ACTA ARITHMETICA
LXXXIX.1 (1999)

Solutions of cubic equations in quadratic fields

by

K. Chakraborty (Chennai) and Manisha V. Kulkarni (Bangalore)

Let K be any quadratic field with $\mathcal{O}_K$ its ring of integers. We study the solutions of cubic equations, which represent elliptic curves defined over $\mathbb{Q}$, in quadratic fields and prove some interesting results regarding the solutions by using elementary tools. As an application we consider the Diophantine equation $r+s+t=rst=1$ in $\mathcal{O}_K$. This Diophantine equation gives an elliptic curve defined over $\mathbb{Q}$ with finite Mordell–Weil group. Using our study of the solutions of cubic equations in quadratic fields we present a simple proof of the fact that except for the ring of integers of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$, this Diophantine equation is not solvable in the ring of integers of any other quadratic fields, which is already proved in [4].

1. Introduction. Let $K=\mathbb{Q}(\sqrt{d})$ be a quadratic number field, where d is a square-free rational integer, and let $\mathcal{O}_K$ denote the ring of integers of K. We write $R=\mathcal{O}_K[S^{-1}]$, where S is a finite set of primes in $\mathcal{O}_K$. Hence $\mathcal{O}_K\subset\mathcal{O}_K[S^{-1}]\subset K$. For any $s\in K$ we let $\overline{s}$ denote the conjugate of s over $\mathbb{Q}$. We study the elliptic curve E defined over $\mathbb{Q}$ with Weierstraß equation

$$E:\quad y^2=x^3+Ax+B \tag{1}$$

in the ring of S-integers of K. As an application we consider the Diophantine system of equations $r+s+t=rst=1$. From this equation one gets an elliptic curve

$$y^2=x^3+621x+9774. \tag{2}$$

Using the solutions of the cubic equation (2) in $\mathbb{Q}$, the equation $r+s+t=rst=1$ can also be solved.

Let $E(K)$ denote the group of K rational points of E with identity element denoted as $\mathcal{O}$. We write $\overline{P}=(\overline{s},\overline{t})$ for an element $P=(s,t)\in E(K)$. The symbol $E(R)$ will always denote the set of solutions (s,t) of E with

1991 *Mathematics Subject Classification*: Primary 11D25, 11D41, 11G05.
Key words and phrases: elliptic curves, Diophantine equation.

$s, t \in R$. We are influenced by the treatment of M. Laska in [3], where he handled the equation $y^2 = x^3 + k$ in quadratic fields. Following him, we call an element $P = (s,t) \in E(R)$ *exceptional* if $s \notin \mathbb{Q}$. Hence $E(R)$ consists of two parts, exceptional and non-exceptional. We study these two parts separately.

We state the results of this paper:

THEOREM 1.1. *Let E be an elliptic curve defined over $\mathbb{Q}$. Then there exist infinitely many distinct quadratic fields K such that $E(\mathbb{Q})$ is properly contained in $E(K)$.*

THEOREM 1.2. *Let K be a quadratic field and $Q = (s,t) \in E(K)$. Let $P = (u,v) = Q + \overline{Q} \in E(\mathbb{Z})$. Then Q is $\wp$-integral for every inert or ramified prime $\wp$ in $\mathcal{O}_K$.*

PROPOSITION 1.3. *Let E be an elliptic curve defined over $\mathbb{Q}$ with finite Mordell–Weil group. Then there are only finitely many imaginary quadratic fields K for which $E(K)$ contains integral points (s,t) with $s \notin \mathbb{Q}$.*

THEOREM 1.4. *If $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field with d a square-free integer, then except for $d = -1$ and 2, the equation $r + s + t = rst = 1$ has no solution in the ring of integers of K.*

In Section 2, we study non-exceptional elements of $E(R)$ and prove Theorem 1.1. Section 3 is devoted to exceptional elements of $E(R)$ along with the proof of Theorem 1.2 and Proposition 1.3 as stated above. In Section 4 we give an application and present a simple proof of Theorem 1.4, which is already proved more generally in [4].

