of the two equations

$$-5y_1^6 + 3y_2^6 = 2x^3, \quad y_1, y_2 \text{ odd}, \quad (5y_1, 3y_2) = 1 \tag{19}$$

and

$$-16y_1^6 + 15y_2^6 = x^3, \quad (2y_1, 15y_2) = 1. \tag{20}$$

We work in $K = \mathbb{Q}(\phi)$, $\phi^2 = 15$, with maximal order $\mathcal{O}_K$. The ideal $\langle 2 \rangle = \mathfrak{p}_2^2$, $\mathfrak{p}_2 = \langle 2, 1+\phi \rangle$, and the ideal classgroup of $\mathcal{O}_K$ is of order 2, generated by $\mathfrak{p}_2$. We have $\langle 3 \rangle = \mathfrak{p}_3^2$, $\mathfrak{p}_3 = \langle 3, \phi \rangle$; $\langle 5 \rangle = \mathfrak{p}_5^2$, $\mathfrak{p}_5 = \langle 5, \phi \rangle$. A fundamental unit is $\epsilon = 4 - \phi$.

4.1.1. Equation (19)

We have

$$(y_1^3\phi + 3y_2^3)(y_1^3\phi - 3y_2^3) = -6x^3,$$

and the gcd of the two factors on the left is precisely $\mathfrak{p}_2\mathfrak{p}_3 = \langle -3 + \phi \rangle$. Thus

$$\langle y_1^3\phi + 3y_2^3 \rangle = \langle -3 + \phi \rangle \mathcal{A}^3,$$

for an ideal $\mathcal{A}$ prime to $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$ of $\mathcal{O}_K$. Since $\mathcal{A}^3$ is principal and the class-number of K is 2, $\mathcal{A}$ is principal. So there exists $y_3 \in \mathcal{O}_K$ satisfying

$$y_1^3\phi + 3y_2^3 = \epsilon^i(-3+\phi)y_3^3, \quad i = 0, \pm 1. \tag{21}$$

Equation (21) represents a curve of genus 1 over K, which is locally unsolvable at $\mathfrak{p}_3$ when $i = 1$; further, since $\epsilon^{-1}(-3+\phi) = (3+\phi)$, the curve with $i = -1$ is simply the conjugate of the curve with $i = 0$. It suffices therefore to find all points with rational $y_1 : y_2$ on

$$y_1^3\phi + 3y_2^3 = (-3+\phi)y_3^3, \tag{22}$$

which is an elliptic curve since it possesses the point $(y_1, y_2, y_3) = (1, -1, 1)$. The Magma routine `PseudoMordellWeilGroup` tells us that the curve has rank 3 over K, however, exceeding the degree of K, and so we cannot directly use the elliptic Chabauty method and Magma's relevant routines. We overcome this difficulty as follows. In (22), put $y_3 = a + b\phi$, where $(a, 15) = 1$, $a + b \equiv 1 \pmod 2$, and where, changing the sign of each y_i if necessary, we may assume $a \equiv 1 \pmod 3$. Then

$$\begin{cases} a^3 - 9a^2b + 45ab^2 - 45b^3 = y_1^3, \\ -a^3 + 15a^2b - 45ab^2 + 75b^3 = y_2^3, \end{cases} \tag{23}$$

defining rational elliptic curves of rank 1, 2, respectively. The cubics at (23) factor over the field $L = \mathbb{Q}(\psi)$, $\psi^3 - 3\psi + 8 = 0$. A fundamental unit in the ring of integers $\mathcal{O}_L = \mathbb{Z}[1, \psi, \psi^2]$ is $\eta = 5 + 2\psi$. We have $\langle 2\rangle = \mathfrak{P}_2\mathfrak{P}_2'^2$ with $\mathfrak{P}_2 = \langle 2, \psi\rangle$, $\mathfrak{P}_2' = \langle 2, 1+\psi\rangle$; $\langle 3\rangle = \mathfrak{P}_3^3$ with $\mathfrak{P}_3 = \langle 3, 2+\psi\rangle$; and the classgroup is of order 3 generated by $\mathfrak{P}_2$, with $\mathfrak{P}_2^3 = \langle\psi\rangle$. From (23),

$$\begin{cases} (a + (\psi^2+\psi-5)b)(a^2 + (-\psi^2-\psi-4)ab + (3\psi^2-3\psi+9)b^2) = y_1^3, \\ (a + (-\psi^2+\psi-3)b)(a^2 + (\psi^2-\psi-12)ab + (-5\psi^2-5\psi+25)b^2) = -y_2^3. \end{cases}$$

