\[ y^2 = x^6 + k, \ k \in \{-39, -47\} \]

ANDREW BREMNER, THO NGUYEN XUAN

ABSTRACT. The aim of this paper is to solve the equation \( y^2 = x^6 + k \) in rational numbers with \( k \in \{-39, -47\} \). These are the two unsolved cases for integers \( k \) in the range \( |k| \leq 50 \).

1. INTRODUCTION

In their paper, Brenner and Tzanakis [2] studied the equation \( y^2 = x^6 + k \) in rational numbers where \( k \) is an integer in the range \( |k| \leq 50 \). They solved all the equations except \( k = -39 \) and \( k = -47 \). The main approach used by Brenner and Tzanakis is the elliptic curve Chabauty method. In this paper, we shall solve the equation \( y^2 = x^6 + k \) with \( k = -39 \) or \( k = -47 \). For \( k = -39 \), we shall present two approaches which might be applicable to other values of \( k \). For \( k = -47 \), only one approach is presented. The main tools here are the elliptic curve Chabauty method and algebraic number theory. In summary, we shall prove:

**Theorem 1.1.** The only rational solutions \((x, y)\) to the equation
\[ y^2 = x^6 - 39 \]
are \((\pm 2, \pm 5)\)

**Theorem 1.2.** The only rational solutions \((x, y)\) to the equation
\[ y^2 = x^6 - 47 \]
are \((\pm \frac{63}{10}, \pm \frac{249953}{10^3})\).

2. EQUATION \( y^2 = x^6 - 39 \)

In this section we shall present the proof of Theorem 1.1.

**Proof.** The equation \( y^2 = x^6 - 39 \) is equivalent to
\[ Y^2 = X^6 - 39Z^6, \]
where \( X, Y, Z \) are coprime integers. We have
\[ (X^3 - Y)(X^3 + Y) = 39Y^2. \]
Let \( d = \gcd(X^3 - Y, X^3 + Y) \). Then \( d | \gcd(2X^3, 2Y) = 2 \). We can choose the sign of \( Y \) such that \( 13 | X^3 + Y \).

Case \( d = 1 \): we have
\[ X^3 + Y = 39V^6, \quad X^3 - Y = U^6, \quad \gcd(U, V) = 1, \]
or
\[ X^3 + Y = 13V^6, \quad X^3 - Y = 3U^6, \quad \gcd(U, V) = 1. \]

2010 Mathematics Subject Classification. Primary: 05C??, Secondary: 05C??
Key words and phrases. Diophantine equation, elliptic curve Chabauty.
So
\[ 2X^3 = 39V^6 + U^6 \quad \text{or} \quad 2X^3 = 13V^6 + 3U^6, \quad \gcd(U, V) = 1. \]
In the former case, we have \( 3 \nmid U \). So \( U \equiv 1 \mod 9 \), hence \( 2X^3 \equiv 3V^6 + 1 \mod 9 \). Thus \( X^3 \equiv -1 \mod 3 \), so \( X \equiv -1 \mod 3 \). Therefore \( X^3 \equiv -1 \mod 9 \). So \( V^6 + 1 \equiv 0 \mod 3 \), impossible.
In the latter case, we have
\[ (2.2) \quad 2X^3 = 13V^6 + 3U^6, \quad \gcd(U, V) = 1. \]
We shall deal with this case later.

Case \( d = 2 \): we have
\[
\begin{align*}
X^3 + Y &= 2 \cdot 39V^6, \quad X^3 - Y = 2^5 \cdot U^6, \quad \gcd(U, V) = 1, \\
X^3 + Y &= 2^5 \cdot 39V^6, \quad X^3 - Y = 2 \cdot U^6, \quad \gcd(U, V) = 1, \\
X^3 + Y &= 2 \cdot 13V^6, \quad X^3 - Y = 2^5 \cdot 3U^6, \quad \gcd(U, V) = 1, \\
X^3 + Y &= 2^5 \cdot 13V^6, \quad X^3 - Y = 2 \cdot 3U^6, \quad \gcd(U, V) = 1.
\end{align*}
\]
This gives
\[
\begin{align*}
X^3 &= 39V^6 + 16U^6, \\
X^3 &= 624V^6 + U^6, \\
X^3 &= 13V^6 + 48U^6, \\
X^3 &= 208V^6 + 3U^6.
\end{align*}
\]
The first equation: \( \pm 1, \pm 5 \equiv 3U^6 \equiv \pm 3 \mod 13 \), impossible.
The third equation: \( \pm 1, \pm 5 \equiv \pm 4 \mod 13 \), impossible.
The fourth equation: \( \pm 1, \pm 5 \equiv \pm 3 \mod 13 \), impossible.
There remains the second equation:
\[ X^3 = 624V^6 + U^6, \quad \gcd(U, V) = 1. \]
This gives
\[ (624(X/U^2))^3 = (624(V^3/U^3))^2 + 624^3. \]
The elliptic curve \( y^2 = x^3 - 624^3 \) has rank 0, so \( X^3 = 624V^6 + U^6 \) only has trivial solutions.
We only need to deal with the case \( (2.2) \)
\[ 2X^3 = 3U^6 + 13V^6, \quad \gcd(U, V) = 1. \]
Observe that \( 2|X \) and \( 2 \nmid U, V \).

**Solution 1:** Let \( K = \mathbb{Q}(\theta) \), where \( \theta = \sqrt[3]{39} \). \( K \) has the ring of integers \( \mathcal{O}_K = \mathbb{Z}[\theta] \) and a fundamental unit \( \epsilon = 2\theta^2 - 23 \) of norm 1.

**Lemma 2.1.** Consider the elliptic curve
\[ E : v^2 = u^3 - 39, \]
let \( \phi \) be a map \( E(\mathbb{Q}) \to K^*/(K^*)^2 \) given by
\[
\begin{align*}
\phi(u, v) &= u - \theta \mod (K^*)^2, \\
\phi(\infty) &= (K^*)^2.
\end{align*}
\]
Then \( \phi \) is a group homomorphism with the kernel \( 2E(\mathbb{Q}) \).

**Proof.** This is the standard 2-descent. See Silverman [5].
We have  
\[ E(\mathbb{Q}) = \mathbb{Z}(10,31) \oplus \mathbb{Z}(4,5). \]
Because \((X^2/Z^2, Y/Z^3) \in E(\mathbb{Q})\), Lemma 2.1 implies  
\[ (X^2 - \theta Z^2) \equiv \alpha \mod (K^*)^2, \]
where \(\alpha \in \{1, 4 - \theta, 10 - \theta, (4 - \theta)(10 - \theta)\}\).
Because \(10 - \theta = \epsilon(3\theta^2 + 10\theta + 34)^2\), we have the following cases:

