ON THE DIOPHANTINE EQUATION $my^2 = x^3 - k^3$

SHENXING ZHANG

Abstract. In this paper, we study the integer solutions of $E_{k,m} : my^2 = x^3 - k^3$, where k has no prime factor $\equiv \pm 1 \bmod 12$. Without loss of generality, we may assume that $m > 0$ is square-free and $\gcd(m, k) = 1$. Let k' be the square-free part of k.

If km has no prime factor $\equiv 1 \bmod 6$, and satisfies certain congruence condition when k' is even, then we determine all integer solutions of $E_{k,m}$. We also show that there are infinitely many square-free m with at least $\omega + 2$ ($\omega+3$ if k' is even) prime factors $\equiv -1 \bmod 6$, such that $E_{k,m}$ only has a trivial integer solution $(k, 0)$, where ω is the number of prime factors $\equiv 1 \bmod 6$ of k'.

1. Introduction

In this paper, we will study the integer solutions of the quadratic twists of the elliptic curve $y^2 = x^3 - 1$. Since different forms may have different integer solutions, we will consider the following equation

$$E_{k,m} : my^2 = x^3 - k^3,$$

where k, m are non-zero integers. Denote by $E_{k,m}(\mathbb{Z})$ the set of integer solutions of $E_{k,m}$.

Clearly, $(k, 0) \in E_{k,m}(\mathbb{Z})$. Since

$$(x, y) \in E_{k,m}(\mathbb{Z}) \iff (-x, y) \in E_{-k,-m}(\mathbb{Z}),$$

we may assume that m is positive. If $m = m'm''^2$ where m' is square-free, then

$$(x, y) \in E_{k,m}(\mathbb{Z}) \implies (x, m''y) \in E_{k,m'}(\mathbb{Z}).$$

Thus we may assume that m is square-free. If $\gcd(k, m) > 1$, then

$$(x, y) \in E_{k,m}(\mathbb{Z}) \implies p \mid \gcd(x, y) \implies \left(\frac{x}{p}, \frac{y}{p}\right) \in E_{k/p,m/p}(\mathbb{Z}), \tag{1.1}$$

where p is a prime factor of $\gcd(k, m)$. Thus we may assume that $\gcd(k, m) = 1$. One can also note that

$$(x, y) \in E_{1,km}(\mathbb{Z}) \implies (kx, k^2y) \in E_{k,m}(\mathbb{Z}) \implies (kmx, k^2m^2y) \in E_{km,1}(\mathbb{Z}).$$

The case that $k = \pm 1, \pm 2$ is studied in several articles [Lju42, KS81b, KS81a, KS81c]. In this paper, we want to study the case that k has no prime factor $\equiv \pm 1 \bmod 12$ for a technical reason. We will keep this hypothesis from now on.

For any non-zero integer n, we will denote by

- n_+ the largest positive divisor of n, whose prime factors are $\equiv 1 \bmod 6$;

Date: March 27, 2025.

2020 *Mathematics Subject Classification.* Primary 11D25; Secondary 11G05.

Key words and phrases. elliptic curves; Diophantine equation; integer solutions.

- n_- the largest positive divisor of n, whose prime factors are $\equiv -1 \bmod 6$;
- $n_\bullet = \frac{n}{n_+ n_-}$ whose prime factors are 2 or 3;
- n' the square-free part of n;
- n'' a positive integer such that $n = n'n''^2$.

The first main result is: there are infinitely many square-free integers m with at least $\omega + 2$ ($\omega + 3$ if k' is even) prime factors $\equiv -1 \bmod 6$, where ω is the number of prime factors of k'_+.

Theorem 1.1. *Let k be a non-zero integer without prime factor $\equiv \pm 1 \bmod 12$. Denote by ω the number of prime factors of k'_+. Then for any non-negative integers $s \geq \omega+2$ ($s \geq \omega+3$ for even k') and t, there are infinitely many square-free integers*

$$m = p_1 \cdots p_t q_1 \cdots q_\omega,$$

such that

- $\gcd(k, m) = 1$*;*
- $p_1 \equiv \cdots \equiv p_t \equiv 1 \bmod 6, q_1 \equiv \cdots \equiv q_\omega \equiv -1 \bmod 6$*;*
- $E_{k,\delta m}(\mathbb{Z}) = \{(k, 0)\}$ *for any* $\delta \in \{1, 2, 3, 6\}$*.*

For any rational number r, denote by

$$d_r = \frac{(3r+1)(r-1)}{4r}.$$

The second main result is: if $k'_+ = m_+ = 1$, and $k'm$ satisfies certain congruence condition when k' is even, then we can determine the set $E_{k,m}(\mathbb{Z})$.

Theorem 1.2. *Let m be a positive square-free integer whose prime factors are $2, 3$ or $\equiv 5 \bmod 6$. Let k be a non-zero integer whose prime factors are $2, 3$ or $\equiv 5 \bmod 12$. Assume that*

(1) $\gcd(k, m) = 1$*;*
(2) *if k' is even, then $k'm \not\equiv 6 \bmod 8$, or $k'm \not\equiv 6, 14 \bmod 40$ if $3 \mid k'm$.*

If $(x, y) \in E_{k,m}(\mathbb{Z})$ with $y > 0$, then

$$x = kd_{\alpha/\beta}.$$

for a rational number α/β, where α and β are integers satisfying $\alpha\beta \mid k$, except

- $(x, y) = (2k''^2, 3k''^3)$*, if* $k = -k''^2, m = 1$*;*
- $(x, y) = (23k''^2, 78k''^3)$*, if* $k = -k''^2, m = 2$*.*

2. Preliminaries

Consider the following Pell's equation:

$$x^2 - 3y^2 = 1 \tag{2.1}$$

Denote by $\varepsilon = 2+\sqrt{3}$ the fundamental unit of $\mathbb{Q}(\sqrt{3})$. It's well-known that the non-negative integer solutions of (2.1) are $\{(x_n, y_n) \mid n \geq 0\}$, where $x_n + y_n\sqrt{3} = \varepsilon^n$. In other words,

$$x_n = \frac{1}{2}(\varepsilon^n + \varepsilon^{-n}), \qquad y_n = \frac{1}{2\sqrt{3}}(\varepsilon^n - \varepsilon^{-n}). \tag{2.2}$$

We list the first several terms here:

n	0	1	2	3	4	5	6	7
x_n	1	2	7	26	97	362	1351	5042
y_n	0	1	4	15	56	209	780	2911

Proposition 2.1. (1) $x_{n+1} = 2x_n + 3y_n, y_{n+1} = x_n + 2y_n$.