By the assumptions on a, b, it is straightforward to verify in each equation that the two factors on the left, considered as principal ideals, are coprime, and hence equal to ideal cubes. Now an ideal equation $\langle u\rangle = \mathcal{B}^3$ implies one of the principal ideal equations

$$\langle u\rangle = \langle v\rangle^3, \quad \langle\psi^2\rangle\langle u\rangle = \langle v\rangle^3, \quad \langle\psi\rangle\langle u\rangle = \langle v\rangle^3,$$

according as $\mathcal{B} \sim 1, \mathfrak{P}_2, \mathfrak{P}_2^2$. So without loss of generality we deduce element equations

$$\begin{cases} \psi^{i_1}(a + (\psi^2+\psi-5)b) = \eta^{j_1}c_1^3, \\ \psi^{i_2}(a^2 + (-\psi^2-\psi-4)ab + (3\psi^2-3\psi+9)b^2) = \eta^{-j_1}c_2^3, \end{cases} \tag{24}$$

with $i_1 + i_2 \equiv 0 \pmod 3$, $j_1 = 0, \pm 1$, and

$$\begin{cases} \psi^{i_3}(a + (-\psi^2+\psi-3)b) = \eta^{j_2}c_3^3, \\ \psi^{i_4}(a^2 + (\psi^2-\psi-12)ab + (-5\psi^2-5\psi+25)b^2) = \eta^{-j_2}c_4^3, \end{cases} \tag{25}$$

with $i_3 + i_4 \equiv 0 \pmod 3$, $j_2 = 0, \pm 1$; and c_i, $i = 1, \ldots, 4$, in $\mathcal{O}_L$.

We denote the $\mathfrak{P}_3$-adic (additive) valuation of an element $\alpha \in \mathcal{O}_L$ by $\nu(\alpha)$, the highest power of $\mathfrak{P}_3$ dividing $\langle\alpha\rangle$, and for reference list here the valuations of certain elements of $\mathcal{O}_L$ (the coefficients of the polynomials occurring at equations (24), (25)):

$$\nu(\psi^2+\psi-5)=2, \quad \nu(-\psi^2-\psi-4)=2, \quad \nu(3\psi^2-3\psi+9)=4,$$

$$\nu(-\psi^2+\psi-3)=1, \quad \nu(\psi^2-\psi-12)=1, \quad \nu(-5\psi^2-5\psi+25)=2;$$

further,

$$\nu(\eta-1)=1, \quad \nu(\psi-1)=1,$$

so that $\psi^3 \equiv 1 \pmod 3$. Thus (24) and (25) imply that $c_i^3 \equiv 1 \pmod{\mathfrak{P}_3}$, $i=1,\ldots,4$, so that $c_i \equiv 1 \pmod{\mathfrak{P}_3}$, whence $c_i^3 \equiv 1 \pmod 3$, $i=1,\ldots,4$. We consider the first equations at (24) and (25) modulo 3, distinguishing cases according as to the residue class of b modulo 3.

Subcase (i): $b \equiv 0 \pmod 3$. Then

$$\psi^{i_1} \equiv \eta^{j_1}, \quad \psi^{i_3} \equiv \eta^{j_2},$$

which forces $(i_1,i_3,j_1,j_2)=(0,0,0,0)$, and $(i_2,i_4)=(0,0)$.

Subcase (ii): $b \equiv 1 \pmod 3$. Then

$$\psi^{i_1}(\psi^2+\psi-4)=\eta^{j_1}, \quad \psi^{i_3}(-\psi^2+\psi-2)=\eta^{j_2},$$

which forces $(i_1,i_3,j_1,j_2)=(1,2,2,2)$ and $(i_2,i_4)=(2,1)$.

Subcase (iii): $b \equiv -1 \pmod 3$. Then

$$\psi^{i_1}(-\psi^2-\psi+6))=\eta^{j_1}, \quad \psi^{i_3}(\psi^2-\psi+4))=\eta^{j_2},$$

which forces $(i_1,i_3,j_1,j_2)=(2,0,1,2)$ and $(i_2,i_4)=(1,0)$.

Consequently, when we form the following equation using factors from (24), (25),

$$\begin{aligned}\psi^{i_1+i_4}(a+(\psi^2+\psi-5)b)(a^2&+(\psi^2-\psi-12)ab\\ &+(-5\psi^2-5\psi+25)b^2)=\eta^{j_1-j_2}c^3,\end{aligned}$$

we have the three possibilities:

$$\begin{cases}(a+(\psi^2+\psi-5)b)(a^2+(\psi^2-\psi-12)ab+(-5\psi^2-5\psi+25)b^2)=c^3,\\ \psi^2(a+(\psi^2+\psi-5)b)(a^2+(\psi^2-\psi-12)ab+(-5\psi^2-5\psi+25)b^2)=c^3,\\ \psi^2(a+(\psi^2+\psi-5)b)(a^2+(\psi^2-\psi+12)ab+(-5\psi^2-5\psi+25)b^2)=\eta^{-1}c^3,\end{cases}$$

each representing an elliptic curve over L having no L-torsion and of rank 2 over L. Note that now the rank is less than the degree of L which permits us to *attempt* the elliptic Chabauty method using the Magma routines. And indeed, these routines show the following. The only point with rational $a:b$ on the first curve is when $a:b=1:0$, returning $(X,Y)=(1,4)$ on (1). Further, there are no such points on the second and third curves.