2. Non-exceptional solutions of E in R. Let $P = (s,t) \in E(R)$ be such that $s = \bar{s}$. Then from the Weierstraß equation of E we get $t = \pm\bar{t}$. Hence either $P \in E(\mathbb{Q})$ or $P + \overline{P} = \mathcal{O}$. The following obvious lemma characterizes those P's in $E(R)$ such that $P + \overline{P} = \mathcal{O}$.

LEMMA 2.1. *Let $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free rational integer. Then*

$$\{P \in E(R) \mid P + \overline{P} = \mathcal{O}\}$$
$$= \{(d^{-1}x, d^{-2}y\sqrt{d}) : (x,y) \in E_d(R \cap \mathbb{Q}),\ x \in d(R \cap \mathbb{Q}) \text{ and } y \in d^2(R \cap \mathbb{Q})\}$$

where E_d is the twist of E by d over $\mathbb{Q}$ and " + " is the usual addition law on E.

REMARK 2.1. The set $E_d(R \cap \mathbb{Q})$ is finite by Siegel's theorem (cf. [7], p. 255). Now one can write down $E_d(R \cap \mathbb{Q})$ for a given d and for particular S by using SIMATH. Thus one gets all non-exceptional solutions of E in R for that d and S.

Now we use these non-exceptional elements to prove Theorem 1.1.

Proof of Theorem 1.1. Let $a \in \mathbb{Z}$ and define l as

$$l^2 d = a^3 + aA + B \tag{3}$$

for square-free integer d.

Then $(a, l\sqrt{d}) \in E(K)$ and these are non-exceptional elements in $\mathcal{O}_K$. If we could show that there exist infinitely many d in (3) as a varies in $\mathbb{Z}$, then we would have proved the theorem. We prove this fact through a couple of claims.

Let P be the set of primes p that divide $f(a) = a^3 + aA + B$ for some a in $\mathbb{Z}$. The first claim is that P is an infinite set. Suppose that P is finite, and $P = \{p_1, \ldots, p_r\}$. We look at the sets $\{f(a) : a \le N\}$ and $\{p_1^{\alpha_1} \ldots p_r^{\alpha_r} : \alpha_i \le 6 \log N\}$. The cardinality of the first set is greater than or equal to $N/3$ as $f(a)$ is of degree 3 and that of the second is at most $(6 \log N)^r$. For large N this is a contradiction, as the first set is properly contained in the second. Thus P is an infinite set.

Now if possible suppose that, as a varies in $\mathbb{Z}$, the numbers $f(a)$ are equal to a square times one of the square-free numbers $d_1, \ldots, d_t$. Choose a prime $p \in P$ which divides neither $d_1 \ldots d_t$ nor the discriminant of f. Since $p \in P$, we have $p \mid f(a)$ and $p \mid f(a+p)$ for some a.

The next claim is that it is not possible that $p^2 \mid f(a)$ and $p^2 \mid f(a+p)$. For if this were possible, then p^2 divides $f(a+p) - f(a)$, so that $p^2 \mid pf'(a)$. Thus p divides both $f(a)$ and $f'(a)$. This implies that $x - a$ is a double root of $f(x)$ in $\mathbb{F}_p[x]$, contrary to the assumption that p does not divide the discriminant of f. Hence the second claim.

Thus p exactly divides either $f(a)$ or $f(a+p)$. In either case p has to appear in the square-free part, and thus p appears at least in one of the d_i's. This contradicts the fact that p does not divide any of the d_i's. Hence the theorem. ∎

3. Exceptional solutions of E in R. Throughout this section E is an elliptic curve defined over $\mathbb{Q}$ with Weierstraß form (1). We locate the elements $Q = (s,t) \in E(R)$ such that $s \ne \overline{s}$ by using the known non-trivial solutions E in $\mathbb{Q}$. Now we come to the proof of Theorem 1.2.

Proof of Theorem 1.2. Let $\wp$ be a prime in $\mathcal{O}_K$ which is either ramified or inert. The elements in $E(K)$ that reduce to non-singular points modulo $\wp$ form a subgroup $E^0(K)$ of $E(K)$. The kernel of the reduction map is a subgroup $E^1(K)$ of $E^0(K)$. The set $E^1(K)$ contains the elements (s,t) for which s and t have denominators divisible by $\wp$.

