ORIGINAL RESEARCH

Integral solutions of certain Diophantine equations in quadratic fields

Richa Sharma[1]

Received: 16 September 2022 / Accepted: 4 December 2025 / Published online: 8 January 2026

Abstract
Let $K = \mathbf{Q}(\sqrt{d})$ a quadratic field and $\mathcal{O}_K$ its ring of integers. We study the solvability of the Diophantine equation $r + s + t = rst = 2$ in $\mathcal{O}_K$. We prove that except for $d = -7, -1, 17$, and 101 this system is not solvable in the ring of integers of other quadratic fields.

Keywords Elliptic curves · Diophantine equation

Mathematics Subject Classification 11D25 · 11D41 · 11G05

1 Introduction

In 1960, Cassels [4] proved that the system of equations

$$r + s + t = rst = 1, \tag{1.1}$$

is not solvable in rationals r, s and t. Later in 1982, Small [3] studied the solutions of (1.1) in the rings $\mathbb{Z}/m\mathbb{Z}$ and in the finite fields F_q where $q = p^n$ with p a prime and $n \geq 1$. Further, in 1987, Mollin et al. [8] considered (1.1) in the ring of integers of $K = \mathbf{Q}(\sqrt{d})$ and proved that solutions exist if and only if $d = -1$, 2 or 5, where r, s and t are units in $\mathcal{O}_K$. Bremner [1, 2] in a series of two papers determined all cubic and quartic fields whose ring of integers contain a solution to (1.1). Later in 1999, Chakraborty et al. [6] also studied (1.1) in the ring of integers of quadratic fields reproducing the findings of Mollin et al. [8] for the original system by adopting a different technique.

Extending the study further, we consider the equation

$$r + s + t = rst = 2. \tag{1.2}$$

The sum and product of numbers equal 1 has natural interest whereas sum and product equal other naturals is a curious question. The method adopted here may not be suitable to consider a general n instead of 2 as for each particular n the system give rise to a particular elliptic curve which may have different 'torsion' and 'rank' respectively. The next case, i.e. when the sum and product equals to 3 is discussed in the last section.

Communicated by Eknath Ghate.

To begin with we perform suitable change of variables and transform (1.2) to an elliptic curve with the Weierstrass form

$$E_{297} : Y^2 = X^3 + 135X + 297 \tag{1.3}$$

and then study E_{297} in the ring of integers of $K = \mathbb{Q}(\sqrt{d})$.

Remark 1 We transform (1.2) into an elliptic curve (1.3) to show that one of the (r, s, t) has to belong to $\mathbb{Q}$ (shown in §3).

System (1.2) gives rise to the quadratic equation

$$x^2 - (2 - r)x + \frac{2}{r} = 0,\ r \neq 0,$$

with discriminant

$$\Delta = \frac{r(r^3 - 4r^2 + 4r - 8)}{r}. \tag{1.4}$$

In hindsight there are infinitely many choices for the quadratic fields contributed by each r of the above form where the system could have solutions. The main result of this article is that the only possibilities are $r = \pm 1, 2$ and -8. Thus (1.2) is solvable only in $K = \mathbf{Q}(\sqrt{d})$ with $d = -7, -1, 17$ and 101. Also the solutions are explicitly given. Throughout this article we denote 'the point at infinity' of an elliptic curve by $\mathcal{O}$. Now we state the main result of the paper.

Theorem 1.1 *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field and $\mathcal{O}_K$ denote its ring of integers. Then the system*

$$r + s + t = rst = 2$$

has no solution in $\mathcal{O}_K$ except for $d = -7, -1, 17$ and 101.

In §4 we discuss the rank of E_{297} in $\mathbb{Q}$ and in quadratic fields of our interest.

2 Preliminaries

In this section we mention some results which are needed for the proof of the Theorem 1.1. First we state a basic result from algebraic number theory.

Theorem 2.1 *Let $K = \mathbb{Q}(\sqrt{d})$ with d a square-free integer, then*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{if } d \equiv 1 \pmod 4, \\ \mathbb{Z}[\sqrt{d}] & \text{if } d \equiv 2, 3 \pmod 4. \end{cases}$$

Now we recall the technique used by Laska in [7] to study the solutions of a family of elliptic curves defined over $\mathbb{Q}$ in the ring of S-integers of a quadratic field. We closely follow this technique to prove Theorem 1.1.

