J. Ramanujan Math. Soc. **31**, No.1 (2016) 63–77

Pell surfaces and elliptic curves

K. J. Manasa and B. R. Shankar

Department of Mathematical and Computational Sciences, National Institute of Technology Karnataka, Surathkal
e-mail: manasakj123@gmail.com, shankarbr@gmail.com

Communicated by: R. Sujatha

Received: May 10, 2015

Abstract. Let E_m be the elliptic curve $y^2 = x^3 - m$, where m is a squarefree positive integer and $-m \equiv 2, 3 \pmod 4$. Let $Cl(K)[3]$ denote the 3-torsion subgroup of the ideal class group of the quadratic field $K = \mathbb{Q}(\sqrt{-m})$. Let $S_3 : y^2 + mz^2 = x^3$ be the Pell surface. We show that the collection of primitive integral points on S_3 coming from the elliptic curve E_m do not form a group with respect to the binary operation given by Hambleton and Lemmermeyer. We also show that there is a group homomorphism κ from rational points of E_m to $Cl(K)[3]$ using 3-descent on E_m, whose kernel contains $3E_m(\mathbb{Q})$. We also explain how our homomorphism κ, the homomorphism ψ of Hambleton and Lemmermeyer and the homomorphism ϕ of Soleng are related.

2000 *Mathematics Subject Classification:* Primary 11G05; Secondary 11R11, 11R29.

1. Introduction

Let m be a squarefree positive integer and $-m \equiv 2, 3 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{-m})$ be an imaginary quadratic field. Any element of this field is of the form $a + b\omega$, where $\omega = \sqrt{-m}$, $a, b \in \mathbb{Q}$ and its norm is $N(a + b\omega) = a^2 + mb^2$. Let $\mathfrak{O}_K$ denote the ring of algebraic integers of K. An element $\alpha \in \mathfrak{O}_K$ is primitive if $p \nmid \alpha$ for every rational prime $p \in \mathbb{N}$.

Let $E_m : y^2 = x^3 - m$ be the associated elliptic curve. It is well known that the set of rational points on it forms a finitely generated abelian group denoted as $E_m(\mathbb{Q})$. Any rational point on E_m is of the form $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ where $r, s, t \in \mathbb{Z}$ with $\gcd(r, t) = \gcd(s, t) = 1$. For standard definitions and results on elliptic curves, we refer to [9] and [10].

Let $S_n : y^2 + mz^2 = x^n$ with $n \geq 2$, a fixed integer, be a Pell surface. In an interesting paper [7] by S. Hambleton and F. Lemmermeyer, it is shown that with respect to a binary operation defined on the primitive integral points of S_n, denoted by $S_n(\mathbb{Z})$, it forms an abelian group. They have also shown that there is a surjective homomorphism $\psi : S_n(\mathbb{Z}) \longrightarrow Cl^+(F)[n]$, the n-torsion subgroup of the narrow class group of the quadratic field $F = \mathbb{Q}(\sqrt{\Delta})$, where Δ is a fundamental discriminant, more generally $S_n : y^2 + \sigma yz + \frac{\sigma - \Delta}{4} z^2 = x^n$ and σ is the remainder of the discriminant Δ modulo 4. In the case we study $\sigma = 0$ and $\Delta < 0$.

In §2 we quickly recall notations and some results in [7] which will be needed later to prove our results in §3.

In §3 we relate the group $E_m(\mathbb{Q})$, the quadratic field K and the primitive integral points on the Pell surface $S_3 : y^2 + mz^2 = x^3$. We define a map $f : E_m(\mathbb{Q}) \longrightarrow S_3(\mathbb{Z})$ by which we obtain primitive integral points on the Pell surface S_3. Let $S_3^E(\mathbb{Z})$ denote the collection of all such points. Clearly $S_3^E(\mathbb{Z}) \subseteq S_3(\mathbb{Z})$. It is natural to ask the following questions: (1) Is the inclusion proper? (2) Does $S_3^E(\mathbb{Z})$ inherit the group structure from $S_3(\mathbb{Z})$? In the same section, we show that the answer is yes to the first question and no to the second question.

In §4 we define a binary operation on $S_3^E(\mathbb{Z})$ under which it becomes a group.

On the other hand some questions about the class number of a quadratic field are related to solutions of Diophantine equations. For example it is well known that the study of integer solutions to the Diophantine equation

$$X^2 - \Delta Y^2 = 4Z^n, \quad \gcd(X, Z) = 1, \quad \Delta = \text{a fundamental discriminant}, \tag{1}$$

gives rise to a quadratic number field with class number divisible by n. For each integral point (X, Y, Z), there is a corresponding ideal $\mathfrak{a} = \left\langle \frac{X + Y\sqrt{\Delta}}{2}, Z \right\rangle$ in the ring of integers of $\mathbb{Q}(\sqrt{\Delta})$ such that $\mathfrak{a}^n = \left\langle \frac{X + Y\sqrt{\Delta}}{2} \right\rangle$. Hence it generates an ideal class of order dividing n. Likewise several authors have related rational points on elliptic curves and ideal classes of quadratic fields, see [2], [3] and [11].

In §3 we define a map $g : E_m(\mathbb{Q}) \longrightarrow \mathfrak{O}_K$ such that for any $\beta \in g(E_m(\mathbb{Q}))$, the ideal $\langle \beta \rangle$ is always the cube of an ideal in $\mathfrak{O}_K$. Using this, later in §5, we define a map $\kappa : E_m(\mathbb{Q}) \longrightarrow Cl(K)[3]$, the 3-part of the class group of K. In the same section we show that κ is a group homomorphism whose kernel contains $3E_m(\mathbb{Q})$ using 3-descent on E_m.

Soleng [11] has considered a group homomorphism ϕ mapping a more generally defined elliptic curve to the ideal class group $Cl(K)$. In the last section §6 we show that the homomorphisms κ, ψ and ϕ are related for the elliptic curve E_m.

2. Preliminaries on Pell surfaces

A binary quadratic form is a homogeneous polynomial of degree 2 in two variables given by $Q_0(y,z) = ay^2 + byz + cz^2$. If the coefficients a, b, c are integers, then it is called an integral binary quadratic form. The quadratic form $Q_0(y,z)$ is said to be primitive if $\gcd(a,b,c) = 1$. Binary quadratic forms come naturally from quadratic fields. Let $F = \mathbb{Q}(\sqrt{\Delta})$ be any quadratic field of discriminant Δ. Then

$$Q_0(y,z) = \begin{cases} y^2 - \frac{\Delta}{4}z^2, & \text{if } \Delta \equiv 0 \pmod 4 \\ y^2 + yz + \frac{1-\Delta}{4}z^2, & \text{if } \Delta \equiv 1 \pmod 4 \end{cases}$$

is the canonical principal binary quadratic form associated with F.