As $Q \in E^1(K)$ and since $\wp$ is either ramified or inert, its Galois conjugate $\overline{Q}$ also belongs to $E^1(K)$. Thus if Q is not $\wp$ integral, neither is $\overline{Q}$. Hence

$Q+\overline{Q}$ is not $\wp$ integral either, as $E^1(K)$ is a group. This contradicts the fact that $Q+\overline{Q}=P$ is integral. Hence the theorem. ∎

From now on S is a finite set of primes in $\mathcal{O}_K$ which are ramified or inert. Thus for any elliptic curve defined over $\mathbb{Q}$, exceptional solutions in the ring of S-integers of quadratic fields are in fact integral.

Although Siegel's theorem ensures that $E(R)$ is finite, there is no effective method to write down all the solutions. We show in course of the proof of Proposition 1.3 that in imaginary quadratic fields, one can explicitly write down all the exceptional solutions in $E(R)$.

Proof of Proposition 1.3. Let (s,t) be an integral point over some quadratic field $K=\mathbb{Q}(\sqrt{d})$. Assume that $s\notin\mathbb{Q}$. This implies that $(s,t)+(\bar{s},\bar{t})=(u,v)$ is a non-trivial element of $E(\mathbb{Q})$. As $E(\mathbb{Q})$ is finite, (u,v) is a torsion point and therefore by Nagell–Lutz it has integer coordinates. Let $s=a+b\sqrt{d}$ and $t=k+l\sqrt{d}$, with a, b, k and l either integers or half integers (i.e. $a/2,\dots$ etc. are integers).

We prove the proposition when a, b, k, l are integers; the other case can be tackled similarly.

Clearly $b\neq 0$ and we have the following equations:

$$a^3+3ab^2d+aA+B-k^2-l^2d=0, \tag{4}$$

$$b^2d+3a^2-2k\lambda+A=0, \tag{5}$$

$$u+2A-\lambda^2=0, \tag{6}$$

$$v+k+\lambda(\lambda^2-3a)=0. \tag{7}$$

The first two relations hold as $(s,t)\in E(\mathcal{O}_K)$ and the last two come from the fact that $(\bar{s},\bar{t})=(u,v)$.

Now from (6) we see that λ^2 is an integer, and as λ is a rational number, it is in fact an integer. We eliminate k and a in equation (5) by using equations (7) and (6) respectively and get

$$(2b)^2d=\lambda^4-6u\lambda^2-8v\lambda-3u^2-4A. \tag{8}$$

Since $d<0$, the equation (8) becomes

$$\lambda^4-6u\lambda^2-8v\lambda-3u^2-4A<0. \tag{9}$$

For each u,v and A the strict inequality (9) is satisfied for finitely many $\lambda\in\mathbb{Z}$. A trivial bound of λ may be

$$\lambda\leq\sqrt{18|u|}+(24|v|^{1/3}+(12A+9u^2)^{1/2}).$$

For these λ's we get at most finitely many d for which (8) is satisfied. ∎

4. An application. The equation

$$r + s + t = rst = 1 \tag{10}$$

was studied over the rationals by Cassels [1], over finite fields by Small [8] and over the ring of integers of quadratic fields by Mollin *et al.* [4]. For example, Cassels [1] proved that the system of equations (10) has no solution in $\mathbb{Q}$. The main part of Cassels' proof consists in showing that (2) has no rational solutions (x, y) with $x \neq 3$; he proved it by using the arithmetic of cubic fields. Some time later Sierpiński [6] gave a simpler proof of impossibility of integer solutions (x, y) of (2) with $x \neq 3$. Again Sansone and Cassels [5] gave an elementary proof of the impossibility of rational solutions of (10). Mollin *et al.* [4] studied a more general equation $r + s + t = rst = u$, where u is a unit, and showed that except for $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ this equation has no solution in the ring of integers of any other quadratic field.

In this section first we derive the elliptic curve with Weierstraß form (2) from the Diophantine equation (10). Then we study the equation (10) via the elliptic curve (2) in $\mathcal{O}_K$.