Let $K = \mathbb{Q}(\sqrt{d})$ and s' be the conjugate of an element $s \in K$ over $\mathbb{Q}$. Further $R = \mathcal{O}_K[S^{-1}]$, where S is some finite set of primes in $\mathcal{O}_K$. Thus $\mathcal{O}_K \subset \mathcal{O}_K[S^{-1}] \subset K$.
Laska [7] considered the equation (for $r \in \mathbb{Z}$ and $r \neq 0$)

$$\Gamma_r :\ y^2 = x^3 - r,$$

which defines the Weierstrass form of an elliptic curve (call it E_r) over $\mathbb{Q}$. For an elliptic curve E over $\mathbb{Q}$ the "trace map"

$$\sigma : E(K) \longrightarrow E(\mathbb{Q})$$

is given by

$$\sigma(\mathcal{P}) = \mathcal{P} \oplus \mathcal{P}'.$$

Here $\mathcal{P}'$ is the conjugate of the element $\mathcal{P} \in E(K)$ arising from the conjugation in K and $\oplus$ is the usual elliptic curve addition. Laska considered the "trace map" for Γ_r and calls it

$$\sigma_{r,R} : \Gamma_r(R) \to \Gamma_r(\mathbb{Q}) \cup \{\mathcal{O}\}.$$

If r, R are fixed we simply write σ instead of $\sigma_{r,R}$. The aim was to study $\sigma^{-1}(P)$ for a given $P \in \Gamma_r(\mathbb{Q}) \cup \{\mathcal{O}\}$. He divided this inverse-image set into two parts and called them 'exceptional' and 'non-exceptional' respectively. These two sets consist of:

- an element $\mathcal{P} = (s, t) \in \Gamma_r(R)$ with $s \neq s'$ is called an exceptional solution of Γ_r in R, where (s', t') is the conjugate of $P = (s, t)$.
- non-exceptional solutions of Γ_r in R are contained in $\sigma^{-1}(P)$ for a given $P \in \Gamma_r(\mathbb{Q}) \cup \{\mathcal{O}\}$.

If $\mathcal{P} = (s, t) \in \Gamma_r(R)$ is a non-exceptional solution then $s = s'$ and from the Weierstrass equation that implies $t = \pm t'$. Thus if $P = \mathcal{O}$, then all candidates in $\sigma^{-1}(P)$ are non-exceptional. More precisely, one can show [7] that,

$$\begin{aligned}\sigma^{-1}(\mathcal{O}) = \{(z^{-1}p, z^{-2}q\theta) : (p, q) \in \Gamma_{z^3r}(R \cap \mathbb{Q}),\\ p \in z(R \cap \mathbb{Q}), q \in z^2(R \cap \mathbb{Q})\}\end{aligned} \tag{2.1}$$

where for simplicity it is assumed that $\theta^{-1} \in R$.

If $P \neq \mathcal{O}$, then the non-exceptional solutions $\mathcal{P}$ contained in $\sigma^{-1}(P)$ are exactly given by the conditions

$$\mathcal{P} \in \Gamma_r(R \cap \mathbb{Q}), \mathcal{P} \oplus \mathcal{P} = P.$$

Thus the non-exceptional solutions of Γ_r in R which are contained in $\sigma^{-1}(P)$ are obtained by solving the equation Γ_{z^3r} respectively Γ_r in $R \cap \mathbb{Q}$. Hence either $\mathcal{P} \in \Gamma_r(\mathbb{Q})$ or $\mathcal{P} \oplus \bar{\mathcal{P}} = \mathcal{O}$.

Here we substitute Γ_r by E_{297} and R by $\mathcal{O}_K$ to study the solutions of (1.2) in $\mathcal{O}_K$ by pulling back the elements of $E_{297}(\mathbb{Q})$ using the above mentioned technique of Laska [7].

3 Proof of Theorem 1.1

Proof Let us first transform the system (1.2) to the desired Weierstrass form E_{297}. The system is

$$r + s + t = rst = 2.$$

Putting the value of t, upon simplification, it becomes

$$s + r + \frac{2}{rs} = 2.$$

Now substituting $r = -2/x$ and $s = -y/x$ in the last equation gives

$$y^2 + 2y + 2xy = x^3. \tag{3.1}$$

Putting $x = x_1$ - 1/2 and $y = \frac{y_1}{2} - x_1 - \frac{1}{2}$ in (3.1) rids it from the xy term

$$y_1^2 = 4x_1^3 - 2x_1^2 + 7x_1 + \frac{1}{2}. \tag{3.2}$$

Further substituting $x_1 = x_2 + \frac{1}{6}$ and $y_1 = y_2$ rids (3.2) the x_1^2 term