Thus, the binary quadratic form associated with the quadratic field

$$\begin{aligned} K = \mathbb{Q}(\sqrt{-m}) \text{ with } m > 0, \quad -m \equiv 2, 3 \pmod 4), \\ \text{discriminant} : -4m, \ m \text{ squarefree} \end{aligned} \qquad (\bigstar)$$

is $Q_0(y,z) = y^2 + mz^2$.

The Pell surface associated with the quadratic field K will be denoted as $S_n : Q_0(y,z) = x^n$, and in the present article we are interested in the Pell surface $S_3 : y^2 + mz^2 = x^3$. From here on we will always use K to mean a quadratic field satisfying the conditions of ($\bigstar$). An integral point (x, y, z) satisfying $S_n : Q_0(y,z) = x^n$ is said to be primitive if $x, y, z \in \mathbb{Z}$ with $\gcd(y,z) = 1$. The set $S_n(\mathbb{Z})$ denotes the primitive integral points of the surface S_n. A correspondence between integral points in $S_n(\mathbb{Z})$ and integral solutions to the Diophantine equation (1), which in fact is a bijection, is given in [7]:

$$(X, Y, Z) = \begin{cases} (2y, z, x), & \text{if } \Delta = 4m \\ (2y + z, z, x), & \text{if } \Delta = 4m + 1 \end{cases}$$

Let $\mathfrak{O}_K^*$ denote the nonzero elements of the ring of integers $\mathfrak{O}_K$ of K. In the case of this article, an algebraic integer of K may be written as $y + z\sqrt{-m}$ and there is a natural map $\pi_0 : S_n(\mathbb{Z}) \to \mathfrak{O}_K^*$ defined by $\pi_0(x,y,z) = y + z\sqrt{-m}$. Let $\mathbb{N}^n = \{\alpha^n \text{ such that } \alpha \in \mathbb{N}\}$. Then the set $\mathfrak{O}_K^*/\mathbb{N}^n$ forms a group with respect to coset multiplication. The norm map induces a group homomorphism $N : \mathfrak{O}_K^*/\mathbb{N}^n \longrightarrow \mathbb{Z}^*/\mathbb{Z}^{*n}$ defined as $N(\alpha\mathbb{N}^n) = N(\alpha)\mathbb{Z}^{*n}$, where $\mathbb{Z}^{*n}$ denotes the set of nonzero integer n-th powers.

As we make use of some results from [7] in the course of proving our results in §3, they are stated below for the sake of clarity and completeness.

Lemma 2.1. *Let $\alpha \in \mathfrak{O}_K^*$. If $N(\alpha) = a^n$ for some $n \geq 2$, then α is primitive if and only if $\langle\alpha\rangle + \langle\alpha'\rangle = \langle 1 \rangle$.*

Lemma 2.2. *Let α be a primitive element. If $\alpha\mathbb{N}^n \in Ker\ N$, then $\langle\alpha\rangle = \mathfrak{a}^n$ is an n-th ideal power.*

Theorem 2.3. *The cosets of primitive elements in the kernel of the norm map $N : \mathfrak{O}_K^*/\mathbb{N}^n \longrightarrow \mathbb{Z}^*/\mathbb{Z}^{*n}$ form a subgroup Π_n of $\mathfrak{O}_K^*/\mathbb{N}^n$. The map $\pi : S_n(\mathbb{Z}) \longrightarrow \Pi_n$ defined by $\pi(x, y, z) = (y + z\sqrt{-m})\mathbb{N}^n$ is bijective; thus $S_n(\mathbb{Z})$ becomes an abelian group by transport of structure.*

Definition 2.4. *For (x_1, y_1, z_1), $(x_2, y_2, z_2) \in S_n(\mathbb{Z})$ the group law on $S_n(\mathbb{Z})$ defined as $(x_1, y_1, z_1) \oplus (x_2, y_2, z_2) = (x_3, y_3, z_3)$ where*

$$(x_3, y_3, z_3) = \left(\frac{x_1x_2}{e^2}, \frac{y_1y_2 + \frac{\Delta-\sigma}{4}z_1z_2}{e^n}, \frac{y_1z_2 + y_2z_1 + \sigma z_1z_2}{e^n}\right)$$

and

$$gcd\left(y_1y_2 + \frac{\Delta - \sigma}{4}z_1z_2,\ y_1z_2 + y_2z_1 + \sigma z_1z_2\right) = e^n.$$

In the case $\Delta = -4m$, the group law is

$$(x_3, y_3, z_3) = \left(\frac{x_1x_2}{e^2}, \frac{y_1y_2 - mz_1z_2}{e^n}, \frac{y_1z_2 + y_2z_1}{e^n}\right)$$

where

$$\gcd(y_1y_2 - mz_1z_2,\ y_1z_2 + y_2z_1) = e^n.$$

Proposition 2.5. *The map $\psi : S_n(\mathbb{Z}) \rightarrow Cl^+(F)[n]$ given by $\psi(x, y, z) = [\mathfrak{a}]$ where $\langle y + z\omega\rangle = \mathfrak{a}^n$ is a surjective group homomorphism where $\omega = \frac{\sigma+\sqrt{\Delta}}{2}$ and $\sigma \in \{0, 1\}$.*

For proofs see [7].

3. Relation between quadratic fields, elliptic curves and Pell surfaces

As before E_m denotes the elliptic curve

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

On the elliptic curve E_m, points $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ and $\left(\frac{r}{(-t)^2}, \frac{-s}{(-t)^3}\right)$ are the same and similarly the points $\left(\frac{r}{t^2}, \frac{-s}{t^3}\right)$ and $\left(\frac{r}{(-t)^2}, \frac{s}{(-t)^3}\right)$ are also identical. So, by taking $s > 0$, we see that all rational points on E_m are considered. Hence

$$E_m(\mathbb{Q}) = \left\{\left(\frac{r}{t^2}, \frac{s}{t^3}\right) \text{ such that } r, t, s \in \mathbb{Z},\ s > 0,\ \gcd(r, t) = \gcd(s, t) = 1\right\} \cup \{\mathcal{O}\}$$

where $\mathcal{O}$ is the point at infinity.