**Case 1:** \(X^2 - \theta Z^2 \in K^2\).
Because \(X^2 - \theta Z^2 \in \mathbb{Z}[\theta] = \mathcal{O}_K\), we have  
\[ X^2 - \theta Z^2 = (a + b\theta + c\theta^2)^2, \]
where \(a, b, c \in \mathbb{Z}\). Comparing coefficients of \(\theta^0, \theta, \theta^2\) gives:
\[
\begin{cases}
  X^2 = a^2 + 78bc, \\
  Z^2 = -2ab - 39c^2, \\
  0 = 2ac + b^2.
\end{cases}
\]
From \(\gcd(X, Z) = 1\), we have \(\gcd(a, b, c) = 1\). Because \(2 \mid X\), from the first and the third equations, we have \(2 \nmid a, b\). Thus \(2 \nmid c\). Let \(a = 2a_1, b = 2b_1\). Then  
\[
\begin{cases}
  (X/2)^2 = a_1^2 + 39b_1c, \\
  Z^2 = -8a_1b_1 - 39c^2, \\
  0 = a_1c + b_1^2.
\end{cases}
\]
Since \(\gcd(a, b, c) = 1\), the third equation implies \(\gcd(a_1, c) = 1\). Hence \(\exists r, s \in \mathbb{Z}, r > 0\) such that

\[ a_1 = r^2, \quad c = -s^2, \quad b_1 = -rs, \quad \gcd(r, s) = 1, \]

or

\[ a_1 = -r^2, \quad c = s^2, \quad b_1 = -rs, \quad \gcd(r, s) = 1. \]

Case (2.3) gives

\[
\begin{align*}
  (X/2)^2 &= r(r^3 - 39s^3), \\
  Z^2 &= s(8r^3 - 39s^3).
\end{align*}
\]
Because \(\gcd(X, Z) = 1\), we have \(\gcd(r, 39) = \gcd(s, 2) = 1\). Hence \(\gcd(r, r^3 - 39s^3) = \gcd(s, 8r^3 - 39s^3) = 1\). Because \(r > 0\), we have \(8r^3 - 39s^3 > r^3 - 39s^3 > 0\). Thus \(s > 0\). It follows that

\[
\begin{align*}
  r &= A^2, \\
  r^3 - 39s^3 &= C^2, \\
  X &= \pm AC,
\end{align*}
\]

\[
\begin{align*}
  s &= B^2, \\
  8r^3 - 39s^3 &= D^2, \\
  Z &= \pm BD.
\end{align*}
\]
Therefore \(D^2 = 8A^6 - 39B^6\). So \(D^2 + A^6 \equiv 0\) mod 3. Hence \(A \equiv D \equiv 0\) mod 3. Thus \(3 \mid X, Z\), a contradiction.

Case (2.4) gives

\[
\begin{align*}
  (X/2)^2 &= r(r^3 - 39s^3), \\
  Z^2 &= -s(8r^3 + 39s^3).
\end{align*}
\]
We have \(\gcd(r, 39) = \gcd(s, 2) = 1\). Because \(r > 0\), if \(s > 0\), then \(Z^2 = -s(8r^3 + 39s^3) < 0\), impossible. Therefore \(s < 0\). Thus

\[
\begin{align*}
  r &= A^2, \\
  r^3 - 39s^3 &= C^2, \\
  X &= \pm AC,
\end{align*}
\]

\[
\begin{align*}
  s &= -B^2, \\
  8r^3 + 39s^3 &= D^2, \\
  Z &= \pm BD.
\end{align*}
\]
Thus $D^2 = 8A^6 - 39B^6$. So $D^2 + A^6 \equiv 0 \mod 3$. Therefore $A \equiv D \equiv 0 \mod 3$. Hence $3|X, Z$, a contradiction.

**Case 2:** $(X^2 - \theta Z^2) \in \epsilon K^2$.

Because $\epsilon$ is a unit and $X^2 - \theta Z^2 \in \mathcal{O}_K$, we have

$$X^2 - \theta Z^2 = (2\theta^2 - 23)(a + b\theta + c\theta^2)^2,$$

where $a, b, c \in \mathbb{Z}$. Comparing the coefficients of $\theta^0, \theta, \theta^2$ gives

$$\begin{cases} 
X^2 = -23a^2 + 156ab - 1794bc + 3042c^2, \\
Z^2 = 46ab - 156ac - 78b^2 + 897c^2, \\
0 = 2a^2 - 46ac - 23b^2 + 156bc.
\end{cases}$$

Because $\gcd(X, Z) = 1$, we have $\gcd(a, b, c) = 1$. From the third equation, we have $2|b, 2|X$. Thus the first equation implies $2|a$. Hence $2 \nmid c$. The first equation gives

$$X^2 \equiv 2c^2 \equiv 2 \mod 4,$$

impossible.

**Case 3:** $X^2 - \theta Z^2 \in \epsilon(4 - \theta)K^2$.

Let

$$X^2 - \theta Z^2 = \epsilon(4 - \theta)(\frac{a + b\theta + c\theta^2}{n})^2,$$

where $n, a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$. Comparing the coefficients of $\theta^0, \theta, \theta^2$ gives

$$\begin{cases} 
(nX)^2 = -170a^2 + 624ab + 1794ac + 897b^2 - 13260bc + 12168c^2, \\
(nZ)^2 = -23a^2 + 340ab - 624ac - 312b^2 - 1794bc + 6630c^2, \\
0 = 8a^2 + 46ab - 340ac - 170b^2 + 624bc + 897c^2.
\end{cases}$$

From the third equation, we have $2|c$. Because $2|nX$, from the first equation, we have $2|b$. Therefore $2 \nmid a$. Then the first equation gives

$$(nX)^2 \equiv 2a^2 \equiv 2 \mod 4,$$

impossible.

**Case 4:** $(X^2 - \theta Z^2)(4 - \theta) \in K^2$.

We have $x = X/Z$, $y = Y/Z$, $y^2 = (x^2 - \theta)(x^4 + \theta x^2 + \theta^2)$, and $(x^2 - \theta)(4 - \theta) \in K^2$. Thus

$$(4 - \theta)(x^4 + \theta x^2 + \theta^2) \in K^2.$$ 

Let $(4 - \theta)(x^4 + 4\theta x^2 + \theta^2) = \beta^2$. Then $((4 - \theta)x^2, (4 - \theta)\beta)$ is a point on

$$G : v^2 = u(u^2 + \theta(4 - \theta)u + \theta^2(4 - \theta)^2).$$

We have

$$G(K) = \mathbb{Z}/2\mathbb{Z}(0, 0) \oplus \mathbb{Z}(\frac{4\theta^2 - 39}{4}, \frac{20\theta^2 - 195}{8}).$$

The curve $G$ has rank 1 over $K$, and $[K : \mathbb{Q}] = 3$.

The first approach is to use the elliptic curve Chabauty method. With the search bound of 350 and the assumption of the Generalized Riemann Hypothesis, Pseudo-Mordell-Weil returns "false". The second approach is to use the formal group technique as in Flynn [3] which will almost guarantee the solution when $\text{rank}(G(K)) < [K : \mathbb{Q}]$. If we follow this approach, then the smallest prime that might work is $p = 7$. The order of the generator $(\frac{3\theta^2 - 39}{4}, \frac{20\theta^2 - 195}{8})$ in $\mathbb{F}_7(\theta)$ with $\theta^3 - 39 = 0$ is 86. In $G(K)$, we shall need to compute the set $\{m(0, 0) + n(\frac{4\theta^2 - 39}{4}, \frac{20\theta^2 - 195}{8}) : n = 0, 1, m = -42, -41, ..., m = 43\}$ and then compute the corresponding formal power series, see
Flynn [3] for more details about this approach. This might work, but it shall take too much computation. We will take another approach which might possibly be applicable in case \( \text{rank}(G(K)) \geq [K : \mathbb{Q}] \).