(2) $y_{2n+1} = 2x_{n+1}y_n + 1 = 2x_ny_{n+1} - 1$.

(3) *Modulo* 8,

$$x_n \equiv \begin{cases} (-1)^a, & n = 2a; \\ 2, & n = 2a+1, \end{cases} \qquad y_n \equiv \begin{cases} (-1)^a, & n = 2a+1; \\ 0, & n = 4a; \\ 4, & n = 4a+2. \end{cases}$$

(4) *Modulo* 3,

$$y_n \equiv \begin{cases} 0, & n = 3a; \\ 1, & n = 6a+1 \ \textit{or}\ 6a+2; \\ -1, & n = 6a+4 \ \textit{or}\ 6a+5. \end{cases}$$

(5) *Modulo* 5,

$$y_n \equiv \begin{cases} 0, & n = 3a; \\ 1, & n = 3a+1; \\ -1, & n = 3a+2. \end{cases}$$

(6) $(x_n, x_{n\pm1}) = (x_n, y_{n\pm1}) = 1$ *or* 2.

(7) *If* $n \geq 1$, *then neither* x_{2n} *nor* $2x_{2n+1}$ *is a square.*

(8) *The odd prime factors of* x_n *are* $\equiv 1 \bmod 6$.

Proof. (1)–(2) by direct calculations.

(3)–(5) by the relation

$$x_{n+2} = 4x_{n+1} - x_n, \qquad y_{n+2} = 4y_{n+1} - y_n$$

and induction on n.

(6) Since $x_n^2 - 3y_n^2 = 1$, we have $(x_n, y_n) = 1$ and $3 \nmid x_n$ for all n. Thus

$$(x_n, x_{n\pm1}) = (x_n, 2x_n \pm 3y_n) = (x_n, 3y_n) = 1,$$
$$(x_n, y_{n\pm1}) = (x_n, 2y_n \pm x_n) = (x_n, 2y_n) = 1 \text{ or } 2.$$

(7) If $x_{2n} = u^2$, then (u^2, uy_{2n}) is an integer solution of the elliptic curve $3Y^2 = X^3 - X$ whose Mordell-Weil rank is zero. Therefore, $y_{2n} = Y = 0$ and $n = 0$.

If $x_{2n+1} = 2u^2$ for some integer $u > 0$, then

$$3y_{2n+1}^2 = 4u^4 - 1 = (2u^2+1)(2u^2-1).$$

Note that $3 \nmid u$ and $\gcd(2u^2+1, 2u^2-1) = 1$, we have $2u^2 + 1 = 3a^2, 2u^2 - 1 = b^2$ for some integers $a > 0, b$. Thus

$$3a^2 = 4u^2 - b^2 = (2u+b)(2u-b).$$

It's easy to see that $\gcd(2u+b, 2u-b) = 1$. By choosing a suitable sign of b, we may assume that $2u + b = 3c^2, 2u - b = d^2, a = cd$ for some positive integers c, d. Then

$$d^4 - 1 = d^4 - (3a^2 - 2u^2) = 2\Big(\frac{3}{4}(c^2 - d^2)\Big)^2.$$

Note that d is odd, thus $d^2+1=2s^2, d^2-1=t^2$ for some integers s,t. Therefore, $d=1, t=0, c=1, a=1, u=1, n=0$.

(8) If $p>2$ is a prime factor of x, then $-3y^2 \equiv 1 \bmod p$ and $\left(\frac{-3}{p}\right)=1$. This implies that $p \equiv 1 \bmod 6$. □

3. General case

Proposition 3.1. *Let m be a positive square-free integer. Let k be a nonzero integer without prime factor $\equiv \pm 1 \bmod 12$. Assume that $\gcd(k,m)=1$ and*

(1) *for any $1<A \mid m_+$, there is a prime $p>3$ such that $p \mid \frac{m}{A}$ and $\left(\frac{A}{p}\right)=-1$; or, $p \mid k$ and $\left(\frac{A}{p}\right)=1$;*
(2) *for any $1<A \mid m_+$, there is a prime $p>3$ such that $p \mid \frac{m}{A}$ and $\left(\frac{3A}{p}\right)=-1$; or, $p \mid k$ and $\left(\frac{3A}{p}\right)=1$;*
(3) *if k' is odd, then for any $1<A \mid k'_+m_+$, there is a prime $p \mid \frac{k'm}{A}$, such that $p \equiv 1 \bmod 4$ and $\left(\frac{A}{p}\right)=-1$;*
(4) *if $k'm \equiv -1 \bmod 8$, then for any $1<A \mid k'_+m_+$, there is a prime $p \mid \frac{k'm}{A}$, such that $p \equiv 1 \bmod 4$ and $\left(\frac{2A}{p}\right)=-1$;*
(5) *if k' is even, then $k'm \not\equiv 6 \bmod 8$, or $k'm \not\equiv 6, 14 \bmod 40$ if $3 \mid k'm$.*

If $(x,y) \in E_{k,m}(\mathbb{Z})$ with $y>0$ and $\gcd(x,y)=1$, then

$$x = kd_{\alpha/\beta}$$

for a rational number α/β, where α and β are integers satisfying $\alpha\beta \mid k$, except

- *$(x,y)=(2k''^2, 3k''^3)$, if $k=-k''^2, m=1$;*
- *$(x,y)=(23k''^2, 78k''^3)$, if $k=-k''^2, m=2$.*