4.1. *Weierstraß form.* Clearly (10) is the same as

$$r + s + \frac{1}{rs} = 1.$$

Putting $r = -1/x$ and $s = -y/x$ reduces this to

$$y^2 + y + xy = x^3. \tag{11}$$

To get rid of the xy term in (11) we change $x = x_1 - 1/12$ and $y = y_1 - x_1/2 - 1/2$. Thus we get

$$y_1^2 = x_1^3 + \frac{23}{48}x_1 + \frac{362}{1728}. \tag{12}$$

Finally, if one puts $x_1 = X/36$ and $y_1 = Y/216$, one gets the required Weierstraß form (2).

The only $\mathbb{Q}$ rational points of (2) are $\mathcal{O}$ and $(3, \pm 108)$. This fact is borrowed from Cremona's table [2].

The inverse transformation

$$r = 36/(3 - X) \quad \text{and} \quad s = (Y - 3X - 99)/(6(3 - X))$$

allows us to pass from (2) to (10).

4.2. *Ring of integers of K.* Here we give a simpler and direct proof of Theorem 1.4 which has already been proved in [4], where a more general equation is considered.

Proof of Theorem 1.4. We claim that one of the (r, s, t) satisfying (10) belongs to $\mathbb{Q}$. If $P = (a + b\sqrt{d}, k + l\sqrt{d})$ is a non-exceptional solution, i.e.,

$P+\overline{P}=\mathcal{O}$, then $b=0$ and $k=0$. Thus $P=(a,l\sqrt{d})$ and in this case $r=36/(3-a)\in\mathbb{Q}$. Now if P is exceptional then $P+\overline{P}=(3,\pm108)$.

Our elliptic curve (2) has exactly three points over $\mathbb{Q}$ and they are points of order 3. Call them $\mathcal{O}$, ω and 2ω. If $P+\overline{P}=\omega$, then clearly $P+\omega$ is non-exceptional, since

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

Now if $P+\overline{P}=2\omega$, similarly one can show that $P+2\omega$ is also non-exceptional. As the claim is valid for non-exceptional elements, it is true for $P+\omega$. Hence it is true for P itself.

Now, without loss of generality assume that $r\in\mathbb{Q}$. As $rst=1$ with $r,s,t\in\mathcal{O}_K$, r,s,t are units. As $r\in\mathbb{Q}$, it follows that $r=\pm1$.

When $r=1$, from (10) we have $s+t=0$ and $st=1$. Thus $(s,t)=(i,-i)$. Now when $r=-1$, then $s+t=2$ and $st=1$ give

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

Thus $(1,i,-i)$, $(-1,1+\sqrt{2},1-\sqrt{2})$ and their permutations are the only solutions of (10) in the algebraic integers of quadratic fields. ■

Acknowledgements. We are extremely grateful to R. Balasubramanian and René Schoof for many fruitful discussions that helped us to improve the presentation and simplify the proofs. We are grateful to Dipendra Prasad for his constant encouragement with valuable comments and to Swarup Mohalik for his kind help in some computations.

Work on this paper began when both the authors were in Mehta Research Institute and was completed when the second author was visiting the Institute of Mathematical Sciences. The second author wishes to acknowledge the hospitality of the Institute of Mathematical Sciences during her stay there.

References

[1] J. W. S. Cassels, *On a diophantine equation*, Acta Arith. 6 (1960), 47–52.

[2] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, Cambridge, 1992.

[3] M. Laska, *Solving the equation $x^3-y^2=r$ in number fields*, J. Reine Angew. Math. 333 (1981), 73–85.

[4] 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.

[5] G. Sansone et J. W. S. Cassels, *Sur le problème de M. Werner Mnich*, ibid. 7 (1962), 187–190.

[6] W. Sierpiński, *Remarques sur le travail de M. J. W. S. Cassels "On a diophantine equation"*, ibid. 6 (1961), 469–471.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[8] C. Small, *On the equation $xyz = x + y + z = 1$*, Amer. Math. Monthly 89 (1982), 736–749.

Institute of Mathematical Sciences
C.I.T. Campus, Taramani
Chennai 600113, India
E-mail: kalyan@imsc.ernet.in

Department of Mathematics
Indian Institute of Science
Bangalore 560012, India
E-mail: manisha@math.iisc.ernet.in

Received on 23.9.1997
and in revised form on 29.9.1998 (3265)