We have
\[
X^2 - \theta Z^2 = (4 - \theta)(a + b\theta + c\theta^2)^2,
\]
where \( a, b, c \in \mathbb{Q} \). Thus
\[
(2.5) \quad X^2 = 4a^2 - 78ac - 39b^2 + 312bc,
\]
\[
(2.6) \quad Z^2 = a^2 - 8ab + 78bc - 156c^2,
\]
\[
(2.7) \quad 0 = -2ab + 8ac + 4b^2 - 39c^2.
\]
If \( 4c - b = 0 \), then from (2.7), we have \( 4b^2 - 39c^2 = 0 \). So \( b = c = 0 \). Therefore
\[
x = \frac{X}{Z} = \pm 2.
\]
If \( 4c - b \neq 0 \), then from (2.7), we have \( a = \frac{39c^2 - 4b^2}{2(4c - b)} \).

Let \( P = 5c \) and \( Q = 4c - b \). Then
\[
X^2 = \frac{P^4 - 5P^2Q + 24P^2Q^2 - 20PQ^3 - 23Q^4}{Q^2},
\]
\[
Z^2 = \frac{P^4 - 24P^2Q^2 + 40PQ^3 - 48Q^4}{4Q^2}.
\]
Let \( P = dp, Q = dq, X_1 = \frac{X}{d}, Z_1 = \frac{Z}{d} \), where \( d = \gcd(P, Q) \). Then
\[
(2.8) \quad X_1^2 = p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4,
\]
\[
Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4.
\]
We have \( \gcd(p, q) = 1 \) and \( X_1, Z_1 \in \mathbb{Z} \).

**Lemma 2.2.** In (2.8), we have
\[
\gcd(X_1, 39) = \gcd(Z_1, 13) = \gcd(Z_1, 2) = 1.
\]

**Proof.** First, we show that \( 2 \nmid Z_1 \).

If \( q \nmid d \), then \( \exists \) a prime \( l \mid q \) such that \( l \mid X_1 = \frac{X}{d} \). Thus
\[
l \mid p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4.
\]
Because \( l \mid q \), we have \( l \mid p \). So \( l \mid \gcd(p, q) > 1 \), a contradiction. Therefore \( q \mid d \). Thus \( X_1 \mid X \) and \( Z_1 \mid Z \). From (2.2), we have \( \gcd(U, V) = 1 \), \( 2 \mid X \) and \( 2 \nmid Z \). If \( 2 \nmid Z_1 \). Then from
\[
Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4,
\]
we have \( 2 \nmid p \). Thus \( 2 \nmid X_1 \). Hence \( 2 \nmid X \). From \( 2 \mid X = (\frac{d}{q})X_1 \), we have \( 2 \nmid \frac{d}{q} \). So \( \frac{d}{q} \in \mathbb{Z} \).

Because \( 2 \nmid Z = (\frac{d}{2q})Z_1 \), we have \( 2 \nmid Z_1 \), a contradiction. So \( 2 \nmid Z_1 \).

If \( 3 \mid X_1 \), then
\[
3 \mid p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4.
\]
Thus
\[
3 \mid p^4 + q^4 + p^3q + qp^3.
\]
Because \( \gcd(p, q) = 1 \), we have \( 3 \nmid p, q \). Hence \( 3 \mid 2 + 2pq \). So \( pq \equiv -1 \mod 3 \), thus \( p + q \equiv 0 \mod 3 \). Therefore
\[
Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4 \equiv -3p^4 \mod 9,
\]
which is not possible. So \(3 \nmid X_1\).
If \(13 \mid X_1\), then
\[
13\mid p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4.
\]
Thus \(13 \mid p + 2q\). So
\[
Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4 \equiv -39q^4 \mod 13^2,
\]
which is not possible. Hence \(13 \nmid X_1\).
If \(13 \mid Z_1\), then
\[
13\mid p^4 - 24p^2q^2 + 40pq^3 - 48q^4.
\]
Thus
\[
13\mid (p + 2q)(p + 7q).
\]
If \(13 \mid p + 2q\) or \(13 \mid p + 7q\), then
\[
Z_1^2 = p^4 - 24p^2q^2 + 40pq^3 - 48q^4 \equiv -39q^4 \mod 13^2,
\]
which is not possible. So \(13 \nmid Z_1\).

Let \(L = \mathbb{Q}(\phi)\), where \(\phi, \sim 2.8502\), is the largest real root of \(x^4 - 6x^2 - 5x - 3 = 0\).\n\(L\) has class number 1, the ring of integers \(\mathcal{O}_L = \mathbb{Z}[\phi]\), and two positive fundamental units \(\epsilon_1 = \phi + 2, \epsilon_2 = \phi^3 - \phi^2 - \phi - 1\) with \(\text{Norm}(\epsilon_1) = \text{Norm}(\epsilon_2) = -1\).

Let
\[
F(p, q) = p^4 - 5p^3q + 24p^2q^2 - 20pq^3 - 23q^4,
\]
\[
G(p, q) = p^4 - 24p^2q^2 + 40pq^3 - 48q^4.
\]
Then
\[
F(p, q) = (p + (\phi^3 - 7\phi - 5)q)A(p, q),
\]
\[
G(p, q) = (p + 2\phi q)B(p, q),
\]
where
\[
A(p, q) = p^3 + (-\phi^3 + 7\phi)p^2q + (4\phi^2 - 5\phi)pq^2 + (4\phi^3 - 5\phi^2 - 12\phi - 5)q^3,
\]
\[
B(p, q) = p^3 - 2\phi p^2q + (4\phi^2 - 24)pq^2 + (-8\phi^3 + 48\phi + 40)q^3.
\]
In \(\mathbb{Z}[\phi]\), let
\[
p_1 = -2\phi^3 + \phi^2 + 12\phi + 4, \quad p_2 = \phi, \quad p_3 = \phi + 1, \quad q_1 = \phi^3 - 6\phi - 4, \quad q_2 = \phi - 1.
\]
Then
\[
3 = p_1p_2p_3^3, \quad 13 = q_1q_2^3,
\]
\[
\text{Norm}(p_1) = 1, \text{Norm}(p_2) = \text{Norm}(p_3) = -3,
\]
\[
\text{Norm}(q_1) = \text{Norm}(q_2) = -13.
\]
We also have
\[
\text{Res}(p + 2\phi q, B(p, q)) = -8p_1p_2^5q_2^2,
\]
\[
\text{Res}(p + (\phi^3 - 7\phi - 5)q, A(p, q)) = (4\phi^3 + 6\phi^2 - 31\phi - 53)p_2p_3^5q_1q_2^3.
\]
Because $\gcd(X_1, 39) = \gcd(Z_1, 39) = \gcd(Z_1, 2) = 1$ and $\Norm(4\phi^3 + 6\phi^2 - 31\phi - 53) = 1$, we have
\[
\begin{cases}
p + (\phi^3 - 7\phi - 5)q = (-1)^h \epsilon_1^i \epsilon_2^j S^2, & p + 2\phi q = (-1)^h \epsilon_1^i \epsilon_2^j T^2, \\
A(p, q) = (-1)^h \epsilon_1^i \epsilon_2^j S_1, & B(p, q) = (-1)^h \epsilon_1^i \epsilon_2^j T_1^2,
\end{cases}
\]
where $X_1 = SS_1$ and $Z_1 = TT_1$.