Proof. If $(x,y) \in E_{k,m}(\mathbb{Z})$ with $y>0$ and $\gcd(x,y)=1$, then $x>k$ and

$$my^2 = x^3-k^3 = (x-k)(x^2+kx+k^2).$$

One can easily show that $\gcd(k,x)=\gcd(k,y)=1$ and

$$\gcd(x-k, x^2+kx+k^2) = \gcd(x-k, 3k^2) = 1 \text{ or } 3.$$

If k is odd, then clearly x^2+kx+k^2 is odd. If k is even, then both x,y are odd, and so is x^2+kx+k^2. Therefore, we may assume that

$$\begin{cases} x^2+kx+k^2 = \delta_1 M a^2, \\ x-k = \delta_2 \frac{m}{M} b^2, \end{cases} \tag{3.1}$$

where M,a,b are positive integers, $M \mid m_+m_-$ and

$$(\delta_1,\delta_2) = (1,1) \text{ or } \begin{cases} (3,3), & \text{if } 3 \nmid m; \\ (3,1/3), & \text{if } 3 \mid m. \end{cases}$$

Let p be a prime factor of M. Then $p>3$ and p divides

$$4\delta_1 M a^2 = (2x+k)^2 + 3k^2.$$

Since $p \nmid k$ and $(2x+k)^2 \equiv -3k^2 \bmod p$, we have $\left(\frac{-3}{p}\right) \equiv 1$ and $p \equiv 1 \bmod 6$. Therefore, $M \mid m_+$.

If $M>1$, then one of the following cases will happen by Assumptions (1) and (2).

- There exists a prime $p > 3$ such that $p \mid \frac{m}{M}$ such that $\left(\frac{3\delta_1 M}{p}\right) = -1$. Then $x \equiv k \bmod p$ and $\delta_1 M a^2 \equiv 3k^2 \bmod p$ by (3.1). Since $p \nmid k$, this contradicts to $\left(\frac{3\delta_1 M}{p}\right) = -1$.
- There exists a prime $p > 3$ such that $p \mid k$ such that $\left(\frac{3\delta_1 M}{p}\right) = 1$. Then $\delta_1 M a^2 \equiv x^2 \bmod p$ by (3.1). Since $p \nmid x$ and $p \equiv \pm 5 \bmod 12$, this contradicts to $\left(\frac{\delta_1 M}{p}\right) = -\left(\frac{3\delta_1 M}{p}\right) = -1$.

Hence $M = 1$ and

$$\begin{cases} x^2 + kx + k^2 = \delta_1 a^2, \\ x - k = \delta_2 m b^2. \end{cases}$$

One can see that

$$\delta_1 (2a)^2 - (2\delta_2 m b^2 + 3k)^2 = 3k^2. \tag{3.2}$$

(1) The case $\delta_1 = \delta_2 = 1$. Then

$$(2a)^2 - (2mb^2 + 3k)^2 = 3k^2.$$

Denote by $X = 2a$ and $Y = 2mb^2 + 3k$. Then $X > |Y|$. Denote by

$$t = \gcd(X + Y, X - Y),$$

then

$$X \pm Y = 3\alpha^2 t, \qquad X \mp Y = \beta^2 t$$

for some integers $\alpha > 0$ and β with $\alpha\beta t = k$. Thus

$$Y = \pm\frac{1}{2}(3\alpha^2 - \beta^2)t = \pm\frac{3\alpha^2 - \beta^2}{2\alpha\beta}k = \frac{3r^2 - 1}{2r}k$$

where $r = \pm\alpha/\beta$. Therefore,

$$x = \frac{Y - k}{2} = \frac{3r^2 - 2r - 1}{4r}k = kd_r.$$

(2) The case $\delta_1 = 3$. Denote by $b_1 = b\sqrt{\delta_2/3}$. Then $x = k + 3mb_1^2$ and

$$(2a)^2 - 3(2mb_1^2 + k)^2 = k^2$$

and $b_1 \in \mathbb{Z}$. Let $\mu = \gcd(2a, 2mb_1^2, k)$ and denote by

$$X = \frac{2a}{\mu}, \quad Y = \frac{2mb_1^2 + k}{\mu}, \quad Z = \frac{k}{\mu}.$$

Then $X^2 - 3Y^2 = Z^2$ and $\gcd(X, Y, Z) = 1$. If $\mu < |k|$, then there is a prime p dividing $Z = k/\mu$.

- If $p \equiv \pm 5 \bmod 12$, then $p \nmid XY$ and $X^2 \equiv 3Y^2 \bmod p$, which contradicts to $\left(\frac{3}{p}\right) = -1$.
- If $p = 2$, then Z is even and X, Y are odd. This implies that $Z^2 = X^2 - 3Y^2 \equiv -2 \bmod 8$, which is impossible.
- If $p = 3$, then $3 \mid Z$ and $3 \mid X$. This implies that $9 \mid 3Y^2$ and $3 \mid Y$, which contradicts to $\gcd(X, Y, Z) = 1$.

Hence $\mu = |k|$,

$$X = \frac{2a}{|k|}, \quad Y = \frac{2mb_1^2 + k}{|k|} = \frac{2mb_1^2}{|k|} + \operatorname{sgn}(k)$$

and $X^2 - 3Y^2 = 1$.

(2A) The case that k' is odd. Denote by $b_2 = b_1/(k'k'') \in \mathbb{Z}$. Then

$$Y = 2|k'|mb_2^2 + \operatorname{sgn}(k)$$

is odd. Thus

$$Y = y_{2i+1} = \begin{cases} 2x_{i+1}y_i + 1, & \text{if } k > 0 \\ 2x_i y_{i+1} - 1, & \text{if } k < 0 \end{cases} = 2x_j y_{j^*} + \operatorname{sgn}(k).$$

for some i, where y_i is given in (2.2) and

$$j = \begin{cases} i+1, & \text{if } k > 0; \\ i, & \text{if } k < 0, \end{cases} \qquad j^* = 2i + 1 - j.$$

- Assume that j is even. By Proposition 2.1 (3), we have

  $$|k'|mb_2^2 = x_j y_{j^*} \equiv (-1)^i = -\operatorname{sgn}(k) \bmod 8.$$

  Then b_2 is odd and $k'm \equiv -1 \bmod 8$. In other words, $k'm \not\equiv -1 \bmod 8$ will cause a contradiction.