On substituting $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ in E_m we get,

$$s^2 + mt^6 = r^3. \tag{3}$$

On the Pell surface $S_3 : y^2 + mz^2 = x^3$ when $z = 1$, we obtain integer points of the elliptic curve E_m. The set of all primitive integral points on S_3 will be denoted by $S_3(\mathbb{Z})$. Comparing with equation (3), we see that points on the elliptic curve E_m correspond to integral points on the Pell surface S_3 in a natural way, by the map

$$f : E_m(\mathbb{Q}) \longrightarrow S_3(\mathbb{Z})$$

$$f(P) = \begin{cases} (1, 1, 0), & \text{if } P = \mathcal{O} \\ (r, s, t^3), & \text{if } P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \end{cases} \tag{$\spadesuit$}$$

It is clear that this map is well-defined. As $\gcd(s, t) = 1$, integral points (r, s, t^3) on S_3 coming from the elliptic curve are all primitive integral points. Denote the image, $f(E_m(\mathbb{Q}))$, as $S_3^E(\mathbb{Z})$. Clearly $S_3^E(\mathbb{Z}) \subseteq S_3(\mathbb{Z})$. Also, any point $(r, s, t^3) \in S_3^E(\mathbb{Z})$ gives an integral solution $(2s, t^3, r)$ of (1) with $n = 3$.

Again from (3) we note that $r^3 =$ Norm of $(s + t^3\sqrt{-m})$ in $\mathfrak{O}_K$. So, it is natural to consider the map $g : E_m(\mathbb{Q}) \longrightarrow \mathfrak{O}_K$ defined by

$$g(P) = \begin{cases} 1, & \text{if } P = \mathcal{O} \\ s + t^3\sqrt{-m}, & \text{if } P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \end{cases}$$

As discussed earlier, by considering $s > 0$, the map g is also well defined. Denote $g(E_m(\mathbb{Q}))$ as H^E.

Now we prove that elements in H^E are all primitive in $\mathfrak{O}_K$. For this it is sufficient to show that for $\alpha \in H^E$, ideals $\langle\alpha\rangle$ and $\langle\alpha'\rangle$ are coprime in $\mathfrak{O}_K$ where α' is the conjugate of α. Then, by Lemma 2.1, elements in H^E are primitive. We prove this below:

Lemma 3.1. *Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ be a rational point on E_m for a squarefree positive integer m, and $-m \not\equiv 1 (mod\ 4)$. Assume, as before, $\gcd(r, t) = \gcd(s, t) = 1$. Then the ideals $\langle\alpha\rangle$ and $\langle\alpha'\rangle$ are co-prime in $\mathfrak{O}_K^*$, where $\alpha = g(P) = s + t^3\sqrt{-m}$ and $\alpha' = g(-P) = s - t^3\sqrt{-m}$.*

Proof. Let $\alpha = s + t^3\sqrt{-m}$ and $\alpha' = s - t^3\sqrt{-m}$. Let $\mathfrak{p}$ be a prime ideal such that

$$\mathfrak{p} \mid \langle s + t^3\sqrt{-m}\rangle, \ \ \mathfrak{p} \mid \langle s - t^3\sqrt{-m}\rangle.$$

Hence

$$s + t^3\sqrt{-m} \in \mathfrak{p}, \ \ s - t^3\sqrt{-m} \in \mathfrak{p}.$$

Thus $\mathfrak{p}$ divides the sum $2s$. This implies $\mathfrak{p}|2$ or $\mathfrak{p}|s$. Also,

$$2t^3\sqrt{-m} = (s + t^3\sqrt{-m}) - (s - t^3\sqrt{-m}) \in \mathfrak{p}$$

and so

$$2t^3(-m) = \sqrt{-m}(2t^3\sqrt{-m}) \in \mathfrak{p}.$$

If $\mathfrak{p}|s$, as $\gcd(s, t) = 1$, $\mathfrak{p}$ must divide $2m$. Suppose $\mathfrak{p}$ divides m and s; then it also divides r, as $s^2 + t^6m = r^3$. Also norm of $\mathfrak{p}$ divides both r and s. Hence the square of the norm divides $r^3 - s^2 = mt^6$. As $\gcd(s, t) = 1$, the square of the norm divides m, a contradiction.

So, the only possibility for the prime ideal $\mathfrak{p}$ is either it is above 2 or $\mathfrak{p} = \langle 1 \rangle$. Suppose $\mathfrak{p}$ is an ideal above 2, then $\mathfrak{p}|N(\alpha) = r^3$. Thus $2|r$. We have $s^2 \equiv 0, 1 \pmod 4$, $-m \equiv 2, 3 \pmod 4$. This implies $r^3 = s^2 - (-m)t^6 \equiv 1, 2, 3 \pmod 4$. But $r^3 \equiv 1, 3 \pmod 4 \Rightarrow r \equiv 1 \pmod 2$. Thus r is odd, a contradiction. Hence $\langle \alpha \rangle$ and $\langle \alpha' \rangle$ are coprime. □

Now we show that $\alpha \in H^E$ has an interesting property by using Lemma 2.2: $\langle \alpha \rangle$ is a cube of an ideal in $\mathfrak{O}_K$.

Theorem 3.2. *Let m be a squarefree positive integer with $-m \not\equiv 1 (mod\ 4)$. Let $K = \mathbb{Q}(\sqrt{-m})$ and $E_m : y^2 = x^3 - m$ be the corresponding elliptic curve. For any $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \in E_m(\mathbb{Q}) \setminus \mathcal{O}$, with $gcd(r, t) = gcd(s, t) = 1$, the ideal $\langle s + t^3\sqrt{-m} \rangle$ is the cube of an ideal, i.e., $\langle s + t^3\sqrt{-m} \rangle = \mathfrak{a}^3$.*

Proof. Let $\alpha = s + t^3\sqrt{-m} \in H^E$. Then $N(\alpha) = r^3$ by equation (3). As before the norm map induces a group homomorphism $N : \mathfrak{O}_K^*/\mathbb{N}^3 \longrightarrow \mathbb{Z}^*/\mathbb{Z}^{*3}$ defined as $N(\alpha\mathbb{N}^3) = N(\alpha)\mathbb{Z}^{*3}$. The kernel of this map is

$$\begin{aligned} ker\ N &= \{\alpha\mathbb{N}^3 \text{ such that } N(\alpha)\mathbb{Z}^{*3} = \mathbb{Z}^{*3}\}, \\ &= \{\alpha\mathbb{N}^3 \text{ such that } N(\alpha) \in \mathbb{Z}^{*3}\}. \end{aligned}$$

Let $\Pi_3^E = \{\alpha\mathbb{N}^3 \text{ such that } \alpha \in H^E\}$. Clearly $\Pi_3^E \subseteq \ker N$. Also by Lemmas 3.1 and 2.1, α is primitive, and so by Lemma 2.2, the ideal $\langle \alpha \rangle = \mathfrak{a}^3$ is the cube of an ideal. □

