Annales Univ. Sci. Budapest., Sect. Comp. 27 (2007) 145-154

ON THE DIOPHANTINE EQUATION $x + y + z = xyz = 1$

K. Chakraborty (Allahabad, India)

Dedicated to the memory of M.V. Subbarao

Abstract. In this article we survey the results relating to the study of solutions of the Diophantine system of equations $x + y + z = xyz = 1$. We study the equation over the finite fields, the rationals and in the ring of integers of quadratic number fields.

1. Introduction

In 1956 *Werner Mnich* asked "Whether there exist three rationals whose sum and product equals one?", i.e. whether the Diophantine system of equations

$$x + y + z = xyz = 1 \tag{1}$$

is solvable in $\mathbb{Q}$?

In general, *A. Schinzel* demonstrated that for $s > 3$ there exist infinitely many systems of s rational numbers $x_1, \ldots, x_s$ such that

$$x_1 + \ldots + x_s = x_1 \cdots x_s = 1. \tag{2}$$

For example, when $s = 4$, the numbers

$$x_1 = -\frac{1}{n^2 - 1}, \qquad x_2 = \frac{n^2}{n^2 - 1},$$

Mathematics Subject Classification: Primary 11R58; Secondary 11R29

$$x_3 = \frac{1-n^2}{n}, \qquad x_4 = \frac{n^2-1}{n}$$

for $n = 2, 3, 4, \ldots$ satisfy (2).

In this article, I would like to survey the results relating to the study of solutions of this Diophantine system of equtions over finite fields, over rationals and over the ring of integers of the quadratic number fields.

There exist various equivalent form of *Mnich's* question:

(a) The only rational solutions of

$$(r+s+t)^3 = rst$$

have $rst = 0$.

(b) Do the equation

$$\frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 1$$

has integer solutions?

(c) Do there exist rationals r such that all the roots of the equation

$$x^3 - x^2 + rx - 1 = 0$$

are rational?

The equivalence of these questions was proved by *A.Schinzel* [1].

The problem of *Mnich* was orally asked by *L.J. Mordell* to *J.W.S. Cassels*. In 1960, *Cassels* [2] proved the non-existence of rational solutions of (1).

2. Solutions in $\mathbb{Z}/m\mathbb{Z}$ and in $\mathbb{F}_q$

C. Small [4] studied this Diophantine equation in the rings $\mathbb{Z}/m\mathbb{Z}$ and in the finite fields $\mathbb{F}_q$, where $p = p^n$ for some prime p and $n \geq 1$. One can trivially note the following:

- In $\mathbb{Z}/2\mathbb{Z}$ the equation has solution $x = y = z = 1$.
- In $\mathbb{Z}/3\mathbb{Z}$ and in $\mathbb{Z}/4\mathbb{Z}$ there is no solution, as in these rings $xyz = 1$ forces $x, y, z = \pm 1$.

C. Small proved the following result.

Theorem 1. *The equation*

$$x + y + z = xyz = 1 \tag{3}$$

has solutions in $\mathbb{Z}/m\mathbb{Z}$ *iff* $2, 3 \not| m$.

Proof. (Brief sketch) Let $m = 2^{a_0} p_1^{a_1} \cdots p_t^{a_t}$. We need to solve the equation modulo m. The Chinese remainder theorem ensures it is equivalent to solving the same congruence modulo 2^{a_0} and modulo $p_i^{a_i}$. Thus, **Theorem 1** follows from

Theorem 2. *(3) has solutions in* $\mathbb{Z}/p^n\mathbb{Z}$ *for all primes* $p \neq 2, 3$.

The following two steps are required:

- Reduce to the case $n = 1$.
- Use quadratic reciprocity to show existence of solutions in $\mathbb{Z}/p\mathbb{Z}$.