  Assume that $k'm \equiv -1 \bmod 8$. By Proposition 2.1 (6) and (8), x_j is odd with prime factors $\equiv 1 \bmod 6$ and $\gcd(x_j, y_{j^*}) = 1$. We may write

  $$x_j = Nu^2, \qquad y_{j^*} = \frac{|k'|m}{N}v^2$$

  for some positive integers $N \mid k'_+ m_+$ and u, v.
  - If $N > 1$, then there exists a prime $3 < p \mid \frac{k'm}{N}$ such that $\left(\frac{\pm 2N}{p}\right) = -1$ by Assumption (4). If $k > 0$, then

    $$x_i = \frac{1}{2}(x_{i+1} - 3y_i) \equiv \frac{1}{2}Nu^2 \bmod p;$$

    if $j < 0$, then

    $$x_{i+1} = \frac{1}{2}(x_i + 3y_{i+1}) \equiv \frac{1}{2}Nu^2 \bmod p.$$

    Since $x_{j^*}^2 - 3y_{j^*}^2 = 1$, we have $\frac{1}{2}Nu^2 \equiv x_{j^*} \equiv \pm 1 \bmod p$, which contradicts to $\left(\frac{\pm 2N}{p}\right) = -1$.
  - If $N = 1$, then $x_j = u^2$ and $j = 0$ by Proposition 2.1 (7). This implies that

    $$i = 0, \quad k < 0, \quad -k'mb_2^2 = x_0 y_1 = 1.$$

    Thus $m = 1, k = -k''^2$, $x = k + 3mb_1^2 = 2k''^2$ and $y = 3k''^3$.
- Assume that j is odd. Then $x_j \equiv 2 \bmod 8$. Similarly

  $$x_j = 2Nu^2, \qquad y_{j^*} = \frac{2|k'|m}{N}v^2$$

  for some positive integers $N \mid k'_+ m_+$ and u, v.

– If $N > 1$, then there exists a prime $3 < p \mid \frac{k'm}{N}$ such that $\left(\frac{\pm N}{p}\right) = -1$ by Assumption (3). Then similarly

$$x_{j^*} = \frac{1}{2}\big(x_j - 3\,\mathrm{sgn}(k) y_{j^*}\big) \equiv Nu^2 \bmod p.$$

Since $x_{j^*}^2 - 3y_{j^*}^2 = 1$, we have $Nu^2 \equiv x_{j^*} \equiv \pm 1 \bmod p$, which contradicts to $\left(\frac{\pm N}{p}\right) = -1$.

– If $N = 1$, then $x_j = 2u^2$ and $j = 1$ by Proposition 2.1 (7). If $k > 0$, then $i = 0$ and $k'mb_2^2 = x_1 y_0 = 0$, which is impossible. If $k < 0$, then $i = 1$ and

$$-k'mb_2^2 = x_1 y_2 = 8.$$

Thus $k = -k''^2$, $m = 2$, $x = k + 3mb_1^2 = 23k''^2$ and $y = 78k''^3$.

(2B) The case that k' is even. Since $\gcd(k, m) = \gcd(k, x) = \gcd(k, y) = 1$, $m, x = k + 3mb_1^2, y$ are all odd, so is b_1. Denote by $b_2 = 2b_1/(k'k'')$. Then

$$Y = \left|\frac{k'mb_2^2}{2} + 1\right|$$

is even and $Y = y_{2i}$ for some i. Since $4 \mid y_{2i}$, we obtain that

$$k'm \equiv -2 \equiv 6 \bmod 8,$$

which contradicts to Assumption (5) if $3 \nmid k'm$.

If $3 \mid k'm$, then

$$y_{2i} = Y \equiv \mathrm{sgn}(k) \bmod 3.$$

This implies that $i \equiv \mathrm{sgn}(k) \bmod 3$ by Proposition 2.1 (4). By Proposition 2.1 (5),

$$y_{2i} \equiv -\mathrm{sgn}(k) \bmod 5, \qquad \frac{k'mb_2^2}{2} = \mathrm{sgn}(k) y_{2i} - 1 \equiv -2 \bmod 5.$$

Thus $5 \nmid k'mb_2$ and $k'm \equiv \pm 1 \bmod 5$. Since $k'm \equiv 6 \bmod 8$, we have $k'm \equiv 6, 14 \bmod 40$. This contradicts to Assumption (5). $\square$

If we enhance the conditions in Proposition 3.1, one can determine all integer solutions of $E_{k,m}$.

Proposition 3.2. *Let m be a positive square-free integer. Let k be a nonzero integer without prime factor $\equiv \pm 1 \bmod 12$. Let k' be the square-free part of k. Assume that $\gcd(k, m) = 1$ and*

(1) *for any $1 < A \mid k'_+ m_+$, there is a prime $3 < p \mid m$, such that $p \nmid A$ and $\left(\frac{A}{p}\right) = -1$;*
(2) *for any $1 < A \mid k'_+ m_+$, there is a prime $3 < p \mid m$, such that $p \nmid A$ and $\left(\frac{3A}{p}\right) = -1$;*
(3) *for any $1 < A \mid k'_+ m_+$, there is a prime $p \mid \frac{k'm}{A}$, such that $p \equiv 1 \bmod 4$ and $\left(\frac{A}{p}\right) = -1$;*
(4) *if $k'm \equiv -1 \bmod 8$, then for any $1 < A \mid k'_+ m_+$, there is a prime $3 < p \mid \frac{k'm}{A}$, such that $p \equiv 1 \bmod 4$ and $\left(\frac{2A}{p}\right) = -1$;*
(5) *if k' is even, then $k'm \not\equiv 6 \bmod 8$, or $k'm \not\equiv 6, 14 \bmod 40$ if $3 \mid k'm$.*

If $(x, y) \in E_{k,m}(\mathbb{Z})$ with $y > 0$, then

$$x = kd_{\alpha/\beta}$$

for a rational number α/β, where α and β are integers satisfying $\alpha\beta \mid k$, except

- $(x, y) = (2k''^2, 3k''^3)$, *if* $k = -k''^2, m = 1$;
- $(x, y) = (46k''^2, 78k''^3)$, *if* $k = -k''^2, m = 2$.