$$y_2^2 = 4x_2^3 + \frac{20}{3}x_2 + \frac{44}{27}. \tag{3.3}$$

Now again putting $y_2 = Y_1/27$ and $x_2 = X_1/9$ give

$$Y_1^2 = 4X_1^3 + 540X_1 + 1188. \tag{3.4}$$

Finally substituting $Y_1 = 2Y$ and $X_1 = X$ get us the required Weierstrass form

$$E_{297} : Y^2 = X^3 + 135X + 297. \tag{3.5}$$

Here with the help of SAGE [9] we can conclude that

$$E_{297}(\mathbb{Q})_{tors} \cong \mathbb{Z}_3 = \{\mathcal{O}, (3, \pm 27)\}$$

and the $\mathbb{Q}$-rank of E_{297} is zero (we give a mathematical proof of this fact in §4).

Thus $\mathcal{O}$ and $(3, \pm 27)$ are the only $\mathbb{Q}$ rational points of (3.5). It is not difficult to see that the inverse transformation

$$r = 18/(3 - X) \text{ and } s = (Y - 3X - 18)/(3(3 - X))$$

allows us to pass from (3.5) to (1.2). Before proceeding to final leg of the proof of Theorem 1.1, we make a couple of claims and give their proofs.

Claim 1: One of the (r, s, t) satisfying (1.2) must belong to $\mathbb{Q}$.

Proof of claim 1 Two cases need to be considered.

Case I: $\mathcal{P}$ is non-exceptional. In this case either $\mathcal{P} \in E_{297}(\mathbb{Q})$ or $\mathcal{P} \oplus \bar{\mathcal{P}} = \mathcal{O}$. If $\mathcal{P} \in E_{297}(\mathbb{Q})$ then this implies $r \in \mathbb{Q}$.

Let $\mathcal{P} \oplus \bar{\mathcal{P}} = \mathcal{O}$ and $\mathcal{P} = (a + b\sqrt{d}, k + l\sqrt{d})$. As $\mathcal{P}$ is non-exceptional, $b = 0$ and $k = 0$. Thus $\mathcal{P} = (a, l\sqrt{d})$ and in this case too

$$r = 18/(3 - a) \in \mathbb{Q}.$$

Case II: Now if $\mathcal{P}$ is exceptional then $\mathcal{P} + \bar{\mathcal{P}} = (3, \pm 27)$. The curve (3.5) has exactly three elements over $\mathbb{Q}$ and the non-trivial elements are of order 3. Let's call them $\mathcal{O}$, Ω and 2Ω. If $\mathcal{P} + \bar{\mathcal{P}} = \Omega$, then clearly $\mathcal{P} + \Omega$ is non-exceptional, since

$$(\overline{\mathcal{P} + \Omega}) + \mathcal{P} + \Omega = \overline{\mathcal{P}} + \mathcal{P} + 2\Omega = 3\Omega = \mathcal{O}.$$

Now if $\mathcal{P} + \overline{\mathcal{P}} = 2\Omega$, as before we can show that $\mathcal{P} + 2\Omega$ is also non-exceptional. As the claim is valid for non-exceptional elements, it is true for $\mathcal{P} + \Omega$ and $\mathcal{P} + 2\Omega$. Hence it is true for $\mathcal{P}$ itself. □

Hence without loss of generality we assume that $r \in \mathbb{Q}$.
Claim 2 The only possibilities for r satisfying the system

$$r + s + t = rst = 2$$

in $\mathcal{O}_K$ are ± 1, 2 and -8.

Proof of claim 2 As $r \in \mathbb{Q}$ and we are looking for solutions in $\mathcal{O}_K$, this would imply that $r \in \mathbb{Z}$. Three possibilities need to be considered:

- If $r = \pm 1$. In this case solutions exist.
- If r is odd. In this case the denominator of (1.4) will be multiple of an odd number but in $\mathcal{O}_K$ denominator is only 2 or 1 by Theorem 2.1. So in this case there do not exist any solution in $\mathcal{O}_K$.
- If r is even. In this case save for $r = 2$ and -8, the denominator of (1.4) will be multiple of 2 and in some other cases denominator is 1 but $d \equiv 1 \mod 4$. Thus again by Theorem 2.1, in this case too we don't (except for $r = 2, -8$) get any solution in $\mathcal{O}_K$.

Thus except these values of $r = \pm 1$, 2 and -8, this system of equations is not solvable in the ring of integers of other quadratic fields.