4.1.2. Equation (20)

We have

$$(y_2^3\phi + 4y_1^3)(y_2^3\phi - 4y_1^3) = x^3,$$

and the two factors on the left are coprime, so that

$$\langle y_2^3\phi + 4y_1^3\rangle = \mathcal{A}^3,$$

for some ideal $\mathcal{A}$ prime to $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$ of $\mathcal{O}_K$. Then as above, there exists $y_3 \in \mathcal{O}_K$ satisfying

$$y_2^3\phi + 4y_1^3 = \epsilon^i y_3^3, \quad i = 0, \pm 1. \tag{26}$$

Equation (26) is not locally solvable at $\mathfrak{p}_3$ when $i = 0$, and the curves corresponding to $i = \pm 1$ are conjugate; so it suffices to consider only the case $i = 1$:

$$y_2^3\phi + 4y_1^3 = (4 - \phi)y_3^3, \tag{27}$$

which is an elliptic curve since it possesses the point $(y_1, y_2, y_3) = (1, -1, 1)$. The K-rank of the curve is 3.

In (27), put $y_3 = a + b\phi$, with $(a, 15) = 1$, $a + b \equiv 1 \pmod 2$, and where, without loss of generality, $a \equiv 1 \pmod 3$, to give

$$\begin{cases} -a^3 + 12a^2b - 45ab^2 + 60b^3 = y_2^3, \\ 4a^3 - 45a^2b + 180ab^2 - 225b^3 = 4y_1^3, \end{cases} \tag{28}$$

defining rational elliptic curves of ranks 2, 1, respectively. Note that the second equation implies $b(a^2 + b^2) \equiv 0 \pmod 4$, so that necessarily a is odd, $b \equiv 0 \pmod 4$.

In (28) we factor over L:

$$\begin{cases} (a + (\psi - 4)b)(a^2 + (-\psi - 8)ab + (\psi^2 + 4\psi + 13)b^2) = -y_2^3, \\ (a + \frac{1}{4}(-\psi^2 - 4\psi - 13)b)(a^2 + \frac{1}{4}(\psi^2 + 4\psi - 32)ab + \frac{15}{4}(-\psi + 4)b^2) = y_1^3, \end{cases}$$

and again in each equation the two factors on the left, considered as principal ideals, are coprime and hence ideal cubes. Just as above, we deduce element equations

$$\begin{cases} \psi^{i_1}(a + (\psi - 4)b) = \eta^{j_1}c_1^3, \\ \psi^{i_2}(a^2 + (-\psi - 8)ab + (\psi^2 + 4\psi + 13)b^2) = \eta^{-j_1}c_2^3, \end{cases} \tag{29}$$

with $i_1 + i_2 \equiv 0 \pmod 3$, $j_1 = 0, \pm 1$, and

$$\begin{cases} \psi^{i_3}(a + \frac{1}{4}(-\psi^2 - 4\psi - 13)b) = \eta^{j_2}c_3^3, \\ \psi^{i_4}\big(a^2 + \frac{1}{4}(\psi^2 + 4\psi - 32)ab + \frac{15}{4}(-\psi + 4)b^2\big) = \eta^{-j_2}c_4^3, \end{cases} \tag{30}$$

with $i_3 + i_4 \equiv 0 \pmod 3$, $j_2 = 0, \pm 1$, and c_i, $i = 1, \ldots, 4$, in $\mathcal{O}_L$.

We have the following valuations:

$$\nu(\psi - 4) = 1, \quad \nu(-\psi - 8) = 1, \quad \nu(\psi^2 + 4\psi + 13) = 2,$$
$$\nu(\psi^2 + 4\psi - 32) = 2, \quad \nu(15(-\psi + 4)) = 4,$$

so that as before, $c_i^3 \equiv 1 \pmod 3$. We consider modulo 3 the first equations in (29) and (30), distinguishing cases according as to the residue class of b modulo 3.

Subcase (i): $b \equiv 0 \pmod 3$. Then

$$\psi^{i_1} \equiv \eta^{j_1}, \quad \psi^{i_3} \equiv \eta^{j_2},$$

forcing $(i_1, i_3, j_1, j_2) = (0, 0, 0, 0)$ and $(i_2, i_4) = (0, 0)$.

Subcase (ii): $b \equiv 1 \pmod 3$. Then

$$\psi^{i_1}(\psi - 3) = \eta^{j_1}, \quad \psi^{i_3}(-\psi^2 - 4\psi - 9) = \eta^{j_2},$$

forcing $(i_1, i_3, j_1, j_2) = (2, 2, 0, 1)$ and $(i_2, i_4) = (1, 1)$.

Subcase (iii): $b \equiv -1 \pmod 3$. Then

$$\psi^{i_1}(-\psi + 5) = \eta^{j_1}, \quad \psi^{i_3}(\psi^2 + 4\psi + 17)) = \eta^{j_2},$$

forcing $(i_1, i_3, j_1, j_2) = (0, 1, 1, 2)$ and $(i_2, i_4) = (0, 2)$.