In [7] it is shown that $S_3(\mathbb{Z})$ is an abelian group with respect to the binary operation given in Definition 2.4. Observe that the neutral element of $S_3(\mathbb{Z})$ is $(1, 1, 0)$. Similarly the inverse of $(x, y, z) \in S_3(\mathbb{Z})$ is given as

$$-(x, y, z) = \begin{cases} (x, y, -z), & \text{if } x > 0 \\ (x, -y, z), & \text{if } x < 0. \end{cases}$$

In fact, the identity $(1, 1, 0) \in S_3^E(\mathbb{Z})$ as this corresponds to the point at infinity on the elliptic curve E_m. Also, for $(r, s, t^3) \in S_3^E(\mathbb{Z})$, the inverse point is $(r, s, -t^3)$, since we must have $r > 0$, because $s^2 = r^3 - mt^6 > 0$ and $m > 0$. This coincides with the inverse $\left(\frac{r}{t^2}, \frac{s}{-t^3}\right)$ of the point $\left(\frac{r}{t^2}, \frac{s}{t^3}\right)$ of $E_m(\mathbb{Q})$. Thus, the set $S_3^E(\mathbb{Z})$ has the identity, and every element in it has an inverse with respect to the binary operation $\oplus$ of $S_3(\mathbb{Z})$. However, with this binary operation the set $S_3^E(\mathbb{Z})$ is **not** a group. We illustrate it with the following example:

Example 3.3. *For $m = 26$, $E_{26} : y^2 = x^3 - 26$. The two points $P = (3, 1)$ and $Q = (35, 207)$ on E_{26} correspond to $(3, 1, 1)$ and $(35, 207, 1)$ respectively in $S_3^E(\mathbb{Z})$. The discriminant of $K = \mathbb{Q}(\sqrt{-26})$ is equal to -104. Thus the group law on the Pell surface S_3 corresponding to this discriminant is*

$$(x_1, y_1, z_1) \oplus (x_2, y_2, z_2) = \left(\frac{x_1x_2}{e^2}, \frac{y_1y_2 - 26z_1z_2}{e^3}, \frac{y_1z_2 + y_2z_1}{e^3}\right)$$

where

$$gcd(y_1y_2 - 26z_1z_2,\ y_1z_2 + y_2z_1) = e^3.$$

Therefore

$$\begin{aligned}&(3, 1, 1) \oplus (35, 207, 1)\\ &= \left(\frac{3 \times 35}{e^2}, \frac{1 \times 207 - 26 \times 1 \times 1}{e^3}, \frac{1 \times 1 + 207 \times 1}{e^3}\right)\\ &= (105, 181, 208) \text{ since } gcd(181, 208) = 1.\end{aligned}$$

*This shows that $S_3^E(\mathbb{Z})$ is **not** closed under the binary operation $\oplus$ of $S_3(\mathbb{Z})$. Clearly $(105, 181, 208) \in S_3(\mathbb{Z})$ but $(105, 181, 208) \notin S_3^E(\mathbb{Z})$. Hence $S_3^E(\mathbb{Z}) \subsetneq S_3(\mathbb{Z})$.*

Let F be any quadratic field. An element $\beta \in F$ is said to be totally positive if $N(\beta) > 0$. Let P_F^+ be the group of principal fractional ideals $\langle\beta\rangle = \beta\mathfrak{O}_F$ where $N(\beta) > 0$. The quotient group I_F/P_F^+ is called the narrow class group $Cl^+(F)$ of F. For imaginary quadratic fields, the norm of any element is positive, thus the class group and the narrow class group are identical. The collection of ideal classes of order dividing n in F forms a subgroup of $Cl(F)$ and is called the n-part of the ideal class group, denoted as $Cl(F)[n]$.

By applying Proposition 2.5 to $S_3(\mathbb{Z})$ and the field K we get a surjective homomorphism ψ from $S_3(\mathbb{Z})$ to $Cl(K)[3]$.

Consider the diagram

$$\begin{tikzcd} E_m(\mathbb{Q}) \arrow[d, "f"'] & \\ S_3(\mathbb{Z}) \arrow[r, "\psi"'] & Cl(K)[3] \end{tikzcd}$$

Here f is as defined in (♠) and ψ is the surjective homomorphism defined in §2 (Proposition 2.5). We note that f is injective but not a homomorphism since $f(E_m(\mathbb{Q})) = S_3^E(\mathbb{Z})$ is not a subgroup of $S_3(\mathbb{Z})$. Also, the image of f is not equal to the kernel of ψ. The following example illustrates it.

Example 3.4. *Let* $K = \mathbb{Q}(\sqrt{-53})$ *and* $E_{53} : y^2 = x^3 - 53$, *where* $-53 \not\equiv 1 (mod\ 4)$. *Let* $P = (29, 156) \in E_{53}(\mathbb{Q})$. *Then* $f(P) = (29, 156, 1) \in f(E_{53}(\mathbb{Q}))$. *However,* $\psi(f(P)) = \langle 156 + \sqrt{-53} \rangle = \mathfrak{b}^3$, *where* $\mathfrak{b} = \langle 29, 11+\sqrt{-53} \rangle$. *We show that the ideal* $\langle 29, 11+\sqrt{-53} \rangle$ *in* $\mathfrak{O}_K$ *is not a principal ideal. Say* $\langle 29, 11 + \sqrt{-53} \rangle = \langle \beta \rangle$. *Then, since* $29 \in \langle 29, 11 + \sqrt{-53} \rangle$ *we have* $29 \in \langle \beta \rangle$, *so* $\beta | 29$ *in* $\mathfrak{O}_K$. *Writing* $29 = \beta\gamma$ *in* $\mathfrak{O}_K$ *and taking norms, we have* $841 = 29^2 = N(\beta)N(\gamma)$ *in* $\mathbb{Z}$. *So,* $N(\beta)|841$ *in* $\mathbb{Z}$. *Similarly, since* $11 + \sqrt{-53} \in \langle \beta \rangle$ *we get* $N(\beta)|174$ *in* $\mathbb{Z}$. *Thus* $N(\beta)$ *is a common divisor of* 841 *and* $174 = 29 \cdot 6$ *in* $\mathbb{Z}$. *So,* $N(\beta)$ *is* 1 *or* 29. *Since* $N(\beta) = a^2 + 53b^2$ *where* a, b *are in* $\mathbb{Z}$, $N(\beta) \neq 29$. *Therefore* $N(\beta) = 1$, *so* β *is a unit and* $\langle 1 \rangle = \langle \beta \rangle$. *Thus* $1 \in \langle \beta \rangle$. *Hence there exist* α *and* δ *in* $\mathfrak{O}_K$ *such that* $29\alpha + (11 + \sqrt{-53})\delta = 1$. *Multiplying both sides by* $11 - \sqrt{-53}$, *we have* $29\{(11 - \sqrt{-53})\alpha + 6\delta\} = 11 - \sqrt{-53}$, *so that* 29 *divides* $11 - \sqrt{-53}$ *in* $\mathfrak{O}_K$. *Thus* $N(29) = 841$ *divides* $N(11 - \sqrt{-53}) = 174$ *which is a contradiction. So,* $\langle 29, 11 + \sqrt{-53} \rangle$ *is not a principal ideal in* $\mathfrak{O}_K$. *Hence* $f(P)$ *is not in the kernel of* ψ.