Taking norms gives
\[
(X_1)^2 = (-1)^{i+j} \Norm(S)^2, \quad Z_1^2 = (-1)^{i+j} \Norm(T)^2.
\]
Thus $2|i + j$ and $2|i_1 + j_1$. Hence $i = j$ and $i_1 = j_1$.

Let $\beta = \epsilon_1 \epsilon_2 = \phi^3 + 3\phi^2 + 2\phi + 1 > 0$. Then
\[(2.9) \quad \begin{cases}
p + (\phi^3 - 7\phi - 5)q = (-1)^h \beta^i S^2, & p + 2\phi q = (-1)^h \beta^i T^2, \\
A(p, q) = (-1)^h \beta^{-i} S_1, & B(p, q) = (-1)^h \beta^{-i} T_1^2.
\end{cases}
\]

**Lemma 2.3.** We have
\[(2.10) \quad (p + (\phi^3 - 7\phi - 5)q)(p + 2\phi q) > 0.
\]

**Proof.** Equation $F(x, 1) = 0$ has 2 real roots
\[x_1 = -\phi^3 + 7\phi + 5 \sim 1.7976, \quad x_2 \sim -0.6206.
\]
Equation $G(x, 1) = 0$ has 2 real roots
\[x_3 = -2\phi \sim -5.7004, \quad x_4 \sim 4.1399.
\]
We have
\[F\left(\frac{p}{q}, 1\right) > 0 \quad \text{and} \quad G\left(\frac{p}{q}, 1\right) > 0.
\]
So
\[\frac{p}{q} < x_3 \quad \text{or} \quad \frac{p}{q} > x_4.
\]
Because $x_3 < x_2 < x_1 < x_4$, we have
\[(p + x_1 q)(p + x_3 q) > 0.
\]

\(\square\)

From **Lemma 2.3** and (2.9), we have $h = h_1$. So by mapping $(p, q) \mapsto (-p, -q)$, we can assume that $h = h_1 = 0$.

Case $i \neq i_1$:

Because $\phi - 1|\phi^3 - 9\phi - 5$, we have
\[(\phi - 1)((\phi^3 - 9\phi - 5)q = \beta^i S^2 - \beta^i T^2.
\]
Because $i - i_1 = \pm 1$ and $\beta$ is a unit, we have
\[\beta S^2 - T^2 \equiv 0 \mod \phi - 1.
\]

If $\phi - 1|S$ or $\phi - 1|T$, then $\phi - 1|S, T$. Hence $13 = -\Norm(\phi - 1)|\Norm(S), \Norm(T)$. Thus $13|X, Z$, impossible. So $\phi - 1 \nmid S, T$. Therefore $S^{12} \equiv T^{12} \equiv 1 \mod \phi - 1$ (because $\Norm(\phi - 1) = -13$). Also $\beta \equiv 7 \mod \phi - 1$, therefore
\[0 \equiv \beta^6 S^{12} - T^{12} \equiv \tau^6 - 1 \mod \phi - 1.
\]
So \( 13 = -\text{Norm}(\phi - 1)|(7^6 - 1)^4 \). But \( 13 \nmid 7^6 - 1 \), so we have a contradiction.

Case \( i = i_1 \):

If \( q \neq 0 \), then

\[
(p + (\phi^3 - 7\phi - 5)q)(p^3 - 2\phi p^2 q + 4(\phi^2 - 6)pq^2 + 8(-\phi^3 + 6\phi + 5)q^3) = (ST_1)^2,
\]

which represents an elliptic curve

\[
C: v^2 = (u + \gamma)(u^3 - 2\phi u^2 + 4(\phi^2 - 6)u + 8(-\phi^3 + 6\phi + 5)),
\]

where \( v = (ST_1)/q^2, u = p/q \). The minimal cubic model at \((-\gamma, 0)\) is

\[
y^2 = x^3 + (-2s^3 + 2s^2 + 10s + 6)x^2 + (-4s^3 + 8s^2 + 12s)x + (1488s^3 + 1776s^2 - 11128s - 17160).
\]

The elliptic Chabauty routine in Magma \([1]\) works and returns \( u = 69/26 \). Hence \( (p,q) = (69,26), (-69,-26) \). This gives no solutions \((X_1,Z_1)\). Therefore \( q = 0 \), so \( X_1 = \pm 2 \) and \( Z_1 = \pm 1 \). Thus

\[
x = \frac{X_1}{Z_1} = \pm 2.
\]

So the only rational solutions to \( y^2 = x^6 - 39 \) are \((x,y) = (\pm 2, \pm 5)\).

**Remark 2.4.** (i) From the system \((2.8)\), we have a curve

\[
(2.11) \quad F: \omega^3 = (\lambda^4 - 5\lambda^3 + 24\lambda^2 - 20\lambda - 23)(\lambda^4 - 24\lambda^2 - 40\lambda - 48),
\]

where \( \omega = \frac{xZ_1}{\tau} \) and \( \lambda = \frac{y}{q} \). This curve has genus 3 and the Jacobian rank at most 3.

We are unable to compute the Jacobian rank. Computer search reveals no rational points on \((2.11)\). It might be possible to show \( F \) has no rational points using the partial descent on hyperelliptic curves as in Siksek and Stoll \([1]\) but we have not proceeded in this way.

(ii) More generally, **Solution 1** gives us an approach to the equation \( y^2 = x^6 + k \) in principle. We write \( y^2 = x^6 + k \) as \( Y^2 = X^6 + kZ^6 \), then compute the generators of the MordellWeil group of the elliptic curve \( E_k: v^2 = x^3 + k \). Using 2-descent as in Lemma \([2.7]\) we shall need to solve a finite number of equations

\[
X^2 - \theta Z^2 = (x_i - \theta)(a_i + b_i\theta + c_i\theta^2)^2,
\]

where \( \theta = k^{1/3} \) and the set \( \{(x_i,y_i)\}_i \) is a finite set \( a_i,b_i,c_i \in \mathbb{Q} \).

Thus for each \( i \), we have a system of equations

\[
\begin{cases}
X^2 = S_0(a_i,b_i,c_i), \\
Z^2 = S_1(a_i,b_i,c_i), \\
0 = S_2(a_i,b_i,c_i),
\end{cases}
\]

where \( S_0,S_1,S_2 \) are homogenous rational polynomials of degree 2 in \( a_i,b_i,c_i \).

Assume from \( S_3(a_i,b_i,c_i) = 0 \) that we can solve for one of \( a_i,b_i,c_i \) in term of the two other variables. Then from \( (XZ)^2 = S_0(a_i,b_i,c_i)S_1(a_i,b_i,c_i) \), we have a genus 3 curve

\[
F_i: \omega^2 = p_i(\lambda)q_i(\lambda),
\]

where \( p_i(\lambda),q_i(\lambda) \) are rational polynomials of degree 4. The partial descent method and the Chabauty method might help to find rational points on \( F_i \).