Consequently, when we form the equation below using factors from (29), (30),

$$\psi^{i_1+i_4}\big(a + (\psi - 4)b\big)\left(a^2 + \tfrac{1}{4}(\psi^2 + 4\psi - 32)ab + \tfrac{15}{4}(-\psi + 4)b^2\right) = \eta^{j_1 - j_2} c^3,$$

we have the three possibilities:

$$\begin{cases} (a + (\psi - 4)b)\big(a^2 + \frac{1}{4}(\psi^2 + 4\psi - 32)ab + \frac{15}{4}(-\psi + 4)b^2\big) = c^3, \\ (a + (\psi - 4)b)(a^2 + \frac{1}{4}(\psi^2 + 4\psi - 32)ab + \frac{15}{4}(-\psi + 4)b^2) = \eta^{-1}c^3, \\ \psi^2(a + (\psi - 4)b)(a^2 + \frac{1}{4}(\psi^2 + 4\psi - 32)ab + \frac{15}{4}(-\psi + 4)b^2) = \eta^{-1}c^3, \end{cases}$$

again each representing an elliptic curve of rank 2 over L. Working 13-adically, having shown that the group index is prime to 3 (actually we need it prime to 6, but the construction of the routine `PseudoMordellWeilGroup` guarantees that the index is odd), we find that the first curve has a point with rational $a : b$ only at $a : b = 1 : 0$, returning $(X, Y) = (-1/2, 31/8)$. Working 13-adically, with auxiliary prime 43, we find there are no points with rational $a : b$ on the second curve (where we needed to show the group index is prime to 3); and working 13-adically, with auxiliary prime 17, we find there are no points with rational $a : b$ on the third curve (where we needed to show the group index is prime to 3). In summary, the only finite points on (1) are given by $(\pm X, \pm Y) = (1, 4), (1/2, 31/8)$.

4.2. Case $k = 43$

Here, the finite points are $(\pm 3/2, \pm 59/9)$, $(\pm 7/3, \pm 386/27)$.

This case is similar to the previous one. The set $S(43)$ derived in section 2.2 contains the three globally solvable equations:

$$2x^3 = -y_1^6 + 43y_2^6, \quad x^3 = -16y_1^6 + 43y_2^6, \quad x^3 = -688y_1^6 + y_2^6. \tag{31}$$

We factor the first two equations over the field $\mathbb{Q}(\phi)$, where $\phi^2 = 43$. As before, we are led to working in a cubic field $\mathbb{Q}(\psi)$, where now $\psi^3 - \psi^2 + \psi - 9 = 0$. In analogy to the equations at the end of sections 4.1.1 and 4.1.2, we obtain the equations:

$$\begin{aligned}\big((-\psi^2-\psi-3)a+(6\psi^2+6\psi+17)b\big)\\ \times\Big((-10\psi^2-13\psi-34)a^2+(124\psi^2+163\psi+417)ab\\ +(-387\psi^2-516\psi-1290)b^2\Big)\\ =\epsilon^\ell(-\psi^2+\psi+3)(2-\psi)^2c^3,\end{aligned}$$

where $\ell=0,1,2$, and

$$\begin{aligned}\big((5\psi^2+6\psi+20)a+\tfrac{1}{2}(-\psi^2-2\psi-5)b\big)\\ \times\Big(\tfrac{1}{2}(-\psi^2-4\psi-5)a^2+\tfrac{1}{2}(\psi^2-2\psi+1)ab-b^2\Big)\\ =\tfrac{1}{2}(-5\psi^2+4\psi+17)\epsilon^\ell c^3,\end{aligned}\tag{32}$$

where $\ell=0,1,2$. Just as before, these equations are amenable to the computer routines, and deliver precisely the two known finite solutions. It is worth mentioning that the relevant Mordell-Weil group on this latter curve of rank 2 over $\mathbb{Q}(\psi)$ could not be computed directly with Magma because of the large height of one of the generators: the generators on (32) may be taken as $(a,b,c)=(0,-7\psi+16,1)$ and

$$\begin{aligned}(a,b,c)=\\ \Big(\tfrac{1}{2}(-24963589\psi^2+48373018\psi+20008291),\\ 18015880\psi^2-132297936\psi+209249791,\\ 31418694\psi^2+46376736\psi+127224108\Big).\end{aligned}$$

It was necessary to consider a 3-isogenous curve where by luck the relevant group could be computed directly. This gives rise to a full rank subgroup on (32), successfully feeding into the `Chabauty` routine.

For the third equation in (31), the solution is accomplished by the elementary methods of section 2.2.

4.3. Case $k=-11$

Here, the finite points are $(\pm 3/2,\pm 5/8)$.

We have to solve $x^6-11y^6=z^2$, where $x,11y,z$ are pairwise relatively prime. Following the approach of (2.2.1), we are left with solving

$$x^3=16y_1^6+11y_2^6,\tag{33}$$

where $y=2y_1y_2$ and $(2y_1,11y_2)=1$. Considering equation (33) modulo 9 shows that, if either y_1 or y_2 is divisible by 3, then both y_1 and y_2 are divisible by 3, a contradiction; hence $y_1y_2\not\equiv 0 \pmod 3$. We factorize equation (33) as

$$\left(4y_1^3+\sqrt{-11}y_2^3\right)\left(4y_1^3-\sqrt{-11}y_2^3\right)=x^3,$$

where the two factors on the left hand side are coprime in the ring of integers of $\mathbb{Q}\left(\sqrt{-11}\right)$, a field of class number 1. It follows that

$$4y_1^3+\sqrt{-11}y_2^3=\left(a+b\,\frac{(1+\sqrt{-11})}{2}\right)^3$$

with $a, b \in \mathbb{Z}$, and hence that

$$b(3a^2 - 3ab - 2b^2) = 2y_2^3, \quad (2a - b)(a^2 - ab - 8b^2) = (2y_1)^3 \tag{34}$$

with $(a, b) = 1$. These equations define elliptic curves of ranks 2 and 1, respectively. Note that the second equation modulo 9 shows that $b \not\equiv 0 \pmod 3$.