4. A Group law on $S_3^E(\mathbb{Z})$ from $E_m(\mathbb{Q})$

By using the binary operation on $E_m(\mathbb{Q})$ we define a binary operation on $S_3^E(\mathbb{Z})$ with respect to which $S_3^E(\mathbb{Z})$ becomes an abelian group. We recall that $E_m(\mathbb{Q})$ is an abelian group with respect to the group law given by the following formulae:-

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be rational points on E_m and define λ as

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2}{2y_1}, & \text{if } P_1 = P_2 \end{cases}$$

Then $P_3 = P_1 + P_2 = (x_3, y_3)$ with $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$. The map $f : E_m(\mathbb{Q}) \longrightarrow S_3^E(\mathbb{Z})$ is as defined in (♠) and is given by

$$f(P) = \begin{cases} (1, 1, 0), & \text{if } P = \mathcal{O} \\ (r, s, t^3), & \text{if } P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \end{cases}$$

This is indeed a bijection. Thus, by transporting the group structure of $E_m(\mathbb{Q})$ to $S_3^E(\mathbb{Z})$, the set $S_3^E(\mathbb{Z})$ becomes an abelian group. We now define the binary operation on $S_3^E(\mathbb{Z})$:

Let $u_i = (r_i, s_i, t_i^3) (i = 1, 2)$ be elements in $S_3^E(\mathbb{Z})$. These elements correspond to $P_i = \left(\frac{r_i}{t_i^2}, \frac{s_i}{t_i^3}\right)$ on the elliptic curve E_m. We show that the sum $P_3 = P_1 + P_2$ corresponds to an element $u_3 \in S_3^E(\mathbb{Z})$, with $u_3 = u_1 * u_2$ where $*$ is defined using the group law on elliptic curves as follows:

Case I. $\frac{r_1}{t_2^2} \neq \frac{r_2}{t_2^2}$, *and* $\lambda = \left(\frac{s_2}{t_2^3} - \frac{s_1}{t_1^3}\right)/\left(\frac{r_2}{t_2^2} - \frac{r_1}{t_1^2}\right)$. *Hence*

$$x_3 = \lambda^2 - \frac{r_1}{t_1^2} - \frac{r_2}{t_2^2} = \left(\frac{s_2 t_1^3 - s_1 t_2^3}{t_1 t_2 (r_2 t_1^2 - r_1 t_2^2)}\right)^2 - \frac{r_1}{t_1^2} - \frac{r_2}{t_2^2},$$

$$y_3 = \lambda(x_1 - x_3) - y_1 = \frac{s_2 t_1^3 - s_1 t_2^3}{t_1 t_2 (r_2 t_1^2 - r_1 t_2^2)} \left(\frac{r_1}{t_1^2} - x_3\right) - \frac{s_1}{t_1^3}$$

This enables one to find $u_3 \in S_3^E(\mathbb{Z})$.

Define $S_- = s_2 t_1^3 - s_1 t_2^3$, $R_- = r_2 t_1^2 - r_1 t_2^2$, $R_+ = r_2 t_1^2 + r_1 t_2^2$ *and* $T = t_1 t_2$. *On simplification and by using above notations we get*

$$x_3 = \frac{S_-^2 - R_+ R_-^2}{R_-^2 T^2}$$

$$y_3 = \frac{R_-^2 R_+ S_- + T^2 R_-^2 (s_2 r_1 t_1 - s_1 r_2 t_2) - S_-^3}{R_-^3 T^3}$$

Hence (r_3, s_3, t_3^3) *is given by*

$$r_3 = S_-^2 - R_+ R_-^2$$

$$s_3 = R_-^2 R_+ S_- + T^2 R_-^2 (s_2 r_1 t_1 - s_1 r_2 t_2) - S_-^3$$

$$t_3^3 = R_-^3 T^3,$$

Case II. $\frac{r_1}{t_2^2} = \frac{r_2}{t_2^2} = \frac{r}{t^2}$, *and* $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right)$, $\lambda = \frac{3r^2}{2st}$.

Hence

$$x_3 = \frac{9r^4}{4s^2t^2} - \frac{2r}{t^2} = \frac{9r^4 - 8rs^2}{4s^2t^2}$$

$$y_3 = \frac{3r^2}{2st}\left(\frac{r}{t^2} - \frac{9r^4 - 8rs^2}{4s^2t^2}\right) - \frac{s}{t^3} = \frac{36r^3s^2 - 27r^6 - 8s^4}{8s^3t^3}$$

Thus for $u_1 = u_2 = (r, s, t^3)$ *we have* (r_3, s_3, t_3^3) *where*

$$r_3 = 9r^4 - 8rs^2$$

$$s_3 = 36r^3s^2 - 27r^6 - 8s^4$$

$$t_3^3 = (2st)^3.$$

In both the cases, certainly (r_3, s_3, t_3^3) satisfies the equation of the Pell surface S_3, but it need not be primitive.

Now, if (x, y, z) is any primitive point on the Pell surface S_3 then $(x', y', z') = (d^2x, d^3y, d^3z)$ will also lie on S_3 for any integer d. Thus, if (x, y, z) is not a primitive point, then $\gcd(x, z) = d^2$ and $\gcd(y, z) = d^3$ for some integer $d \geq 1$. Let $(r_4, s_4, t_4^3) = (r_3/d^2, s_3/d^3, t_3^3/d^3)$. Define $u_3 = (r_4, s_4, t_4^3)$.