From (3)

$$xy(1 - x - y) = 0$$
$$\Rightarrow xy^2 + (x^2 - x)y + 1 = 0.$$

Disc. of the quadratic is

$$\Delta(x) = (x^2 - x)^2 - 4x.$$

- Thus, if $\Delta(x)$ is a square and divisibility by 2 is allowed in a ring R, our equation has solution in R. Thus,

Lemma 1. *Let* R *be a commutative ring in which* 2 *is invertible and define* $\Delta : R \longrightarrow R$ *by*

$$\Delta(x) = (x^2 - x)^2 - 4x.$$

If there exists elt. $x \in R$ *for which* $\Delta(x)$ *is a square then (3) has a solution in* R.

One uses the Lemma on $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ and quadratic reciprocity to show

Lemma 2. $p > 3$ *and* Δ *is as before. Then there exist* $0 \neq x \in \mathbb{F}_p$ *such that* $\Delta(x)$ *is a square.*

Proof. (Sketch) One can easily check the following:

$x = 1$ works unless $p \equiv 7, 11, 19, -1(24)$.

$x = -1$ works when $p \equiv 7, -1(24)$.

$x = 3$ works when $p \equiv 19(24)$.

$x = -3$ works when $p \equiv 11(24)$.

One uses the properties of the *Legendre symbol* to conclude this.

Combining the two lemmas we get

Proposition 1. *(3) has solutions in $\mathbb{F}_p$ for $p \neq 3$.*

Now to establish the theorem we want to lift solution mod p to solution mod p^n.

- Because of the criterion given by the first Lemma the essential requirement is that we be able to lift squares. The following result allows us to do that.

Lemma 3. *Let $p \not| m$. If m is square modulo p then in fact m is square modulo p^n.*

For any prime $p > 3$ and $x \in \{\pm 1, \pm 3, -4\}$, $\Delta(x)$ is a square modulo p. We have, both x and 2 are invertible in $\mathbb{Z}/p^n\mathbb{Z}$ and $\Delta(x)$ is square in $\mathbb{Z}/p^n\mathbb{Z}$. Thus we are done by **Lemma 1**.

In the same paper the author also counts the solutions of the equation in finite fields by using Vinogradov's method on the homogenized form of the transform of the original equation over F_p. Over F_q, where $q = p^n$, this is done by using the machinery of the zeta-function of the curve associated to this equation.

3. Elliptic curves

We sketch the proof of *Cassels* with a brief introduction to elliptic curves.

- An elliptic curve over a field F means a smooth and projective curve E over F of genus 1 with a fixed F-rational point $\mathcal{O}$.
- E has a unique group structure with identity element $\mathcal{O}$.
- E can be embedded into $\mathbb{P}^2$ as a cubic curve defined by a so-called *Weierstrass equation*

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6$$

with a_i's in F.

- The origin $\mathcal{O}$ corresponds to the point at infinity $(0, 1, 0)$.
- The group law on the set $E(F)$ is defined by

$$P \oplus Q \oplus R = \mathcal{O}$$

if P, Q, R are colinear.

- $Char(F) \neq 2, 3$. E can be defined by

$$y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0.$$

- $P = (x, y), \quad P' = (x', y'), \quad x(P \oplus P") = x''$. Then

$$x'' = \left(\frac{y' - y}{x' - x}\right)^2 - x - x'.$$

- Taking limit as $P' \longrightarrow P$, x-coordinate of $2P = (x'', y'')$

$$x'' = \frac{(3x^2 + a)^2}{4x^3 + 4x + 4b} - 2x.$$

One of the main objects of study of modern number theory is the group $E(F)$ of rational points of E. Its structure is given by Mordell–Weil theorem which was conjectured by *Poincare* when $F = \mathbb{Q}$.

Theorem 3. *The group $E(F)$ is finitely generated. Thus one has an isomorphism*

$$E(F) \simeq \mathbb{Z}^r \oplus E(F)_{tors},$$

r is a non-negative integer and is called the rank of E.

Cassels proved the following theorem.

Theorem 4. *The system of equations*

$$(r + s + t)^3 = rst = 1$$

is not solvable in rationals.