Since $(b, 3a) = 1$, the two factors on the left-hand side of the first equation at (34) are coprime. We also have

$$(2a - b, a^2 - ab - 8b^2) = (2a - b, 33) = 1,$$

since $(y_1, 33) = 1$. It follows that

$$b = 2^i \times \text{cube}, \quad 3a^2 - 3ab - 2b^2 = 2^{1-i} \times \text{cube} \ \ (i = 0, 1),$$

$$2a - b = \text{cube}, \quad a^2 - ab - 8b^2 = \text{cube}.$$

If $i = 1$, then we deduce

$$b = 2\beta^3, \quad 2a - b = 8\alpha^3, \quad a^2 - ab - 8b^2 = \gamma^3,$$

so that

$$16\alpha^6 - 33\beta^6 = \gamma^3.$$

This is an equation of type (5), and taking $(A, B) = (16, -33)$, we discover that the corresponding elliptic curve E_3 at (7) has rank 0; and no solutions arise for a, b. Thus $i = 0$, and we have

$$\begin{aligned} & b = \text{cube}, \quad 2a - b = \text{cube}, \\ & a^2 - ab - 8b^2 = \text{cube}, \quad 3a^2 - 3ab - 2b^2 = 2 \times \text{cube}. \end{aligned} \tag{35}$$

Note that, in the above equations, $a^2 - ab - 8b^2$ is not divisible by 11 because it is a factor of y_1. Also, $3a^2 - 3ab - 2b^2$ is not divisible by 11 for, otherwise, it would be divisible by 11^2, which implies $b \equiv 0 \pmod{11}$, hence also $a \equiv 0 \pmod{11}$, a contradiction. These observations will be needed below, when we calculate greatest common divisors.

We work in the field $\mathbb{Q}(\xi)$, $\xi^2 - \xi - 8 = 0$. The class-number is 1, a fundamental unit is $\eta = 19 + 8\xi$, and we have the prime factorization $2 = (2 + \xi)(-3 + \xi)$.

The latter two equations in (35) may be written as follows:

$$\begin{aligned} & (a - \xi b)\ (a + (-1 + \xi)b) = \text{cube}, \\ & ((5 + 2\xi)a + (2 + \xi)b)((7 - 2\xi)a + (3 - \xi)b) = 2 \times \text{cube}. \end{aligned}$$

The greatest common divisor

$$(a - \xi b, a + (-1 + \xi)b) = (a - \xi b, 1 - 2\xi) = (a - \xi b, \sqrt{33}) = 1,$$

since $(y_2, 33) = 1$. Thus

$$a - \xi b = \eta^j \times \text{cube}, \quad a + (-1 + \xi)b = \eta^{-j} \times \text{cube}, \quad j = 0, \pm 1.$$

Further, the greatest common divisor

$$\begin{aligned} & ((5 + 2\xi)a + (2 + \xi)b, (7-2\xi)a + (3 - \xi)b) \\ & \qquad = ((5 + 2\xi)a + (2 + \xi)b, 1 - 2\xi) = 1, \end{aligned}$$

as before. Thus

$$(5+2\xi)a + (2{+}\xi)b = \eta^k\,\pi \times \text{cube},$$
$$(7-2\xi)a + (3-\xi)b = \eta^{-k}\,\bar{\pi} \times \text{cube}, \quad k = 0, \pm 1,$$

for π and $\bar{\pi}$ equal to the two prime factors of 2. Summing up, we have

$$b = \text{cube}, \quad 2a - b = \text{cube},$$
$$a + (-1+\xi)b = \eta^{-j} \times \text{cube}, \quad (5+2\xi)a + (2+\xi)b = \eta^k\,\pi \times \text{cube},$$

for $\pi = 2+\xi$ or $-3+\xi$. We form the elliptic cubic

$$b\,(a + (-1+\xi)b)\,((5+2\xi)a + (2+\xi)b) = \eta^\ell\,\pi \times \text{cube}, \quad \ell = -j + k,$$

where without loss of generality, $\ell = 0, \pm 1$.

Consider first $\pi = 2+\xi$. For each value of $\ell = 0, \pm 1$, the corresponding elliptic curve has rank 1 over $\mathbb{Q}(\xi)$, and we can apply the elliptic Chabauty method. For $\ell = 0$, we find that the only solutions are $a:b = 1:0\,, -7:3$ which are rejected in view of (34). For $\ell = 1$, the only solutions are $a:b = 1:0\,,\ 0:1$ and only the second satisfies (34), giving $y_1 = 1, y_2 = -1$, hence $y = -2, x = 3, z = \pm 5$, which returns the points $(\pm X, \pm Y) = (3/2, 5/8)$ on (1). For $\ell = -1$, the only solution is $a:b = 1:0$ which is rejected in view of (34).