With this binary operation, $S_3^E(\mathbb{Z})$ is an abelian group: the identity element is $(1, 1, 0)$, the inverse of (r, s, t^3) is $(r, s, -t^3)$. We illustrate it with an example:

Example 4.1. *Let $E_{26} : y^2 = x^3 - 26$, $u_1 = (3, 1, 1)$ and $u_2 = (35, 207, 1)$ be in $S_3^E(\mathbb{Z})$, which correspond to the elements $P = (3, 1)$ and $Q = (35, 207)$ respectively in $E_{26}(\mathbb{Q})$. Thus, we have $r_1 = 3$, $s_1 = 1$, $t_1 = 1$, $r_2 = 35$, $s_2 = 207$, $t_2 = 1$, and $S_- = 206, T = 1$, $R_- = 32$, $R_+ = 38$. Hence $r_3 = 3524 = 881 \cdot 2^2$, $s_3 = -125880 = -2^3 \cdot 3 \cdot 5 \cdot 1049$, $t_3^3 = 32768 = 2^{15}$. As (r_3, s_3, t_3^3) is not a primitive point, we consider $u_3 = (r_4, s_4, t_4^3) = (r_3/d^2, s_3/d^3, t_3^3/d^3) = (881, -15735, 4096)$. Clearly $u_3 \in S_3^E(\mathbb{Z})$. Also u_3 corresponds to the rational point $P_3 = \left(\frac{881}{256}, \frac{-15735}{4096}\right) \in E_{26}$.*

Similarly for $u_1 = u_2 = (3, 1, 1)$ we get $r_3 = 705 = 3 \cdot 4 \cdot 47$, $s_3 = -18719$, $t_3^3 = 2^3$. As (r_3, s_3, t_3^3) is a primitive point, $u_3 = (r_3, s_3, t_3^3) = (705, -18719, 8)$. This corresponds to $\left(\frac{705}{4}, \frac{-18719}{8}\right) = 2P \in E_{26}(\mathbb{Q})$, where $P = (3, 1)$.

5. A homomorphism from $E_m(\mathbb{Q})$ to the 3-part of the class group of the quadratic field $\mathbb{Q}(\sqrt{-m})$

In this section we give a group homomorphism from $E_m(\mathbb{Q})$ to $Cl(K)[3]$ using 3-descent on $E_m(\mathbb{Q})$. For the curve E_m, a 3-torsion point T is $(0, -\sqrt{-m})$. There is a natural norm map $N : K^* \longrightarrow \mathbb{Q}^*$ given by $N(a + b\sqrt{-m}) = a^2 + b^2m$ for $a, b \in \mathbb{Q}$. This induces a homomorphism: $K^*/K^{*3} \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*3}$, which will also be denoted by N. Let $G_3 = \{\gamma K^{*3}$ such that $N(\gamma) = t^3, t \in \mathbb{Q}^*\}$. Then $\ker N = G_3$.

Lemma 5.1. *Let m be a squarefree positive integer with $-m \not\equiv 1 \pmod 4$. Let $K = \mathbb{Q}(\sqrt{-m})$ and let $E_m : y^2 = x^3 - m$ be the corresponding elliptic curve. Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \in E_m(\mathbb{Q})$, with $\gcd(r, t) = \gcd(s, t) = 1$, and $G_3 = \{\gamma K^{*3}$ such that $N(\gamma) = t^3,\ t \in \mathbb{Q}^*\}$. The map*

$$\alpha : E_m(\mathbb{Q}) \longrightarrow K^*/K^{*3}, \quad \alpha : \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \longmapsto (s + t^3\sqrt{-m})K^{*3}$$

is a group homomorphism.

Proof. The 3-descent map, given in [5] (pp. 563), applied to the elliptic curve E_m is:

$$\delta : E_m(\mathbb{Q}) \longrightarrow K^*/K^{*3}$$

$$\delta(P) = \begin{cases} (y + \sqrt{-m})K^{*3}, & \text{if } P = (x, y) \\ K^{*3}, & \text{if } P = \mathcal{O}. \end{cases}$$

Observe that $(s + t^3\sqrt{-m})K^{*3} = \left(\frac{s}{t^3} + \sqrt{-m}\right)K^{*3} = (y + \sqrt{-m})K^{*3}$. Since the 3-descent map δ is a group homomorphism, it follows that α is a group homomorphism. □

Lemma 5.2. *Let m be a squarefree positive integer with $-m \not\equiv 1 (mod\ 4)$, let $K = \mathbb{Q}(\sqrt{-m})$, $E_m : y^2 = x^3 - m$, and $\hat{E}_m : \hat{y}^2 = \hat{x}^3 + 27m$. Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \in E_m(\mathbb{Q})$ with $gcd(r, t) = gcd(s, t) = 1$. There is an exact sequence of group homomorphisms*

$$1 \longrightarrow \hat{\phi}(\hat{E}_m(\mathbb{Q})) \longrightarrow E_m(\mathbb{Q}) \xrightarrow{\alpha} \frac{K^*}{K^{*3}} \xrightarrow{N} \frac{\mathbb{Q}^*}{\mathbb{Q}^{*3}}$$

where $\alpha : P \longmapsto (s+t^3\sqrt{-m})K^{*3}$ and $\hat{\phi} : (\hat{x}, \hat{y}) \longmapsto \left(\frac{\hat{x}^3+108m}{9\hat{x}^2}, \frac{\hat{y}(\hat{x}^3-216m)}{27\hat{x}^3}\right)$. $3E_m(\mathbb{Q})$ is a proper subgroup of $\hat{\phi}(\hat{E}_m(\mathbb{Q}))$.

Proof. Clearly there is an exact sequence of group homomorphisms:

$$1 \longrightarrow \hat{\phi}(\hat{E}_m(\mathbb{Q})) \longrightarrow E_m(\mathbb{Q}) \xrightarrow{\alpha} \frac{K^*}{K^{*3}} \xrightarrow{N} \frac{\mathbb{Q}^*}{\mathbb{Q}^{*3}}$$

where, $\hat{E}_m : \hat{y}^2 = \hat{x}^3 + 27m$ and $\hat{\phi}$ is as given in [5] (pp. 558–559),

$$\hat{\phi}(\hat{P}) = \left(\frac{\hat{x}^3 + 108m}{9\hat{x}^2}, \frac{\hat{y}(\hat{x}^3 - 216m)}{27\hat{x}^3}\right).$$

This point satisfies $y^2 = x^3 - m$ since when we replace x with $\frac{\hat{x}^3+108m}{9\hat{x}^2}$ and y with $\frac{\hat{y}(\hat{x}^3-216m)}{27\hat{x}^3}$ in $y^2 - x^3 + m = 0$ and factorize the result, we obtain

$$\frac{(\hat{y}^2 - \hat{x}^3 - 27m)(\hat{x}^3 - 216m)^2}{729\hat{x}^6} = 0.$$

Let us compute $3P$ on E_m, where $P=(x,y)$ and $3P \neq \mathcal{O}$.