Proof. Let (x, y) be an integer solution of $E_{k,m}$ with $y > 0$. Denote the prime decomposition of $\gcd(x, k)$ by

$$\gcd(x,k) = \prod_i \mathfrak{p}_i^{2\alpha_i} \prod_j \mathfrak{q}_j^{2\beta_j+1},$$

where $\mathfrak{p}_i, \mathfrak{q}_j$ are different primes. Let

$$\widetilde{x} = \frac{x}{\gcd(x,k)}, \qquad \widetilde{y} = y \cdot \prod_i \mathfrak{p}_i^{-3\alpha_i} \prod_j \mathfrak{q}_j^{-3\beta_j-2},$$
$$\widetilde{k} = \frac{k}{\gcd(x,k)}, \qquad \widetilde{m} = m \cdot \prod_j \mathfrak{q}_j.$$

Then $\gcd(\widetilde{x}, \widetilde{k}) = 1$ and

$$\widetilde{m}\widetilde{y}^2 = \widetilde{x}^3 - \widetilde{k}^3.$$

If p is a prime factor of $\gcd(\widetilde{x}, \widetilde{y})$, then $p \mid \widetilde{k}$, which contradicts to $\gcd(\widetilde{x}, \widetilde{k}) = 1$. Thus $\gcd(\widetilde{x}, \widetilde{y}) = 1$.

- Since $\gcd(k, m) = 1$, $\mathfrak{q}_j \nmid m$ and then $\widetilde{m} > 0$ is still a square-free positive integer.
- $\widetilde{k}$ is still a non-zero integer without prime factors $\equiv \pm 1 \bmod 12$;
- If p is a prime factor of $\gcd(\widetilde{k}, \widetilde{m})$, then p divides both $\widetilde{x}$ and $\widetilde{y}$, which contradicts to $\gcd(\widetilde{x}, \widetilde{y}) = 1$. Thus $\gcd(\widetilde{k}, \widetilde{m}) = 1$.
- Since $\gcd(\widetilde{k}, \widetilde{m}) = 1$, we have $\mathfrak{q}_j \nmid \widetilde{k}$, $\mathfrak{q}_j \mid k'$ and then

  $$\widetilde{k}' = k' \cdot \prod_j \mathfrak{q}_j^{-1}.$$

  Thus $\widetilde{k}'\widetilde{m} = k'm$.

  Therefore, for any $1 < A \mid \widetilde{m}_+$, we have $A \mid k'_+ m_+$ and there is a prime $3 < p \mid m \mid \widetilde{m}$, such that $p \nmid A$ and $\left(\frac{A}{p}\right) = -1$. In other words, Assumption (1) in Proposition 3.1 holds for $E_{\widetilde{k},\widetilde{m}}$. Similarly, Assumptions (2)–(3) in Proposition 3.1 also hold for $E_{\widetilde{k},\widetilde{m}}$.
- If $\widetilde{k}'\widetilde{m} \equiv -1 \bmod 8$, then $k'm \equiv -1 \bmod 8$. Thus Assumption (4) in Proposition 3.1 holds for $E_{\widetilde{k},\widetilde{m}}$.
- If $\widetilde{k}'$ is even, then k' is even. Since $\widetilde{k}'\widetilde{m} = k'm$, Assumption (5) in Proposition 3.1 holds for $E_{\widetilde{k},\widetilde{m}}$.

By Proposition 3.1, one of the following cases will happen:

- If

  $$\widetilde{k} = -\widetilde{k}''^2, \qquad \widetilde{m} = 1, \qquad \widetilde{x} = 2\widetilde{k}''^2, \qquad \widetilde{y} = 3\widetilde{k}''^3,$$

  then

  $$k = -k''^2, \qquad m = 1, \qquad x = 2k''^2, \qquad y = 3k''^3.$$

- If

  $$\widetilde{k} = -\widetilde{k}''^2, \qquad \widetilde{m} = 2, \qquad \widetilde{x} = 23\widetilde{k}''^3, \qquad \widetilde{y} = 78\widetilde{k}''^3,$$

then

$$\begin{aligned} &k = -k''^2, && m = 2, && x = 23k''^2, && y = 78k''^3 \\ \text{or} \quad &k = -2k''^2, && m = 1, && x = 46k''^2, && y = 312k''^3. \end{aligned}$$

The second case contradicts to the assumption $k'm \not\equiv 6 \mod 8$ since $k' = -2$ is even.

- If
$$\widetilde{x} = \widetilde{k} d_{\alpha/\beta}$$
for some integers $\alpha > 0, \beta$ satisfying $\alpha\beta \mid \widetilde{k}$, then $\alpha\beta \mid k$ and
$$x = kd_{\alpha/\beta}.$$

Hence we finish the proof. □

Remark 3.3. If k' is even and Assumption (5) does not hold, $E_{k,m}$ may have other possible integer solutions. For example, $(5 \times 167, 3 \times 5^2 \times 97) \in E_{10,11}(\mathbb{Z})$, but there is no rational number r such that $10d_r = 5 \times 167$.

If $k'_+ = m_+ = 1$, then Assumptions (1)–(4) holds automatically. Thus we get Theorem 1.2 immediately.

Now let's prove Theorem 1.1.