Second, take $\pi = 3-\xi$. Again, each $\ell = 0, \pm 1$ results in a rank 1 elliptic curve. If $\ell = 0$, application of `Chabauty` shows the only solutions to be $a:b = 1:0\,, 1:1$. In view of (34) the first is rejected, and the second gives $y_1 = -1, y_2 = -1$, hence $y = 2, x = 3, z = \pm 5$, again returning the points $(\pm X, \pm Y) = (3/2, 5/8)$ on (1). If $\ell = 1$, the only solutions are $a:b = 1:0\,, 10:3$ which by (34) we reject. If $\ell = -1$, the only solutions are $a:b = 1:0$, which by (34) we reject.

4.4. Case $k = -15$

Here, the finite points are $(\pm 2, \pm 7)$.

We have to solve $x^6 - 15y^6 = z^2$, where $x, 15y, z$ are pairwise relatively prime. Following the approach of section 2.2.1, we are left with solving the pair of equations

$$80y_1^6 + 3y_2^6 = x^3\,, \qquad (10y_1, 3y_2) = 1,\ \ y = 2y_1y_2, \tag{36}$$

and

$$y_1^6 + 15y_2^6 = 2x^3\,, \qquad (y_1, 15y_2) = 1,\ \ y_1y_2 \text{ odd}\,. \tag{37}$$

To deal with (36), we use ideas of section 2.2.2. On the corresponding curve

$$E_1 : Y^2 = X^3 - 375, \qquad (X, Y) = \left(\frac{5x}{y_2^2}\,, \frac{100y_1^3}{y_2^3}\right),$$

the torsion is trivial, the rank is 1, and a generator P is given by $P = (10, 25)$. We check that if $n \equiv 1, 2, 4, 5 \pmod 6$ then the Y-coordinate of $n \cdot P$ has odd numerator and denominator. Indeed, for $n = 1, 2, 4, 5$ this is straightforward; further, a symbolic computation shows that if we add to $6 \cdot P$ a point $(u/t^2, v/t^3)$, where u, v, t are integers with vt odd, then the resulting point has Y-coordinate with odd numerator and denominator. Hence for $n \equiv 1, 2, 5, 6 \pmod 6$, the Y-coordinate of $n \cdot P$ cannot have the required shape $100y_1^3/y_2^3$ with y_2 odd. It remains to check the cases $n \equiv 0, 3 \pmod 6$. But if n is a multiple of 3, the following are the possibilities for the Y-coordinate of

$n \cdot P$: either it is congruent to ± 9 modulo 19, or its denominator is divisible by 19. The first alternative is impossible because it implies that $100(y_1/y_2)^3 \equiv \pm 9 \pmod{19}$; and the second implies $y_2 \equiv 0 \pmod{19}$, but then the initial equation $80y_1^6 + 3y_2^6 = x^3$ is impossible modulo 19 when $(y_1, y_2) = 1$.

Now we focus our attention on equation (37). We work in the field $\mathbb{Q}(\theta)$, where $\theta^2 + \theta + 4 = 0$, with class-number 2 and integral basis $1, \theta$. We have the ideal factorizations

$$\langle 2 \rangle = \mathfrak{p}_2 \mathfrak{p}_2' , \quad \mathfrak{p}_2 = \langle 2, 1+\theta \rangle , \quad \mathfrak{p}_2' = \langle 2, 2+\theta \rangle .$$

The ideal-class $\mathfrak{p}_2$ generates the classgroup, and $\mathfrak{p}_2^2 = \langle 1+\theta \rangle$. After an appropriate choice of signs for y_1, y_2, the ideal factorization of (37) implies without loss of generality

$$\langle y_1^3 + (2\theta+1) y_2^3 \rangle = \mathfrak{p}_2 \mathfrak{a}^3$$

for some integral ideal $\mathfrak{a}$ such that $\mathfrak{p}_2 \mathfrak{a}$ is principal. This results in an equation

$$(\theta+1) y_1^3 + (\theta - 7) y_2^3 = y_3^3$$

for some $y_3 \in \mathbb{Z}[\theta]$, which represents an elliptic curve over $\mathbb{Q}(\theta)$ (note that it contains the point $(1, -1, 2)$). The $\mathbb{Q}(\theta)$-rank is 1, and Magma routines (but see the Remark below) show that $(y_1, y_2, y_3) = (1, -1, 2)$ is the only point over $\mathbb{Q}(\theta)$ with rational $y_1 : y_2$. This gives $y = -1$, and by (37), $x = 2$. Returning to (1), the only finite points are $(\pm X, \pm Y) = (2, 7)$.

Remark. We had to resort to setting `IndexBound:=3` in order for `Chabauty` to return a result. But it is straightforward to check that the subgroup (in this case, of rank 1) returned by `PseudoMordellWeilGroup` has index in the full Mordell-Weil group which is prime to 3.