Proof. (Brief sketch) This is equivalent to

Theorem 5. *The only rational solutions of*

$$(r + s + t)^3 = rst \tag{4}$$

have

$$rst = 0.$$

If we do the following change

$$r + s + t = -\frac{1}{4}xt \quad , \quad r - s = \frac{1}{4}yt,$$

(4) becomes

$$E : y^2 = x^3 + (x+4)^2, \tag{5}$$

which is the Weierstrass form of an elliptic curve.

Consider its *Mordell–Weil* group $E(\mathbb{Q})$. By the *Lutz-Nagell theorem* (if (x, y) has finite order in $E(\mathbb{Q})$ then x, y are integers and either $x = 0$ or $x^2|\Delta$), the torsion points of $E(\mathbb{Q})$ have x-coordinate $x = 0$.

Target : *To show that these are the only members of* $E(\mathbb{Q})$*, i.e. the rank of* E *is* 0.

The proof is then completed by proving the above observation. The author used fairly complicated cubic extension to prove this fact.

Cassels and Sansone [3] later gave another proof of the non-solubility of the Diophantine equation in $\mathbb{Q}$. This proof is elementary compared to the first one of *Cassels* and uses infinite decent using factorization in the Eisenstein field.

4. Solutions in the quadratic fields

In 1987, *Mollin et' al.* [5] have investigated this equation over quadratic fields. They found finitely many such fields (namely, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$) in which there exists a solution for integer units u_1, u_2, u_3 of $\mathbb{Q}(\sqrt{d})$ of the equation

$$u_1 u_2 u_3 = u_1 + u_2 + u_3.$$

In a joint work with *M. Kulkarni* [6], the present author studied solutions of general cubic equations in quadratic fields and as an application established the result of Mollin et' al. by a different method (possibly simpler). We need to introduce some notations before proceeding to sketch the proof.

Some notations. Let $K = \mathbb{Q}(\sqrt{d})$ with d square-free be a quadratic field. We denote $\mathcal{O}_K$ as its ring of integers.

For any $s \in K$, let $\bar{s}$ denotes its Galois conjugate over $\mathbb{Q}$. As before, let $E(K)$ denote the group of K-rational points of an elliptic curve E.

We write $\bar{P} = (\bar{s}, \bar{t})$ for an element $P = (s, t) \in E(K)$. We say an element $P = (s, t) \in E(K)$ is "exceptional" if $s \notin \mathbb{Q}$. Now we are in a position to state the theorem.

Theorem 6. *If $K = \mathbb{Q}(\sqrt{d})$, then except for $d = -1$ and $d = 2$, the equation*

$$r + s + t = rst = 1 \tag{6}$$

has no solution in $\mathcal{O}_K$.

Proof. (Sketch) Let us assume that $P = (s, t) \in E(K)$ is "non-exceptional" (n.e.). Then by definition $s = \bar{s}$. Using the Weierstrass equation of the elliptic curve one can easily show that

$$t = \pm\bar{t}.$$

Thus, if P is "n.e.", then either $P \in E(\mathbb{Q})$ or

$$P \oplus \bar{P} = \mathcal{O}.$$

Clearly, (6) is same as

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

Change,

$$r = \frac{-1}{x}, \qquad s = \frac{-y}{x},$$

this gives us

$$y^2 + y + xy = x^3.$$

Change,

$$x = x_1 - \frac{1}{12}, \qquad y = y_1 - \frac{x_1}{2} - \frac{1}{2},$$

and get

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

Finally,

$$x_1 = \frac{X}{36}, \qquad y_1 = \frac{Y}{216},$$

and one gets the required Weierstrass form of an elliptic curve

$$E : Y^2 = X^3 + 621X + 9774. \tag{7}$$

The inverse transformation,

$$r = \frac{36}{(3 - X)}, \qquad s = \frac{(Y - 3X - 99)}{6(3 - X)}$$

allows us to go from (7) to (6).

Now suppose, $(r, s, t) \in \mathcal{O}_K$ is a solution of (6).

Claim: *One of* r, s, t *must be in* $\mathbb{Q}$.

Let $P = \left(a + b\sqrt{d}, k + l\sqrt{d}\right)$ be the corresponding solution for the elliptic curve.