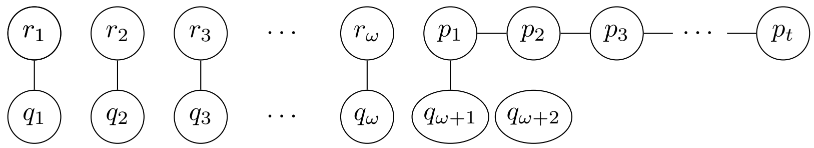
Proof of Theorem 1.1. Denote the prime decomposition of k'_+ by
$$k'_+ = r_1 \cdots r_\omega.$$
We may assume that $t \geq 1$ since $t = 0$ case is similar. Construct m as follows:

- Choose a prime $p_t \nmid k$ such that $p_t \equiv 1 \bmod 24$ and
$$\left(\frac{p_t}{r_1}\right) = \cdots = \left(\frac{p_t}{r_\omega}\right) = 1.$$
- Inductively choose primes $p_j \nmid k$ $(j = t-1, \ldots, 2, 1)$ such that $p_j \equiv 1 \bmod 24$ and
$$\left(\frac{p_j}{r_1}\right) = \cdots = \left(\frac{p_j}{r_\omega}\right) = 1, \quad \left(\frac{p_j}{p_{j+2}}\right) = \cdots = \left(\frac{p_j}{p_t}\right) = 1, \quad \left(\frac{p_j}{p_{j+1}}\right) = -1.$$
- Choose prime $q_i \nmid k$ $(i = 1, \ldots, \omega)$ such that $q_i \equiv 17 \bmod 24$ and
$$\left(\frac{q_i}{r_j}\right) = 1, \forall j \neq i, \quad \left(\frac{q_i}{r_i}\right) = -1, \quad \left(\frac{q_i}{p_1}\right) = \cdots = \left(\frac{q_i}{p_t}\right) = 1.$$
- Choose a prime $q_{\omega+1} \nmid k$ such that $q_{\omega+1} \equiv 17 \bmod 24$ and
$$\left(\frac{q_{\omega+1}}{r_1}\right) = \cdots = \left(\frac{q_{\omega+1}}{r_\omega}\right) = 1, \quad \left(\frac{q_{\omega+1}}{p_2}\right) = \cdots = \left(\frac{q_{\omega+1}}{p_t}\right) = 1, \quad \left(\frac{q_{\omega+1}}{p_1}\right) = -1.$$
- Choose a prime $q_{\omega+2} \nmid k$ such that $q_{\omega+2} \equiv 17 \bmod 24$ and
$$\left(\frac{q_{\omega+2}}{r_1}\right) = \cdots = \left(\frac{q_{\omega+2}}{r_\omega}\right) = 1, \quad \left(\frac{q_{\omega+2}}{p_1}\right) = \cdots = \left(\frac{q_{\omega+2}}{p_t}\right) = 1.$$
- If k' is odd, choose primes $q_i \nmid k$ $(i = \omega+3, \ldots, s)$ such that $q_i \equiv 17 \bmod 24$.
- If k' is even, choose primes $q_i \nmid k$ $(i = \omega + 3, \ldots, s - 1)$ such that $q_i \equiv 17 \bmod 24$; choose a prime $q_s \nmid k$ such that $q_s \equiv 5 \bmod 6$ and $k'm \not\equiv 6 \bmod 8$.

Figuratively speaking, if we denote by G the graph with

- vertex set $V(G) = \{r_1, \ldots, r_\omega, p_1, \ldots, p_t, q_1, \ldots, q_{\omega+2}\}$;
- edge set $E(G) = \{\overline{\mathfrak{pq}} \mid \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right) = -1\}$,

then G has the following form (the possible edges $\overline{r_ir_j}$, $\overline{q_iq_j}$ are omitted):



Let $A > 1$ be a divisor of $k'_+ m_+ = r_1 \cdots r_\omega p_1 \cdots p_t$. If $\gcd(A, m_+) > 1$, let j be the minimal integer such that $p_j \mid A$. If $j > 1$, then $\left(\frac{A}{p_{j-1}}\right) = \left(\frac{2A}{p_{j-1}}\right) = \left(\frac{3A}{p_{j-1}}\right) = -1$; if $j = 1$, then $\left(\frac{A}{q_{\omega+1}}\right) = \left(\frac{2A}{q_{\omega+1}}\right) = -1$, $\left(\frac{3A}{q_{\omega+2}}\right) = -1$. If $\gcd(A, m_+) = 1$, then $r_i \mid A$ for some i and $\left(\frac{A}{q_i}\right) = \left(\frac{2A}{q_i}\right)$, $\left(\frac{3A}{q_{\omega+2}}\right) = -1$.

Denote by $\gamma = \gcd(k, \delta)$. Then Assumptions (1)–(5) in Proposition 3.2 hold for $E_{k/\gamma, \delta m/\gamma}$. Since there are at most finitely many rational numbers $r = \alpha/\beta$, such that α and β are integers satisfying $\alpha\beta \mid \frac{k}{\gamma}$, there are at most finitely many possible x such that $(x, y) \in E_{k/\gamma, \delta m/\gamma}(\mathbb{Z})$ for some m. By (1.1), there are at most finitely many possible x such that $(x, y) \in E_{k,\delta m}(\mathbb{Z})$ for some m. Since δm is the square-free part of $x^3 - k^3$ if $x > k$, there are at most finitely many m we constructed such that $E_{k,m}, E_{k,2m}, E_{k,3m}$ or $E_{k,6m}$ has an integer solution with $y > 0$. Hence there are infinitely many m we constructed such that $E_{k,\delta m}(\mathbb{Z}) = \{(k, 0)\}$ for any $\delta \in \{1, 2, 3, 6\}$. □

Remark 3.4. By [Liv95], the root number of $E_{k,m}$ is

$$w(E_{k,m}) = \begin{cases} \left(\frac{-1}{n}\right), & \varepsilon = \pm 1, \pm 3; \\ +1, & \varepsilon = 2, -6; \\ -1, & \varepsilon = -2, 6, \end{cases}$$

where $n = k_+ k_- m_+ m_-$ and $\varepsilon = km/n$. If the BSD conjecture holds, then $E_{k,\delta m}$ we constructed may have nonzero Mordell-Weil rank, although $E_{k,\delta m}(\mathbb{Z})$ is trivial.

Remark 3.5. One can show that $|x| = |kd_{\alpha/\beta}| \leq k^2$ for any integers α, β satisfying $\alpha\beta \mid k$. In general, Hall in [Hal71] conjectured that: for every $\epsilon > 0$, there is a constant C_ϵ, depending only on ϵ, such that for all $D \in \mathbb{Z}$ with $D \neq 0$ and for all $x, y \in \mathbb{Z}$ satisfying $y^2 = x^3 + D$, we have $|x| \leq C_\epsilon D^{2+\epsilon}$.