5. The unsolved equations

In the considered range of k, we are left with $k = -47, -39$. If we try to apply the ideas of section 3, then relevant Mordell-Weil groups could not be computed. For example, at $k = -47$, $c = 1$, the quartic curve at (17) has Selmer rank 3, with only one point of infinite order found. The curve in (18) has K-rank 4. Trying to apply the ideas of section 4 for $k = -39$ leads to curves with bound on the rank 2, but where we are unable to find any points; and similar obstructions arise for $k = -47$. We have tried various further attacks on these equations, so far without success. It has been suggested to us that the computations of this paper be automated to extend the calculations for k in a range "somewhere in the thousands"; but without a mechanized 2-descent algorithm for elliptic curves over number fields, at the very least, even a range into the hundreds is well beyond our abilities. In exploring the unsolved cases of this section, we have resorted to much manual intervention in Magma programming, primarily choosing appropriate models for curves and their isogenies to replace the ones returned by the routine `EllipticCurve`, which can have huge coefficients, possibly greatly increasing the running time of the algorithms. When the number field has class-number exceeding 1, we know of no uniform method for choosing models that are potentially better suited as input to `PseudoMordellWeilGroup`.

For interest we searched the curves (1) for rational points with height at most 20000 in the range $|k| < 250000$. The maximum number of points found was 22, at $k = 1025$ with the finite points

$$(\pm X, \pm Y) \;=\; \Big(2,\,33\Big)\,,\; \left(\frac{1}{4},\frac{2049}{64}\right),\; \left(\frac{5}{2},\frac{285}{8}\right),\; \Big(8,\,513\Big)\,,\; \left(\frac{20}{91},\frac{24126045}{91^3}\right),$$

and at $k = 110160$, with finite points (all integral)

$$(\pm X, \pm Y) \;=\; (2,332),\; (3,333),\; (6,396),\; (9,801),\; (14,2764)\,.$$

The point of largest height that we observed in this range occurs for $k = -212860$, with point $(3866/427, 45259682826/427^3)$. Increasing the search range and decreasing the height bound finds the curve at $k = 7547408$ with 26 points, the finite points occurring at

$$\begin{aligned}(\pm X, \pm Y) = \Big(4,\,2748\Big)\,,\; \left(\frac{1}{6},\frac{593407}{6^3}\right),\; \left(\frac{7}{5},\frac{343407}{5^3}\right),\\ \Big(16,\,4932\Big)\,,\; \left(\frac{28}{3},\frac{77356}{3^3}\right),\; \left(\frac{139}{10},\frac{3841869}{10^3}\right).\end{aligned}$$

Note that the curve

$$y^2 = x^6 + \left(\frac{1}{4}a^{12} + 1\right)$$

automatically contains the points

$$(\pm X, \pm Y) = \left(\frac{1}{a^2},\frac{1}{a^2} + \frac{1}{2}a^6\right),\; \left(a, 1 + \frac{1}{2}a^6\right) \;\text{ and }\; \left(\frac{1}{2}a^4,\frac{1}{8}a^{12} + 1\right).$$

For the curve at $k = 2089$ only 14 points were found, but the (finite) points comprise

$$(\pm X, \pm Y) \;=\; \left(\frac{96}{11},\frac{886825}{11^3}\right),\; \left(\frac{162}{85},\frac{28389097}{85^3}\right) \;\text{ and }\; \left(\frac{289}{90},\frac{41143681}{90^3}\right),$$

remarkable for their large heights.

6. All rational solutions to (1) in the range $|k| \leq 50$

We summarize the computations of the previous sections in the following table, in which the $*$ symbol means that the given set of points has not been proved to be complete.

TABLE 6.1 All rational solutions $(\pm X, \pm Y)$ to $Y^2 = X^6 + k$, $1 \leq |k| \leq 50$.

k	Solutions	Ref. section	k	Solutions	Ref. section
-50	$\emptyset$	2.1	50	$\emptyset$	2.1
-49	$\emptyset$	2.2	49	$(0,7)$	2.1
-48	$(2,4)$	2.2	48	$(1,7)$	3
-47	$\left(\frac{63}{10},\frac{249953}{1000}\right)^*$	5	47	$\emptyset$	2.2
-46	$\emptyset$	2.1	46	$\emptyset$	2.2

(continued)