□

We are now in a position to complete the proof of Theorem 1.1. We deal with all the four possibilities of r separately.
When $r = 1$, from (3) we have $s + t = 1$ and $st = 2$. Thus we get

$$(s, t) = (\frac{1 - \sqrt{-7}}{2}, \frac{1 + \sqrt{-7}}{2}) \text{ and } (\frac{1 + \sqrt{-7}}{2}, \frac{1 - \sqrt{-7}}{2}).$$

When $r = -1$, we have $s + t = 3$ and $st = -2$. In this case

$$(s, t) = (\frac{3 - \sqrt{17}}{2}, \frac{3 + \sqrt{17}}{2}) \text{ and } (\frac{3 + \sqrt{17}}{2}, \frac{3 - \sqrt{17}}{2}).$$

Similarly when $r = 2$ and -8, we get

$$(s, t) = (i, -i)(-i, i), (\frac{10 + \sqrt{101}}{2}, \frac{10 - \sqrt{101}}{2})$$

$$\text{and } (\frac{10 - \sqrt{101}}{2}, \frac{10 + \sqrt{101}}{2}).$$

To conclude

$$(1, \frac{1 - \sqrt{-7}}{2}, \frac{1 + \sqrt{-7}}{2}), (1, \frac{1 + \sqrt{-7}}{2}, \frac{1 - \sqrt{-7}}{2}),$$
$$(-1, \frac{3 - \sqrt{17}}{2}, \frac{3 + \sqrt{17}}{2}), (-1, \frac{3 + \sqrt{17}}{2}, \frac{3 - \sqrt{17}}{2})$$
$$(-8, \frac{10 + \sqrt{101}}{2}, \frac{10 - \sqrt{101}}{2})(-8, \frac{10 - \sqrt{101}}{2}, \frac{10 + \sqrt{101}}{2})$$
$$(2, i, -i) \text{ and } (2, -i, i).$$

are the only solutions of (3) in $\mathcal{O}_K$. □

4 Rank of E_{297}

In this section we discuss the rank of E_{297} over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{d})$ for $d = -7, -1, 17$ and 101.

Lemma 4.1 *The rank of $E_{297}(\mathbb{Q})$ is zero.*

Proof If possible let rank $E_{297}(\mathbb{Q}) \neq 0$. This would imply that (3.5) have rational solutions. Let $(X, Y) = (\frac{x_1}{x_2}, \frac{y_1}{y_2})$ with $(x_1, x_2) = (y_1, y_2) = 1$, be one such solution. Now putting the values of X and Y in (3.5), we obtain

$$y_1^2 x_2^3 = x_1^3 y_2^2 + 135 x_1 y_2^2 x_2^2 + 297 y_2^2 x_2^3. \tag{4.1}$$

Let p be a prime such that $y_2 = p^\alpha y_{22}$ where $\alpha \in \mathbb{Z}, \alpha \geq 1$ and $(p, y_{22}) = 1$. Putting the value of y_2 in (4.1), gives that right hand side of (4.1) is divisible by p. Therefore $p \mid y_1 x_2$. Which implies either $p \mid y_1$ or $p \mid x_2$. Suppose $p \mid y_1$ then since $y_2 = p^\alpha y_{22}$, we get a contradiction to the fact that $(y_1, y_2) = 1$. Thus $p \mid x_2$ and we write $x_2 = p^\beta x_{22}$ where $\beta \in \mathbb{Z}, \beta \geq 1$ and $(p, x_{22}) = 1$. Now putting this y_2 and x_2 in (4.1), gives

$$p^{3\beta} x_{22}^3 y_1^2 = p^{2\alpha} y_{22}^2 x_1^3 + 135 x_1 p^{2\alpha+2\beta} y_{22}^2 x_{22}^2 + 297 p^{2\alpha+3\beta} y_{22}^2 x_{22}^3. \tag{4.2}$$

Three cases can occur.
Case I. Suppose $3\beta > 2\alpha$. In this case,

$$p^{3\beta-2\alpha} x_{22}^3 y_1^2 = y_{22}^2 x_1^3 + 135 x_1 p^{2\beta} y_{22}^2 x_{22}^2 + 297 p^{3\beta} y_{22}^2 x_{22}^3. \tag{4.3}$$

Further from (4.3)

$$p \mid y_{22} x_1$$

and forces $p \mid x_1$ as $(p, y_{22}) = 1$, which is a contradiction to the fact that $(x_1, x_2) = 1$.
Case II. Suppose $3\beta > 2\alpha$. In that case $p \mid y_1$, which is also contradiction to the fact that $(y_1, y_2) = 1$.
Case III. This case is analogous to Case I.