4. Corollaries with $k'_+ = m_+ = 1$

In this section, we will give some corollaries with $k'_+ = m_+ = 1$. If $m = 1, 2$, $3 \mid m$ or m has a prime factor $\equiv 5 \bmod 12$, we have the following result.

Corollary 4.1. *Let k be a non-zero square-free integer whose prime factors are $2, 3$ or $\equiv 5 \bmod 12$.*

(1) *If k is odd, then*

$$E_{k,1}(\mathbb{Z}) = \begin{cases} \{(-1, 0), (0, \pm 1), (2, \pm 3)\}, & \text{if } k = -1; \\ \{(k, 0)\}, & \text{otherwise.} \end{cases}$$

(2) *If k is even, we assume that $k \not\equiv 6 \bmod 8$, or $k \not\equiv 6, 14 \bmod 20$ if $3 \mid k$. Then*

$$E_{k,1}(\mathbb{Z}) = \{(k, 0)\}.$$

(3) *If k is odd, then*

$$E_{k,2}(\mathbb{Z}) = \begin{cases} \{(-1,0),(1,\pm 1),(23,\pm 78)\}, & \text{if } k=-1;\\ \{(k,0),(x_0,\pm y_0)\}, & \text{if } 6\alpha_0^2 - 12\alpha_0\beta_0 - 2\beta_0^2 \text{ is a square};\\ \{(k,0)\}, & \text{otherwise,}\end{cases}$$

where β_0 is the product of prime factors $\equiv 5 \bmod 24$ of k, $\alpha_0 = k/\beta_0$ and

$$x_0 = \frac{1}{4}(3\alpha_0+\beta_0)(\alpha_0-\beta_0), \quad y_0 = \frac{1}{16}(3\alpha_0^2+\beta_0^2)\sqrt{6\alpha_0^2-12\alpha_0\beta_0-2\beta_0^2}.$$

(4) *Let m be a square-free positive integer prime to k, whose primes factors are $2, 3$ or $\equiv 5 \bmod 6$. If $3 \mid m$ or m has a prime factor $\equiv 5 \bmod 12$, then*

$$E_{k,m}(\mathbb{Z}) = \{(k,0)\}.$$

Proof. If $(x,y) \in E_{-1,1}(\mathbb{Z})$ or $E_{-1,2}(\mathbb{Z})$, then $(x,y) = (-1,0),(2,\pm 3),(23,\pm 78)$ or

$$x = -d_1 = 0, \ -d_{-1} = 1.$$

Thus

$$E_{-1,1}(\mathbb{Z}) = \{(-1,0),(0,\pm 1),(2,\pm 3)\},$$
$$E_{-1,2}(\mathbb{Z}) = \{(-1,0),(1,\pm 1),(23,\pm 78)\}.$$

Assume that $k \neq -1$ from now on. Let m be a square-free positive integer prime to k, whose primes factors are $2, 3$ or $\equiv 5 \bmod 6$. By Corollary 1.2, if $(x,y) \in E_{k,m}(\mathbb{Z})$ with $y \neq 0$, then

$$x = \frac{(3\alpha+\beta)(\alpha-\beta)}{4\alpha\beta}k$$

for some integers α, β satisfying $\alpha\beta \mid k$. Clearly, $\gcd(\alpha,\beta)=1$. If $\alpha-\beta$ is odd, then k is even and $4x$ is odd, which is impossible. Thus $\alpha\beta$ is odd. Denote by $t = k/(\alpha\beta)$ and $\gamma = (\alpha-\beta)/2$. One can obtain that

$$my^2 = x^3 - k^3 = t^3(3\gamma^2-\beta^2)\Big(\frac{3\alpha^2+\beta^2}{4}\Big)^2.$$

Since $\gcd(t,m)=1$, we have $3\gamma^2-\beta^2 = tms^2$ for some integer s. If $p>3$ is a prime factor of $3\gamma^2-\beta^2$, then $\big(\frac{3}{p}\big)=1$ and $p \equiv \pm 1 \bmod 12$.

(1) If m has a prime factor $\equiv 5 \bmod 12$, then $3\gamma^2-\beta^2 = tms^2$ cannot hold. Therefore, $E_{k,m}(\mathbb{Z}) = \{(k,0)\}$.

(2) If $3 \mid m$, then $3 \mid \beta$ and $3 \mid k$, which contradicts to $\gcd(k,m)=1$. Therefore, $E_{k,m}(\mathbb{Z}) = \{(k,0)\}$.

(3) If $m=1$, then $t \mid \gcd(6,k)$ since $t \mid k$ has no prime factor $\equiv \pm 1 \bmod 12$. We have $3\gamma^2-\beta^2 = ts^2$.

- If $3 \mid t$, then $3 \mid \beta$, which contradicts to $k = t\alpha\beta$.
- If $t = 1$ or -2, then $3\gamma^2 - ts^2 = \beta^2$, which contradicts to the Hilbert symbol $(3,-t)_3 = -1$.
- If $t=-1$, then $3\gamma^2+s^2=\beta^2$. If $p>3$ is a prime factor of β, then $\big(\frac{-3}{p}\big)=1$, which contradicts to $p \equiv 5 \bmod 12$. Thus $\beta \mid 3$. One can easily show that $\alpha=\beta=\pm 1, k=-1$ and $x=0$.
- If $t=2$, then $3\gamma^2-\beta^2=2s^2$. Since β is odd, so is γ. Therefore,

$$k = 2\alpha\beta = 4\gamma\beta + 2\beta^2 \equiv 6 \bmod 8,$$

which contradicts to the assumption $k \not\equiv 6 \bmod 8$.

(4) If $m = 2$ and k is odd, then $t \mid \gcd(3, k)$ since $t \mid k$ has no prime factor $\equiv \pm 1 \bmod 12$. We have $3\gamma^2 - \beta^2 = 2ts^2$.