TABLE 6.1 *(continued)*

k	Solutions	Ref. section	k	Solutions	Ref. section
-45	$\emptyset$	2.2	45	$\emptyset$	2.1
-44	$\emptyset$	2.1	44	$\emptyset$	2.1
-43	$\emptyset$	2.2.1	43	$\left(\frac{3}{2}, \frac{59}{9}\right), \left(\frac{7}{3}, \frac{386}{27}\right)$	4.2
-42	$\emptyset$	2.1	42	$\emptyset$	2.1
-41	$\emptyset$	2.1	41	$\emptyset$	2.1
-40	$\emptyset$	2.1	40	$\emptyset$	2.1
-39	$(2,5)^*$	5	39	$\emptyset$	2.2
-38	$\emptyset$	2.1	38	$\emptyset$	2.1
-37	$\emptyset$	2.1	37	$\emptyset$	2.1
-36	$\emptyset$	2.1	36	$(0,6),\ (2,10)$	2.2
-35	$\emptyset$	2.2.1	35	$(1,6)$	3
-34	$\emptyset$	2.1	34	$\emptyset$	2.1
-33	$\emptyset$	2.1	33	$\emptyset$	2.1
-32	$\emptyset$	2.1	32	$\emptyset$	2.1
-31	$\emptyset$	2.1	31	$\emptyset$	2.2.1
-30	$\emptyset$	2.1	30	$\emptyset$	2.1
-29	$\emptyset$	2.2.2	29	$\emptyset$	2.1
-28	$(2,6)$	3	28	$\emptyset$	2.2
-27	$\emptyset$	2.1	27	$\emptyset$	2.1
-26	$\emptyset$	2.1	26	$\emptyset$	2.1
-25	$\emptyset$	2.2.2	25	$(0,5)$	2.1
-24	$\emptyset$	2.1	24	$(1,5),\ \left(\frac{5}{2}, \frac{131}{8}\right)$	3
-23	$\emptyset$	2.1	23	$\emptyset$	2.1
-22	$\emptyset$	2.1	22	$\emptyset$	2.1
-21	$\emptyset$	2.2.1	21	$\emptyset$	2.1
-20	$\emptyset$	2.1	20	$\emptyset$	2.1
-19	$\emptyset$	2.1	19	$\emptyset$	2.1
-18	$\emptyset$	2.1	18	$\emptyset$	2.1
-17	$\emptyset$	2.1	17	$(2,9),\ \left(\frac{1}{2}, \frac{33}{8}\right)$	3
-16	$\emptyset$	2.1	16	$(0,4)$	2.1
-15	$(2,7)$	4.4	15	$(1,4)$	4.1
-14	$\emptyset$	2.1	14	$\emptyset$	2.1
-13	$\emptyset$	2.2	13	$\emptyset$	2.1
-12	$\emptyset$	2.1	12	$\emptyset$	2.1
-11	$\left(\frac{3}{2}, \frac{5}{8}\right)$	4.3	11	$\emptyset$	2.2
-10	$\emptyset$	2.1	10	$\left(\frac{3}{2}, \frac{37}{8}\right)$	3

(continued)

TABLE 6.1 *(continued)*

k	Solutions	Ref. section	k	Solutions	Ref. section
-9	$\emptyset$	2.1	9	$(0,3)$	2.1
-8	$\emptyset$	2.1	8	$(1,3)$	2.1
-7	$\emptyset$	2.1	7	$\emptyset$	2.1
-6	$\emptyset$	2.1	6	$\emptyset$	2.1
-5	$\emptyset$	2.1	5	$\emptyset$	2.1
-4	$\emptyset$	2.1	4	$(0,2)$	2.1
-3	$\emptyset$	2.1	3	$\emptyset$	3
-2	$\emptyset$	2.1	2	$\emptyset$	2.1
-1	$(1,0)$	2.1	1	$(0,1)$	2.1

REFERENCES

[1] M. A. Bennett, *Recipes for ternary Diophantine equations of signature* (p,p,k), Proc. RIMS Kokyuroku (Kyoto) **1319** (2003), 51–55.

[2] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[3] M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine equations of signature* $(p,p,3)$, Compos. Math. **140** (2004), no. 6, 1399-1416.

[4] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993)*, J. Symbolic Comput., **24** (1997), no. 3-4, 235–265.

[5] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society Student Texts **24**, Cambridge University Press, 1991, vi+137 pp.

[6] K. R. Coombes and D. A. Grant, *On heterogeneous spaces*, J. London Math. Soc. (2) **40** (1989), no. 3, 385–397.

[7] H. Darmon and A. Granville *On the equations* $z^m = F(x,y)$ *and* $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. **27** (1995), no. 6, 513–543.

[8] V. A. Dem'janenko, *The indeterminate equations* $x^6+y^6 = az^2$, $x^6+y^6 = az^3$, $x^4+y^4 = az^4$, in Twelve papers in Algebra, 27–34, Amer. Math. Soc. Transl., ser. 2, vol. 119, American Mathematical Society, Providence, RI, 1983, iv+139 pp.

[9] G. Faltings *Endlichkeitssätze für abelsche Varietäten über Zahlkörpen*, Invent. Math. **73** (1983), no. 3, 349-366. *Erratum*: ibid. **75** (1984), no. 2, 381.

[10] E. V. Flynn and J. L. Wetherell, *Covering collections and a challenge problem of Serre*, Acta Arith. **98** (2001), no. 2, 197–205.

[11] J. Gebel, A. Pethő and H. G. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), no. 2, 171–192.

[12] J. Gebel, A. Pethő and H. G. Zimmer, *On Mordell's equation*, Compositio Math. **110** (1998), no. 3, 335–367.

[13] R. J. Stroeker and N. Tzanakis, *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms*, Acta Arith. **67** (1994), no. 2, 177–196.

[14] P. Vojta, *Siegel's theorem in the compact case*, Ann. of Math. (2) **133** (1991), no. 3, 509–548.

A. Bremner, Dept. of Math., Arizona State U., Tempe, AZ 85287-1804, USA
bremner@asu.edu

N. Tzanakis, Dept. of Math., U. of Crete, Iraklion, Greece
tzanakis@math.uoc.gr