**Solution 2:** In this section, we shall present another solution to \( y^2 = x^6 - 39 \). The approach taken here is classical and is applied to the case \( k = -47 \). We shall start from \((2.2)\)

\[
(2.12) \quad 2X^3 = 3U^6 + 13V^6, \quad Z = UV, \quad \gcd(U,V) = 1.
\]
Observe that $U, V$ are odd and $X$ is even. Let $K = \mathbb{Q}(\theta)$, where $\theta^2 = -39$. The ring of integers is $\mathcal{O}_K = \mathbb{Z}[\frac{1+\theta}{2}]$. The class number is 4. The ideal $(2) = p_{21}p_{22}$, where $p_{21} = (2, \frac{1+\theta}{2})$ and $p_{21}^3 = (\frac{1+\theta}{2})$; the ideal $(3) = p_3^2$, where $p_3 = (3, \theta)$; and $(\theta) = p_{13}p_{13}$. We write (2.12) as

$$\frac{(3U^3 + \theta V^3)}{2} = \frac{(3U^3 - \theta V^3)}{2} = 12\left(\frac{X}{2}\right)^3.$$  

A common ideal divisor $J$ of the factors on the left divides $(3U^3) = p_3^2(U^3)$ and $p_{13}(V^3)$. $J^2$ divides $(12\left(\frac{X}{2}\right)^3) = p_{21}^2p_{22}^2p_{3}^2\left(\frac{X}{2}\right)^3$. Certainly, $p_3$ divides $J$. Since $J|p_3p_{13}(V^3)$ and $3 \nmid V$, we have $p_3^2 \nmid J$. Further $p_{13} \nmid J$, otherwise $13|X$, impossible. So $J = p_3$.

Since $p_{22}^2(\frac{3U^3+\theta V^3}{2})$, we have

$$\frac{3U^3 + \theta V^3}{2} = p_3^2p_{22}A^3 = (\frac{3 + \theta}{2})A^3.$$  

It follows that $A$ is principal. Hence $A = (A)$ for some element $A \in \mathcal{O}_K$. Further, any unit in $\mathbb{Q}(\theta)$ is ±1, so it can be absorbed into $A$. Let $A = a + b\frac{\theta + 1}{2}$, where $a, b \in \mathbb{Z}$. Then

$$\frac{3U^3 + \theta V^3}{2} = \frac{3 + \theta}{2}A^3 = \frac{3 + \theta}{2}(a + b(1 + \theta)^3) = \frac{3(a^3 - 18a^2b - 48ab^2 + 44b^3)}{2} + \frac{\theta(a^3 + 6a^2b - 24ab^2 - 28b^3)}{2}.$$  

Thus

$$(2.13) \quad U^3 = a^3 - 18a^2b - 48ab^2 + 44b^3, \quad V^3 = a^3 + 6a^2b - 24ab^2 - 28b^3.$$  

If $3|U$, then $a \equiv b \mod 3$. Hence $a^3 \equiv b^3 \mod 9$. So $0 \equiv 3ab^2 \mod 9$, leading to $a \equiv b \equiv 0 \mod 9$, and hence $\gcd(U, V) > 1$, impossible. Therefore $3 \nmid U$. If $3|V$, then $a \equiv b \mod 3$, implying $3|U$, impossible. So $3 \nmid U, V$.

Let $L = \mathbb{Q}(\phi)$, where $\phi^3 - 12\phi - 10 = 0$. Then $L$ has class number 3 and two fundamental units

$$\epsilon_1 = 1 + \phi, \quad \epsilon_2 = 3 + \phi, \quad \text{Norm}(\epsilon_1) = -1, \quad \text{Norm}(\epsilon_2) = 1.$$  

Let $q_{13} = (13, \phi - 2)$ and $p_7 = (7, \phi)$. Then

$$(2) = p_2^3, \quad (3) = p_3^2, \quad (13) = p_{13}q_{13}^2,$$

where

$$(2 + \phi) = p_2p_3,$$

$$(4 + \phi) = p_2p_{13},$$

$$(-2 + \phi) = p_2q_{13},$$

$$(-\phi^2 - 2\phi + 2) = p_2p_{11},$$

$$(\phi^2 - 2\phi - 6) = p_2^2p_7.$$  

We have

$$\phi \equiv 9 \mod p_{13}, \quad \phi \equiv 2 \mod q_{13}.$$
and
\[ U^3 = (a + (-\phi^2 - 2\phi + 2)b)(a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2), \]
\[ V^3 = (a + (\phi^2 - 2\phi - 6)b)(a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2). \]

The gcd of \( (a + (-\phi^2 - 2\phi + 2)b) \) and \( (a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2) \) divides \( 78(2 + \phi) \). The gcd of \( (a + (\phi^2 - 2\phi - 6)b) \) and \( (a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2) \) divides \( 18(2 - \phi) \).

Let
\[ (a + (-\phi^2 - 2\phi + 2)b) = p_1^{i_1}p_2^{i_2}p_3^{i_3}q_1^{i_4}X^3, \]
where \( X \) is an ideal in \( \mathcal{O}_L \). Taking norms gives
\[ U^3 = 2^{i_1}3^{i_2}13^{i_3+i_4}X^3, \]
where \( X_1 = \text{Norm}(X) \). So
\[ i_1 = i_2 = 0, \quad i_3 + i_4 \equiv 0 \mod 3. \]
Thus
\[ (a + (-\phi^2 - 2\phi + 2)b) = X^3, \]
or
\[ (a + (-\phi^2 - 2\phi + 2)b) = (13)X^3, \]
or
\[ (a + (-\phi^2 - 2\phi + 2)b) = (2\phi^2 - 9\phi - 3)X^3. \]
The later two cases cannot occur. Otherwise, \( a - 6b \equiv 0 \mod 13 \). Setting \( a = 6b + 13c \) gives
\[ U^3 = 13^2(4b^4 + 12b^2c - 13c^3), \quad V^3 = 13(20b^3 + 156b^2c + 312bc^2 + 169c^3). \]
Then \( 13|U, V \), contradicting \( \gcd(U, V) = 1 \). Thus
\[ (a + (-\phi^2 - 2\phi + 2)b) = \mathcal{X}^3, \]
\[ (a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2) = \mathcal{Y}^3, \]
where \( \mathcal{X}\mathcal{Y} = (U) \).
Similarly
\[ (a + (\phi^2 - 2\phi - 6)b) = \mathcal{Y}^3, \]
\[ (a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2) = \mathcal{Y}^3, \]
where \( \mathcal{Y}^2 = (V) \).
If \( \mathcal{X} \sim 1 \), then from (2.14)
\[ a + (-\phi^2 - 2\phi + 2)b = \epsilon_1^{i_1}\epsilon_2^{i_2}X_1^3, \quad X_1 \in \mathcal{O}_L, \]
\[ a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2 = \epsilon_1^{-i_1}\epsilon_2^{-i_2}X_1^3, \quad X_1^X_1 = U. \]
If \( \mathcal{X} \sim p_2 \), then from (2.14)
\[ a + (-\phi^2 - 2\phi + 2)b = \frac{1}{4}\epsilon_1^{i_1}\epsilon_2^{i_2}X_2^3, \quad X_2 \in \mathcal{O}_L, \]
\[ a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2 = \frac{1}{2}\epsilon_1^{-i_1}\epsilon_2^{-i_2}X_2^3, \quad X_2^2 = 2U. \]
If \( X \sim p_2 \), then from (2.14)

\[
a + (-\phi^2 - 2\phi + 2)b = \frac{1}{2} e_1^j e_2^j x_3^3, \quad X_3 \in \mathcal{O}_L,
\]