$$
\begin{aligned}
3P &= (x,y) + \left(\frac{x^4+8mx}{4y^2}, \frac{x^6-20mx^3-8m^2}{8y^3}\right),\\
&= \left(\lambda^2 - x - \frac{x^4+8mx}{4y^2}, \lambda(x-x_3)-y\right), \text{ where}
\end{aligned}
$$

$$
\begin{aligned}
\lambda &= \frac{\frac{x^6-20mx^3-8m^2}{8y^3}-y}{\frac{x^4+8mx}{4y^2}-x},\\
&= \frac{\frac{x^6-20mx^3-8m^2-8y^4}{8y^3}}{\frac{x^4+8mx-4xy^2}{4y^2}},\\
&= \frac{x^6-20mx^3-8m^2-8y^4}{2y(x^4+8mx-4xy^2)},\\
&= \frac{x^6-20mx^3-8m^2-8(x^3-m)^2}{2y(x^4+8mx-4x(x^3-m))},\\
&= \frac{x^6-20mx^3-8m^2-8x^6+16mx^3-8m^2}{2y(x^4+8mx-4x^4+4mx)},\\
&= \frac{7x^6+4mx^3+16m^2}{6xy(x^3-4m)}.
\end{aligned}
$$

Therefore

$$
\begin{aligned}
3P &= (x,y) + \left(\frac{x^4+8mx}{4y^2}, \frac{x^6-20mx^3-8m^2}{8y^3}\right),\\
&= \left(\lambda^2 - x - \frac{x^4+8mx}{4y^2}, \lambda(x-x_3)-y\right),\\
&= \left(\frac{x^9+96mx^6+48m^2x^3-64m^3}{9x^2(x^3-4m)^2},\right.\\
&\qquad \left.\frac{y(x^3+8m)(x^9-228mx^6+48m^2x^3-64m^3)}{27x^3(x^3-4m)^3}\right),\\
&= \left(\frac{p^3+108m}{9p^2}, \frac{q(p^3-216m)}{27p^3}\right), \text{ where}
\end{aligned}
$$

$$
(p,q) = \left(\frac{x^3-4m}{x^2}, \frac{y(x^3+8m)}{x^3}\right) \in \hat{E}_m(\mathbb{Q}) \text{ see [5].}
$$

Since

$$\begin{aligned}\ker\alpha &= \hat{\phi}(\hat{E}_m(\mathbb{Q}))\\ &= \left\{P = \left(\frac{\hat{x}^3+108m}{9\hat{x}^2}, \frac{\hat{y}(\hat{x}^3-216m)}{27\hat{x}^3}\right) \in E_m(\mathbb{Q}) : \hat{y}^2 = \hat{x}^3+27m\right\},\end{aligned}$$

This shows that $3E_m(\mathbb{Q}) \subseteq \ker\alpha$.

Conversely, let $P = (x, y) \in \ker\alpha$. Then there exist $p, q \in \mathbb{Q}$ satisfying $q^2 = p^3 + 27m$ and

$$x = \frac{p^3+108m}{9p^2},$$
$$y = \frac{q(p^3-216m)}{27p^3}.$$

However if we try to solve for p, q we do **not** get $(p, q) = \left(\frac{x^3-4m}{x^2}, \frac{y(x^3+8m)}{x^3}\right)$. This shows that $3E_m(\mathbb{Q}) \neq \ker\alpha$. □

Theorem 5.3. *Let m be a squarefree positive integer with $-m \not\equiv 1 (\mathrm{mod}\ 4)$. Let $K = \mathbb{Q}(\sqrt{-m})$, and $E_m : y^2 = x^3 - m$ be the corresponding elliptic curve. Let $P = \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \in E_m(\mathbb{Q}) \setminus \mathcal{O}$, with $gcd(r,t) = gcd(s,t) = 1$, then $\langle s + t^3\sqrt{-m}\rangle$ is the cube of an ideal, i.e., $\langle s + t^3\sqrt{-m}\rangle = \mathfrak{a}^3$, where $\mathfrak{a} = \langle r, s + t^3\sqrt{-m}\rangle$. There is a group homomorphism $\kappa : E_m(\mathbb{Q}) \longrightarrow Cl(K)[3]$ defined as $\kappa(P) = [\mathfrak{a}]$, whose kernel contains $3E_m(\mathbb{Q})$.*

Proof. The first part is already proved in Theorem 3.2, i.e., $\langle s + t^3\sqrt{-m}\rangle = \mathfrak{a}^3$. Now, let us prove that the map κ is a group homomorphism. Let $y_{P_1} = s_1/t_1^3$, $y_{P_2} = s_2/t_2^3$ and $y_{P_3} = s_3/t_3^3$ for $P_1, P_2, P_3 \in E_m(\mathbb{Q})$. Let $\langle s_1 + t_1^3\omega\rangle = \mathfrak{a}^3$, $\langle s_2 + t_2^3\omega\rangle = \mathfrak{b}^3$ and $\langle s_3 + t_3^3\omega\rangle = \mathfrak{c}^3$, where $\omega = \sqrt{-m}$. Then $\kappa(P_1) = [\mathfrak{a}]$, $\kappa(P_2) = [\mathfrak{b}]$ and $\kappa(P_3) = [\mathfrak{c}]$. To show κ is a homomorphism we need to prove $\kappa(P_1 + P_2) = [\mathfrak{a}\mathfrak{b}] = [\mathfrak{a}][\mathfrak{b}] = \kappa(P_1)\kappa(P_2)$. This is equivalent to proving $\kappa(P_1)\kappa(P_2)\kappa(P_3) = \langle 1\rangle$ for collinear rational points $P_1, P_2, P_3 \in E_m(\mathbb{Q})$. We know by Lemma 5.1 that the map $\alpha : E_m(\mathbb{Q}) \longrightarrow K^*/K^{*3}$ is a homomorphism. Hence, $\alpha(P_1)\alpha(P_2)\alpha(P_3) \in K^{*3}$, i.e., $(s_1 + t_1^3\omega)(s_2 + t_2^3\omega)(s_3 + t_3^3\omega)$ is a cube in K^*. Hence, $(s_1 + t_1^3\omega)(s_2 + t_2^3\omega)(s_3 + t_3^3\omega) = \beta^3$ (say). This gives, $\mathfrak{a}^3\mathfrak{b}^3\mathfrak{c}^3 = \langle\beta\rangle^3$. This implies $\mathfrak{a}\mathfrak{b}\mathfrak{c} = \langle\beta\rangle$. Hence $\kappa(P_1)\kappa(P_2)\kappa(P_3) = \langle\beta\rangle$, a principal ideal, the identity of $Cl(K)[3]$.