Hence (4.3) has no solution in $\mathbb{Z}$ and that in turn implies (3.5) has no solution in $\mathbb{Q}$. Thus the rank of $E_{297}(\mathbb{Q})$ defined by the equation (3.5) is zero. □

Lemma 4.2 *The rank of $E_{297}(\mathbb{Q}(\sqrt{d}))$ for $d = -7, 17$ is 1 and for $d = 101$ it is 2.*

Proof Let E/K be an elliptic curve and $d \in K^*$ be such that $L = K(\sqrt{d})$ is a quadratic extension. Let E_d/K be the twist of E/K, then by [5],

$$\text{rank } E(L) = \text{rank } E(K) + \text{rank } E_d(K). \tag{4.4}$$

We conclude using SAGE [9] that (already we have noted that rank $E_{297}(\mathbb{Q}) = 0$) rank $E_{-7\cdot 297}(\mathbb{Q}) = 1$, rank $E_{-1\cdot 297}(\mathbb{Q}) = 1$, rank $E_{17\cdot 297}(\mathbb{Q}) = 1$ and rank $E_{101\cdot 297}(\mathbb{Q}) = 2$.

Now using (4.4) we have,

$$\text{rank } (E(\mathbb{Q}(\sqrt{-7})) = \text{rank } (E(\mathbb{Q}(\sqrt{-1})) = \text{rank } (E(\mathbb{Q}(\sqrt{17})) = 1.$$

$$\text{and rank } (E(\mathbb{Q}(\sqrt{101})) = 2$$

□

5 Concluding remarks

We showed that the system

$$r + s + t = rst = 2$$

has no solution in $\mathcal{O}_K$ except for $d = -7, -1, 17$ and 101 and the solutions are explicitly given.

It would be of interest to consider the next case, i.e,

$$r + s + t = rst = 3. \tag{5.1}$$

Suitable change of variables transform (5.1) to an elliptic curve with Weierstrass form

$$E_{13122} : y^2 = x^3 + 3645x - 13122.$$

Torsion of E_{13122} over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}_3$ and its rank is zero (using SAGE [9]).

We can conclude that except for $d = -2, -1, 7, 10$ and 13, the system (5.1) has no solutions in the ring of integers of K and the solutions can be explicitly given (following analogous argument). Analogously other individual cases can be treated.

Acknowledgements A part of this manuscript was completed while the author was visiting Prof. Sanoli Gun at the Institute of Mathematical Sciences (IMSc), Chennai. She is sincerely grateful to Prof. Sanoli for her generous support and encouragement. It is also a pleasure to thank Prof. Michel Waldschmidt for his valuable comments and suggestions during her visit to IMSc. The author further wishes to express her gratitude to Arkabrata Ghosh for the fruitful discussions related to this work.

References

1. A. Bremner, The equation $xyz = x + y + z = 1$ in integers of a cubic field. *Manuscripta Math.*, **65(4)** (1989), 479–487.
2. A. Bremner, The equation $xyz = x + y + z = 1$ in integers of a quartic field. *Acta Arith.*, **57(4)** (1991), 375–385.
3. C. Small, On the equation $xyz = x + y + z = 1$, *Amer. Math. Monthly*, **89** (1982), 736—749.
4. J. W. S. Cassels, On a diophantine equation, *Acta Arith.*, **6** (1960), 47–52.
5. J. H. Silverman, The Arithmetic of Elliptic Curves, *Grad. Texts in Math.*, **106**, Springer, 1986.
6. K. Chakraborty, M Kulkarni, Solutions of cubic equations in quardratic fields, *Acta Arithmetica*, 1999. https://doi.org/10.4064/AA-89-1-37-43 Corpus ID: 59378550.
7. M. Laska, Solving the equation $x^3 - y^2 = r$ in number fields, *J. Reine Angew. Math.*, **333** (1981), 73–85.
8. R. A. Mollin, C. Small, K. Varadarajan and P. G. Walsh, On unit solutions of the equation $xyz = x + y + z$ in the ring of integers of a quadratic field, *Acta Arith.*, **48** (1987), 341–345.
9. SAGE software, version 4.5.3, http://www.sagemath.org.

Authors and Affiliations

Richa Sharma[1]

✉ Richa Sharma
richasharma582@gmail.com

[1] Department of Mathematics, Jamia Millia Islamia, 110025 New Delhi, India