(2.18)

\[
a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2 = \frac{1}{4} e_{-i}^j e_{-j}^j x_3^3, \quad X_3 X_3 = 2U.
\]

Similarly:

If \( Y \sim 1 \), then from (2.15)

\[
a + (\phi^2 - 2\phi - 6)b = \frac{1}{2} e_1^j e_2^j y_3^3, \quad Y_1 \in \mathcal{O}_L,
\]

(2.19)

\[
a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2 = \frac{1}{2} e_{-i}^j e_{-j}^j y_3^3, \quad Y_1 Y_1 = V.
\]

If \( Y \sim p_2 \), then from (2.15)

\[
a + (\phi^2 - 2\phi - 6)b = \frac{1}{4} e_1^j e_2^j y_3^3, \quad Y_2 \in \mathcal{O}_L,
\]

(2.20)

\[
a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2 = \frac{1}{4} e_{-i}^j e_{-j}^j y_3^3, \quad Y_2 Y_2 = 2V.
\]

If \( Y \sim p_2^2 \), then from (2.15)

\[
a + (\phi^2 - 2\phi - 6)b = \frac{1}{2} e_1^j e_2^j y_3^3, \quad Y_3 \in \mathcal{O}_L,
\]

(2.21)

\[
a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2 = \frac{1}{2} e_{-i}^j e_{-j}^j y_3^3, \quad Y_3 Y_3 = 2V.
\]

The equations (2.16) – (2.18) and (2.19) – (2.21) give the following equations respectively in \( \mathcal{O}_L \):

\[
a + (-\phi^2 - 2\phi + 2)b = \frac{1}{\mu} e_1^i e_2^i x_3^3,
\]

\[
a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2 = \frac{1}{\mu} e_{-i}^j e_{-j}^j x_3^3,
\]

where \((\mu, \mu') = (1, 1), (4, 2), (2, 4)\); and

\[
a + (\phi^2 - 2\phi - 6)b = \frac{1}{v} e_1^j e_2^j y_3^3, \quad Y_j \in \mathcal{O}_L,
\]

\[
a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2 = \frac{1}{v} e_{-j}^j e_{-j}^j y_3^3, \quad Y_j Y_j = V,
\]

where \((v, v') = (1, 1), (4, 2), (2, 4)\).

We accordingly have equations in \( \mathcal{O}_L \):

\[
(a + (-\phi^2 - 2\phi + 2)b)(a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2) = \frac{1}{\mu v} e_1^i e_2^i x_3^3 y_3^3,
\]

(2.22)

\[
(a + (\phi^2 - 2\phi - 6)b)(a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2) = \frac{1}{\mu v} e_1^j e_2^j x_3^3 y_3^3,
\]

(2.23)

where \( r(= i_1 - j_1) = 0, \pm 1, s(= i_2 - j_2) = 0, \pm 1 \).

Now \( t \mid UV \), so \( (X_i), (X_j), (Y_i), (Y_j) \) are coprime to \( p_3 \). Then for \( \alpha \in \mathcal{O}_L \) and \( p_3 \nmid (\alpha) \), we have \( p_3 | (\alpha^2 - 1) \). Therefore \( 3 = p_3^2 | (\alpha^2 - 1)^3 \equiv \alpha^6 - 1 \mod 3 \). Hence \( \alpha^3 \equiv \pm 1 \).
mod 3. It follows that $X_{i}^{3} Y_{i}^{3} \equiv \pm 1 \mod 3$. Since $\mu, \mu', v, v' \equiv \pm 1 \mod 3$, equation (2.22) gives

$$(a + b)(a^2 + ab + b^2) + b(a^2 + ab + b^2)\phi^2 \equiv \pm \epsilon_1 \epsilon_2 \mod 3,$$

and equation (2.23) gives

$$(a + b)(a^2 - b^2) + b^2(a - b)\phi - b(a^2 - b^2)\phi^2 \equiv \pm \epsilon_1^{-\epsilon_2} \mod 3.$$ We have

|\begin{array}{c|c|c|c|c|}
\hline
r, s & \epsilon_1 \epsilon_2 & \epsilon_1^{-\epsilon_2} \\
\hline
(-1,-1) & -\phi^2 + 2\phi + 7 & \phi^2 + 4\phi + 3 \\
(-1,0) & -\phi^2 + \phi + 11 & \phi + 1 \\
(-1,1) & -2\phi^2 + 2\phi + 23 & -2\phi^2 + 6\phi + 7 \\
(0,-1) & \phi^2 - 3\phi - 3 & \phi + 3 \\
(0,0) & 1 & 1 \\
(0,1) & \phi + 3 & \phi^2 - 3\phi - 3 \\
(1,-1) & -2\phi^2 + 6\phi + 7 & -2\phi^2 + 2\phi + 23 \\
(1,0) & \phi + 1 & -\phi^2 + \phi + 11 \\
(1,1) & \phi^2 + 4\phi + 3 & -\phi^2 + 2\phi + 7 \\
\hline
\end{array}|

Comparing coefficients of $\phi$, equation (2.24) eliminates all but $(r, s) = (0, -1), (0, 0), (1, -1)$, with corresponding units $\zeta = \epsilon_1 \epsilon_2^3 = \phi^2 - 3\phi - 3, 1, -2\phi^2 + 6\phi + 7$. It remains to treat the nine pairs of equations at (2.22), (2.23):

$$(2.26)$$

$C_1: (a + (-\phi^2 - 2\phi + 2)b)(a^2 + (-\phi^2 + 2\phi + 12)ab + (-2\phi^2 - 2\phi + 8)b^2) = \frac{1}{\lambda} \cdot \zeta \cdot \text{cube},$$

$C_2: (a + (\phi^2 - 2\phi - 6)b)(a^2 + (\phi^2 + 2\phi - 20)ab + (-6\phi^2 + 14\phi + 32)b^2) = \frac{1}{\lambda'} \cdot \zeta \cdot \text{cube},$

where $(\lambda, \lambda') = (1, 1), (4, 2), (2, 4)$ and $\zeta \in \{\phi^2 - 3\phi - 3, 1, -2\phi^2 + 6\phi + 7\}$. For each pairs of equations in (2.26), the elliptic curve Chabauty routine in Magma [1] works on either $C_1$ or $C_2$. The result is recorded in the following table, where $\emptyset$ means there are no solutions.