We have two cases to consider:

Case I. P is "n.e.". In this case we have

$$\left(a + b\sqrt{d}, k + l\sqrt{d}\right) \oplus \left(a - b\sqrt{d}, k - l\sqrt{d}\right) = \mathcal{O}.$$

Now from the group law on elliptic curves, if

$$P = (x, y) \text{ then } -P = (x, -y).$$

Thus,

$$\textbf{(i)} \quad a + b\sqrt{d} = a - b\sqrt{d} \Rightarrow b = 0,$$

$$\textbf{(ii)} \quad k + l\sqrt{d} = -k + l\sqrt{d} \Rightarrow k = 0.$$

That makes

$$P = \left(a,\ l\sqrt{d}\right).$$

Thus,

$$r = \frac{36}{(3 - a)} \in \mathbb{Q}.$$

Case II. P is "exceptional". Note that

$$E(\mathbb{Q}) = \{\mathcal{O}, (3, 108), (3, -108)\}.$$

Thus our elliptic curve has exactly three points over $\mathbb{Q}$ and they are points of order 3. Let us call them $\mathcal{O}, \omega, 2\omega$.

- If $P \oplus \bar{P} = \omega$, then $P \oplus \omega$ is "n.e.", as

$$\begin{aligned}(P \oplus \omega) \oplus (P \oplus \omega) &= P \oplus \bar{P} \oplus 2\omega \\ &= \omega \oplus 2\omega \\ &= \mathcal{O}.\end{aligned}$$

- Similarly, if $P \oplus \bar{P} = 2\omega$, then $P \oplus 2\omega$ is "n.e."

As the claim is valid for "n.e." elements, it is true for $(P \oplus \omega)$. Hence it is valid for P. Thus w.o.l.g., we can assume that $r \in \mathbb{Q}$. One has $rst = 1$ with

$r, s, t \in \mathcal{O}_K$. That implies r, s, t are units. As $r \in \mathbb{Q}$, we must have $r = \pm 1$. We need to consider the following possibilities:

- $r = 1 \Rightarrow s + t = 0$ and $st = 1$. That implies

$$(s, t) = (i, -i).$$

- $r = -1 \Rightarrow s + t = 2$ and $st = 1$. That would imply,

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

Thus,

$$(1, i, -i), \quad \left(1, 1 + \sqrt{2}, 1 - \sqrt{2}\right)$$

and all their permutations are the only solutions of our Diophantine equation in $\mathcal{O}_K$.

The next case is the ring of integers of cubic fields and *A. Bremner* [7] have characterized the fields and wrote down the solutions. In another work *A. Bremner* [8] have studied this equation over quadratic fields.

References

[1] **Schinzel A.,** Sur quelques problèmes non résolus d' arithmétique, *L'Enseignement Mathemat.,* **V** (44) (1959).

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

[3] **Sansone G. and Cassels J.W.S.,** Sur le problème de M. Werner Mnich, *Acta Arith.,* **7** (1961/1962), 187-190.

[4] **Small C.,** On the equation $xyz = x + y + z = 1$, *Amer. Math. Monthly,* **89** (10) (1982), 736-749.

[5] **Mollin R.A., Small C., Varadarajan K. and Walsh P.G.,** On unit solutions of the equation $xyz = x + y + z$ in the ring of integers of a quadratic field, *Acta Arith.,* **48** (4) (1987), 341-345.

[6] **Chakraborty K. and Kulkarni Manisha V.,** Solutions of cubic equations in quadratic fields, *Acta Arith.,* **89** (1) (1999), 37-43.

[7] **Bremner A.,** The equation $xyz = x + y + z = 1$ in integers of a cubic field, *Manuscripta Math.,* **65** (4) (1989), 479-487.

[8] **Bremner A.,** The equation $xyz = x + y + z = 1$ in integers of a quartic field, *Acta Arith.,* **57** (4) (1991), 375-385.

(Received February 14, 2007)

K. Chakraborty
Harish Chandra Research Institute
Chhatrag Road, Jhusi
Allahabad 211019, India
kalgan@mri.ernet.in