We know that $3P \in \ker\alpha$. Thus, $\alpha(3P)$ is a cube, say γ^3 for some $\gamma \in K^*$. Hence for any $P \in E_m(\mathbb{Q})$, $\kappa(3P) = [\mathfrak{b}]$ where $\mathfrak{b}$ is the principal ideal generated by γ. Hence $3E_m(\mathbb{Q}) \subseteq \ker\kappa$. □

Example 5.4. *Let* $K = \mathbb{Q}(\sqrt{-79})$ *and* $E_{79} : y^2 = x^3 - 79$, *where* $-m \equiv 1(mod\ 4)$. *Then* $E_{79}(\mathbb{Q})$ *is generated by* $P = (20, 89)$. *The ideal* $\langle 89 + \sqrt{-79}\rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{q}^3$, *where* $\langle 2\rangle = \mathfrak{p}_1\mathfrak{p}_2$ *and* $\mathfrak{q}$ *is a prime ideal above* 5. *This shows that the condition* $-m \not\equiv 1(mod\ 4)$ *in the above theorem cannot be dropped.*

Example 5.5. *Let* $K = \mathbb{Q}(\sqrt{-26})$ *and* $E_{26} : y^2 = x^3 - 26$, *where* $-m \not\equiv 1(mod\ 4)$. *Then* $E_{26}(\mathbb{Q})$ *is generated by* $P = (3, 1)$ *and* $Q = (35, 207)$. *Also* $P + Q = (881/256, -15735/4096)$. *Then we have* $\langle 1 + \sqrt{-26}\rangle = \mathfrak{p}_3^3$, $\langle 207 + \sqrt{-26}\rangle = \mathfrak{a}^3$, $\langle -15735 + 4096\sqrt{-26}\rangle = \mathfrak{p}_{881}^3$. *The ideals* $\mathfrak{p}_3 = \langle(3, \sqrt{-26} + 1)\rangle$ *and* $\mathfrak{p}_{881} = \langle(881, \sqrt{-26} + 624)\rangle$ *generate ideal classes of order* 3, *whereas the ideal* $\mathfrak{a} = \langle\sqrt{-26} - 3\rangle$ *is principal.*

6. Conclusion

Soleng's homomorphism given in [11] applied to $E_m(\mathbb{Q})$ is $\phi : \left(\frac{r}{t^2}, \frac{s}{t^3}\right) \mapsto [\langle r, -ks + \sqrt{-m}\rangle]$, where $kt^3 + lr = 1$. Let $\mathfrak{a} = \langle r, s + t^3\sqrt{-m}\rangle$, $\mathfrak{b} = \langle r, -ks + \sqrt{-m}\rangle$ and $\mathfrak{c} = \langle r, -ks - \sqrt{-m}\rangle$. Then $\mathfrak{c} \subseteq \mathfrak{a}$ since

$$-ks - \sqrt{-m} = -l\sqrt{-m}(r) - k(s + t^3\sqrt{-m}).$$

Also, since $s + t^3\sqrt{-m} = ls(r) - t^3(-ks - \sqrt{-m})$, $\mathfrak{a} \subseteq \mathfrak{c}$. It follows that $\mathfrak{a} = \mathfrak{c}$. To show that $\mathfrak{b}\mathfrak{c}$ is principal, observe that the conjugate ideal $\bar{\mathfrak{c}} = \bar{\mathfrak{a}}$ of $\mathfrak{c} = \mathfrak{a}$ is equal to $\mathfrak{b}$. It follows that $\mathfrak{a}\mathfrak{b} = \langle N\mathfrak{a}\rangle$, the principal ideal generated by the norm of $\mathfrak{a}$, see [6]. It follows that the classes of the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are inverses in the ideal class group of K. This means that the homomorphism κ and Soleng's homomorphism ϕ are quite similar. The precise relationship, when Soleng's elliptic curve is E_m, is

$$\kappa(P) = (\phi(P))^{-1}.$$

But Soleng did not show that when the elliptic curve is E_m, the image of ϕ belongs to $Cl(K)[3]$.

Similarly there is a relation between the homomorphism ψ given by Hambelton and Lemmermeyer and the homomorphism κ which is given in the following diagram:

$$\begin{tikzcd}
E_m(\mathbb{Q}) \arrow[r, "\kappa"] \arrow[d] \arrow[dr, "f"] & Cl(K)[3] \\
f(E_m(\mathbb{Q})) = S_3^E(\mathbb{Z}) \arrow[r, hook] & S_3(\mathbb{Z}) \arrow[u, "\psi"']
\end{tikzcd}$$

As shown towards the end of §3, f is not a homomorphism. However, the diagram commutes, i.e., $f \circ \psi = \kappa$.

All computations were done using Sage.

7. Acknowledgement

We are extremely grateful to Prof. Sujatha Ramdorai for her kind encouragement. We also want to express our gratitude to the referee whose comments were invaluable and helped us to improve the paper considerably and correct a few mistakes.

References

[1] Ş. Alaca and K. S. Williams, Introductory algebraic number theory, Cambridge Univ. Press, (2004).

[2] D. A. Buell, Class groups of quadratic fields, *Math. Comp.*, **30** (1976), no. 135, 610–623.

[3] D. A. Buell, Elliptic curves and class groups of quadratic fields, *J. London Math. Soc. (2)*, **15** (1977), no. 1, 19–25.

[4] D. A. Buell, Binary quadratic forms, Classical theory and modern computations. Springer-Verlag, New York, (1989).

[5] H. Cohen, Number theory, Vol. I, Tools and Diophantine equations, Springer, New York, (2007).

[6] K. Conrad, Factoring in quadratic fields, http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/quadraticgrad.pdf.

[7] S. Hambleton and F. Lemmermeyer, Arithmetic of Pell surfaces, *Acta Arith.*, **146** (2011), no. 1, 1–12.

[8] F. Lemmermeyer, Why is the class number of $\mathbb{Q}(\sqrt[3]{11})$ even?, *Math. Bohem.*, **138** (2013), no. 2, 149–163.

[9] J. H. Silverman and J. Tate, Rational points on elliptic curves, Springer, New York, (1992).

[10] J. H. Silverman, *The arithmetic of elliptic curves*, Springer, Dordrecht, (2009).

[11] R. Soleng, Homomorphisms from the group of rational points on elliptic curves to class groups of quadratic number fields, *J. Number Theory* **46** (1994), no. 2, 214–229.