|\begin{array}{c|c|c|c|c|c|}
\hline
\lambda & (r, s) & \text{Curve} & \text{Rank} & \text{Cubic model} & (a, b) \\
\hline
1 & (0,-1) & C_2 & 1 & y^2 = x^3 + 9(-17\phi^2 + 16\phi + 193) & \emptyset \\
1 & (0,0) & C_2 & 1 & y^2 = x^3 + (3608020\phi^2 - 6430320\phi - 7101783) & (\pm 1, 0) \\
1 & (-1,1) & C_1 & 0 & y^2 = x^3 + (2168127\phi^2 - 6430320\phi - 7101783) & \emptyset \\
4 & (0,-1) & C_1 & 0 & y^2 = x^3 + (9204\phi^2 - 27144\phi - 30732) & \emptyset \\
4 & (0,0) & C_1 & 0 & y^2 = x^3 + (-4312\phi^2 + 312\phi + 4212) & \emptyset \\
4 & (1,-1) & C_1 & 1 & y^2 = x^3 + (28\phi^2 - 68\phi - 83) & \emptyset \\
2 & (0,-1) & C_2 & 1 & y^2 = x^3 + (28\phi^2 - 68\phi - 83) & \emptyset \\
2 & (0,0) & C_1 & 0 & y^2 = x^3 + (64584\phi^2 + 247104\phi + 169533) & \emptyset \\
\hline
\end{array}|

Table 1: Possible Values Of $(r, s)$

Table 2: Solutions Corresponding to the Values Of $(\lambda, r, s)$
\( y^2 = x^6 + k, \ k \in \{-39, -47\} \)

\[
\begin{array}{c|c|c|c|c|c}
2 & (1,-1) & C_2 & 1 & y^2 = x^3 + (7\phi^2 - 20\phi - 23) & \emptyset \\
\end{array}
\]

So \((a, b) = (\pm 1, 0)\). Hence \(|U| = |V| = 1\). Thus \(X = 2\) and \((x, y) = (\pm 2, \pm 5)\). \(\square\)

3. **Equation** \(y^2 = x^6 - 47\)

In this section, we will prove Theorem 1.2.

*Proof.* Equation \(y^2 = x^6 - 47\) is equivalent to

\[ Y^2 = X^6 - 47Z^6, \]

where \(X, Y, Z\) are coprime. We have

\[ (X^3 - Y)(X^3 + Y) = 47Z^6. \]

The \(\gcd(X^3 - Y, X^3 + Y)\) divides \(\gcd(2X^3, 2Y)\), so divides 2. We can choose the sign of \(Y\) such that \(47|X^3 + Y\).

Case \(gcd\) is 1:

\[ X^3 + Y = 47V^6, \quad X^3 - Y = U^6, \quad \gcd(U, V) = 1. \]

So

\[ 2X^3 = 47V^6 + U^6, \quad \gcd(U, V) = 1. \]

If \(13 \nmid UV\), then \(2X^3 \equiv \pm 1 \pm 47 \pmod{13}\). Thus \(4X^6 \equiv (1 \pm 5)^2 \pmod{13}\). So \(\pm 4 \equiv \pm 3 \pmod{13}\), impossible. Therefore \(13|UV\). If \(13|U\), then \(2X^3 \equiv 47V^6 \equiv \pm 5 \pmod{13}\). Thus \(4X^6 \equiv 25 \equiv -1 \pmod{13}\). So \(\pm 4 \equiv -1 \pmod{13}\), impossible. If \(13|V\), then \(2X^3 \equiv U^6 \pmod{13}\). Thus \(4X^6 \equiv U^{12} \equiv 1 \pmod{13}\). So \(\pm 4 \equiv \pm 1 \pmod{13}\), impossible.

Case \(gcd\) is 2:

Then

\[ X^3 + Y = 47 \cdot 2 \cdot V^6, \quad X^3 - Y = 25 \cdot U^6, \quad \gcd(U, V) = 1, \]

or

\[ X^3 + Y = 47 \cdot 2^5 \cdot V^6, \quad X^3 - Y = 2 \cdot U^6, \quad \gcd(U, V) = 1; \]

So

\[ X^3 = 47V^6 + 16U^6, \quad \gcd(U, V) = 1, \]

or

\[ X^3 = 47 \cdot 2^4 \cdot V^6 + U^6, \quad \gcd(U, V) = 1. \]

The latter case gives \((X/V^2)^3 = 752 + (U^3/V^3)^2\). The elliptic curve \(y^2 = x^3 - 752\) has rank 0, and the trivial torsion subgroup, implying \(V = 0\). So we only need to consider the case

\[ (3.1) \quad X^3 = 16U^6 + 47V^6. \]

From \(63^3 = 16 \cdot 5^3 + 47\), we would like to show that \(X = 63, \ |U| = |V| = 1\).

If \(3|U\), then from \((3.1)\), we have \(X^3 \equiv 47V^6 \equiv 2 \pmod{9}\). Thus \(X^6 \equiv 4 \pmod{9}\), so \(1 \equiv 4 \pmod{9}\), impossible. So \(3 \nmid U\). If \(3|V\), then \(X^3 \equiv 16U^6 \equiv -2 \pmod{9}\). Thus \(X^6 \equiv 4 \pmod{9}\), impossible. So \(3 \nmid V\). Therefore \(X^3 \equiv 0 \pmod{9}\), giving \(3|X\).

From \((3.1)\), we also have \(2 \nmid X, V\).

Let \(K = \mathbb{Q}(\theta)\), where \(\theta = \sqrt{-47}\). \(K\) has the class number 5, the trivial fundamental
unit group, and the ring of integers $\mathcal{O}_K = \mathbb{Z}[\frac{1+\theta}{2}]$. The class group of $K$ is generated by the ideal $I = (2, \frac{1+\theta}{2})$. Now

$$\text{(3.2)} \quad (X)^3 = (4U^3 + \theta V^3)(4U^3 - \theta V^3).$$

Let $J$ be a common ideal dividing both factors on the right side. Then

$$J|(8U^3), \quad J|(2\theta V^3), \quad J^2|(X)^3.$$

Taking norms gives

$$\text{Norm}(J)|64U^6, \quad \text{Norm}(J)|4 \cdot 47 \cdot V^6, \quad \text{Norm}(J)|X^3.$$

But $2 \nmid X$, so $\text{Norm}(J)|\gcd(X^3, U^6, 47V^6) = 1$. Therefore $(4U^3 + \theta V^3)$ and $(4U^3 - \theta V^3)$ are coprime ideals. Thus

$$\text{(3.3)} \quad 4U^3 + \theta V^3 = A^3,$$

with $A \in \mathcal{O}_K$. Let $A = u + v\left(\frac{1+\theta}{2}\right)$, where $u, v \in \mathbb{Z}$. Then

$$A^3 = (3/2u^2v + 3/2uv^2 - 11/2v^3)\theta + u^3 + 3/2u^2v - 69/2uv^2 - 35/2v^3.$$