- If $t = \pm 3$, then $3 \mid \beta$, which contradicts to $k = t\alpha\beta$.
- If $t = -1$, then $3\gamma^2 + 2s^2 = \beta^2$, which contradicts to the Hilbert symbol $(3, 2)_3 = -1$.
- If $t = 1$, then $2s^2 = 3\gamma^2 - \beta^2$. It's well-known that all rational solutions of this equation in $\mathbb{P}^2_{\mathbb{Q}}$ can be parametrized by

$$h = \frac{s - \beta}{\gamma - \beta} = \frac{a}{b}, \quad \gcd(a, b) = 1.$$

Then one can get

$$\begin{aligned} \gamma &= (2a^2 - 4ab + 3b^2)/u, \\ s &= -(2a^2 - 6ab + 3b^2)/u, \\ \beta &= (2a^2 - 3b^2)/u, \\ \alpha &= (6a^2 - 8ab + 3b^2)/u \end{aligned}$$

for some u. One can show that

$$|u| = \gcd(6a^2 - 8ab + 3b^2, 2a^2 - 3b^2) = \gcd(3, a)\gcd(2, b) = 1, 2, 3 \text{ or } 6.$$

If $p > 3$ is a prime factor of $\alpha \mid k$, then $p \mid 2a^2 + (4a - 3b)^2$. Thus $\left(\frac{-2}{p}\right) = 1$ and $p \equiv 17 \bmod 24$. If p is a prime factor of $\beta \mid k$, then $p \mid 2a^2 - 3b^2$. Thus $\left(\frac{6}{p}\right) = 1$ and $p \equiv 5 \bmod 24$. Therefore, $\beta = \beta_0$ or $3\beta_0$. If $\beta = 3\beta_0$, then $3 \mid a, 3 \mid u$ and $3 \nmid b$, which implies that $3 \nmid \beta$. Hence $\beta = \beta_0, \alpha = k/\beta_0$, and

$$16s^2 = 6\alpha_0^2 - 12\alpha_0\beta_0 - 2\beta_0^2$$

is a square. □

Example 4.2. If $\alpha_0 = -1, \beta_0 = 5$, then $6\alpha_0^2 - 12\alpha_0\beta_0 - 2\beta_0^2 = 16$ is a square. Therefore,

$$E_{-5,2}(\mathbb{Z}) = \{(-5, 0), (-3, \pm 7)\}.$$

Example 4.3. Let m be a square-free positive integer prime to k. Assume that $m_+ = k'_+ = 1$. If k' is even, assume that $k'm \not\equiv 6 \bmod 8$, or $k'm \not\equiv 6, 14 \bmod 40$ if $3 \nmid k'm$.

(1) Note that

$$d_1 = d_{-1/3} = 0, \quad d_{-1} = d_{1/3} = -1, \quad 3d_3 = 5, \quad 3d_{-3} = 8.$$

If $k \mid 6$, it's not hard to show that

$$E_{k,m}(\mathbb{Z}) = \begin{cases} \{(-1, 0), (0, \pm 1), (2, \pm 3)\}, & \text{if } k = -1, m = 1; \\ \{(-1, 0), (1, \pm 1), (23, \pm 78)\}, & \text{if } k = -1, m = 2; \\ \{(3, 0), (5, \pm 7)\}, & \text{if } k = 3, m = 2; \\ \{(-3, 0), (8, \pm 7)\}, & \text{if } k = -3, m = 11; \\ \{(6, 0), (10, \pm 28)\}, & \text{if } k = 6, m = 1; \\ \{(k, 0)\}, & \text{otherwise.} \end{cases}$$

The case that $k = \pm 1, \pm 2$ can be found in [Lju42, KS81b, KS81a, KS81c].

(2) Note that

$$
\begin{gathered}
5d_5 = 5d_{-1/15} = 16, \quad 5d_{-5} = 5d_{1/15} = -21, \\
5d_{1/5} = 5d_{-5/3} = -9, \quad 5d_{-1/5} = 5d_{5/3} = 3, \\
15d_{3/5} = -7, \quad 15d_{-3/5} = -8, \quad 15d_{15} = 161, \quad 15d_{-15} = -176.
\end{gathered}
$$

If $5 \mid k \mid 30$, it's not hard to show that

$$
E_{k,m}(\mathbb{Z}) = \begin{cases}
\{(5,0),(16,\pm 19)\}, & \text{if } k=5, m=11; \\
\{(-5,0),(-3,\pm 7)\}, & \text{if } k=-5, m=2; \\
\{(-10,0),(-6,\pm 28)\}, & \text{if } k=-10, m=1; \\
\{(-15,0),(7,\pm 13)\}, & \text{if } k=-15, m=22; \\
\{(-15,0),(8,\pm 13)\}, & \text{if } k=-15, m=23; \\
\{(-15,0),(176,\pm 169)\}, & \text{if } k=-15, m=191; \\
\{(-30,0),(14,\pm 52)\}, & \text{if } k=-30, m=11; \\
\{(k,0)\}, & \text{otherwise.}
\end{cases}
$$

Acknowledgements. This work is partially supported by the Fundamental Research Funds for the Central Universities (No. JZ2023HGTB0217).

References

[Hal71] Marshall Hall, Jr. The Diophantine equation $x^3 - y^2 = k$. In *Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969)*, pages 173–198. Academic Press, London-New York, 1971.

[KS81a] Chao Ko and Chi Sun. On the Diophantine equations $x^3 \pm 1 = 3Dy^2$. *Sichuan Daxue Xuebao*, (2):1–6, 1981.

[KS81b] Chao Ko and Chi Sun. On the Diophantine equations $x^3 \pm 1 = Dy^2$. *Kexue Tongbao*, (6):381, 1981.

[KS81c] Chao Ko and Chi Sun. On the Diophantine equations $x^3 \pm 8 = Dy^2$ and $x^3 \pm 8 = 3Dy^2$. *Sichuan Daxue Xuebao*, (4):1–5, 1981.

[Liv95] Eric Liverance. A formula for the root number of a family of elliptic curves. *J. Number Theory*, 51(2):288–305, 1995.

[Lju42] Wilhelm Ljunggren. Sätze über unbestimmte Gleichungen. *Skr. Norske Vid.-Akad. Oslo I*, 1942(9):53, 1942.

School of Mathematics, Hefei University of Technology, Hefei, Anhui 230000, China
Email address: zhangshenxing@hfut.edu.cn