$A^3 \in \mathbb{Z}[\theta]$ implies $u^3 + 3/2u^2v - 69/2uv^2 - 35/2v^3 \in \mathbb{Z}$, hence $\frac{u^2v - uv^2 - v^3}{2} \in \mathbb{Z}$. If $2 \nmid v$, then $\frac{u^2 - u - 1}{2} \in \mathbb{Z}$, impossible. So $2|v$. Therefore $A \in \mathbb{Z}[\theta]$. Let

$$4U^3 + \theta V^3 = (a + b\theta)^3,$$

where $a, b \in \mathbb{Z}$. Taking norms gives

$$X = a^2 + 47b^2.$$

$2|X$ implies $2 \nmid a, \ b; \ 3|X$ implies $3 \nmid a, \ b$. Expanding $(a + b\theta)^3$ gives

$$\text{(3.4)} \quad 4U^3 = a(a^2 - 141b^2), \quad V^3 = b(3a^2 - 47b^2).$$

In the second equation, we have

$$\gcd(b, 3a^2 - 47b^2) = \gcd(b, 3a^2) = \gcd(b, 3) = 1.$$

Further, $V$ is odd so $b$ is odd. $3a^2 - 47b^2|V^3$ so $3a^2 - 47b^2$ is odd, hence $a$ is even. Thus $a^2 - 141b^2$ is odd, so $4|a$. If $47|a$, then $47|v^3$ and $47|U^3$. So $47|\gcd(U, V)$, contradicting $\gcd(U, V) = 1$. Hence $47 \nmid a$, so $\gcd(a, a^2 - 141b^2) = 1$. Therefore from (3.4), we have

$$a = 4A^3, \quad b = B^3, \quad 3a^2 - 47b^2 = C^3, \quad a^2 - 141b^2 = D^3,$$

where $A, B, C, D \in \mathbb{Z}$, $AD = U, \ CB = V$.

Because $\gcd(U, V) = \gcd(a, b) = \gcd(a, 141) = \gcd(b, 3) = 1$, we have $A, B, C, D$ are coprime. Further, $3, 47 \nmid a, \ 3, 47 \nmid A, \ D; \ 2, 3 \nmid b$ so $2, 3 \nmid B, \ C$. Now

$$48A^6 - 47B^6 = C^3, \quad 16A^6 - 141B^6 = D^3.$$

We will show $|A| = |B| = 1$ and $C = 1, \ D = -5$. Indeed, we have

$$3C^3 - D^3 = 128A^6, \quad C^3 - 3D^3 = 376B^6.$$
\[ y^2 = x^6 + k, \ k \in \{-39, -47\} \]

Note that \( C^3 \equiv 3D^3 \mod 8 \) and \( 2 \nmid C \), so
\[
C \equiv 3D \mod 8.
\]

Also \( C^3 \equiv 3D^3 \mod 47 \) and \( 47 \nmid D \), so
\[
D \equiv -5C \mod 47.
\]

Let \( L = \mathbb{Q}(\phi) \), where \( \phi = \sqrt{3} \). \( L \) has class number 1, the ring of integers \( \mathcal{O}_L = \mathbb{Z}[\phi] \), and a fundamental unit \( \epsilon = \phi^2 - 2 \) of norm 1. The ideal \( (2) = p_2q_2 \), where \( p_2 = (-1 + \phi) \) and \( q_2 = (1 + \phi + \phi^2) \). The ideal \( (47) = p_{47}q_{47} \), where \( p_{47} = (2 + \phi + 2\phi^2) \) and \( q_{47} = (2 - 10\phi + 3\phi^2) \). Now
\[
(C - D\phi)(C^2 + CD\phi + D^2\phi^2) = 2^3 \cdot 47 \cdot B^6.
\]

Because
\[
\gcd(C - D\phi, C^2 + CD\phi + D^2\phi^2) = \gcd(C - D\phi, 3D^2\phi^2) = \gcd(C - D\phi, \phi^5) = 1,
\]

the two factors on the left are coprime.

We note that
\[
C - D\phi \equiv C(1 + 5\phi) \equiv 0 \mod p_{47},
\]
\[
C - D\phi \equiv D(3 - \phi) \equiv 0 \mod p_3.
\]

Thus
\[
C - D\phi = (-1)^h\epsilon^i p_{47}^j G^6,
\]

where \( G \in \mathcal{O}_L \), and \( 0 \leq h \leq 1, 0 \leq i, j, k \leq 5 \). Taking norms gives
\[
2^4 \cdot 47 \cdot B^6 = (-1)^h 2^j 4^k \epsilon^{i \phi^3} (C\phi^2)^6.
\]

So \( h \) is even, \( j \equiv 3 \mod 6 \), \( k \equiv 1 \mod 6 \). Thus \( (h, j, k) = (0, 3, 1) \). Then
\[
C - D\phi = \epsilon^i (13 - 10\phi + \phi^2) G^6.
\]

We claim that \( i = 5 \).

If \( i \equiv 0 \mod 2 \), then
\[
C - D\phi = (13 - 10\phi + \phi^2)(M + N\phi + P\phi^2)^2, \quad M, N, P \in \mathbb{Z}.
\]

Comparing coefficients of \( \phi^2 \) gives
\[
M^2 - 20MN + 13N^2 + 26MP + 6NP - 30P^2 = 0,
\]

which is locally unsolvable at 2. Thus \( i \) is odd.

If \( i = 3 \), then
\[
C - D\phi = (13 - 10\phi + \phi^2)(M + N\phi + P\phi^2)^3, \quad M, N, P \in \mathbb{Z}.
\]

Comparing coefficients of \( \phi^2 \) gives
\[
M^3 - 30M^2N + 39MN^2 + 3N^3 + 39M^2P + 18MPN - 90N^2P - 90MP^2 + 117NP^2 + 9P^3 = 0,
\]

which is locally unsolvable at 3.

If \( i = 1 \), then
\[
C - D\phi = (-56 + 23\phi + 11\phi^2)(M + N\phi + P\phi^2)^3, \quad M, N, P \in \mathbb{Z}.
\]

Comparing coefficients of \( \phi^2 \) gives
\[
11M^3 + 69M^2N - 168MN^2 + 33N^3 - 168M^2P + 198MPN + 207NP^2 + 207MP^2 - 504NP^2 + 99P^3 = 0,
\]

which is locally unsolvable at 3. Therefore \( i = 5 \), equivalently, on taking \( i = -1 \), we have
\[
C - D\phi = (1 + 5\phi) G^6.
\]
It follows that
\[(C - D\phi)(3C^3 - D^3) = 2(1 + 5\phi)(2AG)^6,\]
or
\[2(1 + 5\phi)(x - \phi)(3x^3 - 1) = y^2,
\]
where \(x = \frac{C}{D}\) and \(y = 2(1 + 5\phi)(2AG)^3/D^2\), representing an elliptic curve over \(L\).

The cubic model is
\[y^2 = x^3 + (-30\phi^2 + 174\phi + 36)x^2 + (9012\phi^2 + 5040\phi - 12708)x + (207576\phi^2 - 409536\phi + 449064).\]

This curve has rank 2. The Chabauty routine in Magma \([1]\) shows \(\frac{C}{D} = \frac{-1}{5}\). Hence \(C = 1, D = -5,\) and \(|A| = |B| = 1\). Therefore the only solutions to \(y^2 = x^6 - 47\) are \(x = \pm \frac{63}{10}\) and \(y = \pm \frac{249953}{10^3}\).

\[\square\]

References