Indian J. pure appl. Math., **36**(12) : 707-717, December 2005

ON SUMS OF TWO RATIONAL CUBES

KH. HESSAMI PILEHROOD* AND T. HESSAMI PILEHROOD**

*Mathematics Department, Shahrekord University, Iran
E-mail: hessamik@ipm.ir; hessamit@ipm.ir
**Institute for Studies in Theoretical Physics and Mathematics (IPM), Tehran, Iran

(*Received* 22 *September* 2004; *after final revision* 9 *March* 2006; *accepted* 7 *April* 2006)

The aim of this paper is to prove the following statement:

Let p, q be prime numbers, $p \equiv 2 \pmod 3$, $q \equiv 1 \pmod 3$, $4q - p^2 \not\equiv 3 \pmod 9$. Suppose, furthermore, that p is not a cubic residue modulo q. Then the equation $x^3 + y^3 = pqz^3$ has no solutions in nonzero integers x, y, z.

Key Words: Cubic Diophantine Equation; Cubic Residue; Quadratic Field.

1. INTRODUCTION

Since every rational number is a sum of three rational cubes (see, for example, [1, p. 726], [2, p. 83]), it is an interesting question to determine the rational numbers which are sums of two rational cubes, or, if we prefer, the integers a for which

$$x^3 + y^3 = az^3 \qquad \ldots (1)$$

is solvable in integers. We can assume without loss of generality that $a \in \mathbf{N}$ and a is cubefree.

This equation has attracted the attention of many mathematicians over a period of years. Euler [1] proved that eq. (1) is impossible if $a = 1$ and $a = 4$, and that $x = \pm y$ if $a = 2$. Dickson lists 50 papers on the subject before 1918 in his monograph [1], and there has been a comparable amount of work since. We mention in particular the theorem of Sylvester [1].

Theorem — *(see also [2, p. 127]). Let p_1, p_2, p, q_1, q_2, q be primes, $p_1, p_2, p \equiv 5$ (mod 18), $q_1, q_2, q \equiv 11$ (mod 18). Then there are no integer solutions of (1) except $z = 0$ when*

$$a \in \left\{ p, 2p, 9p, p^2, 9p^2, 4p^2, pq, p_1 p_2^2, q, 4q, 9q, 2q^2, q^2, 9q^2, q_1 q_2^2, p^2 q^2 \right\}$$

*This research was in part supported by a grant from IPM (No. 81110028)
**This research was in part supported by a grant from IPM (No. 81110029).

Various methods have been applied to solve (1) or to prove some assertions about its number of solutions (see, for example, [3]). Note that (1) represents the elliptic curve of genus 1

$$E: \quad X^3 + Y^3 = a, \qquad X, Y \in \mathbf{Q} \qquad \ldots (2)$$

so, the theory of elliptic curves can be brought to bear on the problem.

In the works of Cassels [4] and Selmer [5, 6] the method of descent was applied to prove the insolubility of (2) or exhibit a solution (sometimes very large) for all $a < 500$. In the paper of Satgé [7] it was shown that (2) is always soluble for $a = 2p$, $p \equiv 2 \pmod 9$ or $a = 2p^2$, $p \equiv 5 \pmod 9$, p prime. Zagier and Kramarz in their numerical work [8] examined the family of elliptic curves (2) for all $0 < a \leq 70000$. They point out, for example, that among 70000 curves 6347 ones (38.145%) have rank 0 (rank of the elliptic curve E is positive if and only if the equation defining E has infinitely many rational solutions).

The aim of this paper is to prove that for $a = pq$, where p, q are primes, $p \equiv 2 \pmod 3$, $q \equiv 1 \pmod 3$ the eq. (1) is not solvable in nonzero integers x, y, z.

Theorem — *Let p, q be prime numbers, $p \equiv 2 \pmod 3$, $q \equiv 1 \pmod 3$, $4q - p^2 \not\equiv 3 \pmod 9$. Suppose, furthermore, that p is not a cubic residue modulo q. Then the equation*

$$x^3 + y^3 = pqz^3 \qquad \ldots (3)$$

has no solutions in nonzero integers x, y, z.

We have the following equivalent statements about a number a (see [8]):

(*i*) a is a sum of two cubes;

(*ii*) a is a product of three rational numbers with sum 0;

(*iii*) $-432\,a^2$ can be expressed as a square minus a cube;

(*iv*) $16\,a^2$ can be so expressed.

(Here "square" and "cube" mean square or cube of a rational number).

The equivalence of (*i*) and (*ii*) says that the elliptic curve E defined by (2) has a solution if any of the curves

$$a_1 X^3 + a_2 Y^3 + a_3 Z^3 = 0 \quad (a_1, a_2, a_3 \in \mathbf{N}, a_1 a_2 a_3 = a) \qquad \ldots (4)$$

do, and comes from the fact that E is the Jacobian of each of the genus 1 curves (4). The equivalence of (*ii*) and (*iii*) says that the Weierstrass form of E is

$$Y^2 = X^3 - 432\,a^2 \qquad \ldots (5)$$

And the equivalence of (*iii*) and (*iv*) comes from the fact that E is 3-isogenous to the curve

$$Y^2 = X^3 + 16a^2. \qquad \ldots (6)$$

From (4), (5), (6) we have that under the above theorem conditions the equations

$$X^3 + pY^3 + qZ^3 = 0,$$

$$Y^2 = X^3 - 432p^2q^2$$

and

$$Y^2 = X^3 + 16p^2q^2$$

are not solvable in nonzero rationals x, y, z.

For a recent numerical study of Mordell's equation

$$Y^2 = X^3 + k, \qquad 0 \neq k \in \mathbf{Z} \qquad \ldots (7)$$

we mention the work [9], where equation (7) was solved in $\mathbf{Z}$ for all integers k within the range $0 < |k| \leq 10000$ and partially for $10000 < |k| \leq 100000$.

2. AUXILIARY STATEMENTS

Let $\mathbf{Z}[\rho]$ be a ring of integers of the form $a + b\rho$, where $a, b \in \mathbf{Z}$, $\rho^2 + \rho + 1 = 0$. For numbers z_1, z_2, c from this ring we write $z_1 \equiv z_2 \pmod{c}$ if $\frac{z_1 - z_2}{c} \in \mathbf{Z}[\rho]$.

Lemma 1 — Let a, b be integers and let s be a prime number, $s \neq 3$, $a^2 + 3b^2 \not\equiv 0 \pmod{s}$. Then

$$(a + b\sqrt{-3})^{s^2-1} \equiv 1 \pmod{s}.$$

PROOF : The statement is obvious when $s = 2$. When $s > 3$ we have

$$(a + b\sqrt{-3})^s \equiv a^s + b^s\sqrt{-3}^s \equiv a + b(-3)^{\frac{s-1}{2}}\sqrt{-3} \pmod{s},$$

$$(a + b\sqrt{-3})^{s^2} \equiv a^s + b^s(-3)^{\frac{s(s-1)}{2}}(-3)^{\frac{s-1}{2}}\sqrt{-3} \equiv a + b\sqrt{-3} \pmod{s},$$

i.e.,

$$(a + b\sqrt{-3})^{s^2} \equiv a + b\sqrt{-3} \pmod{s}.$$

Since $a+b\sqrt{-3}$ and s are coprime numbers in $\mathbf{Z}[\rho]$, where $\rho^2+\rho+1=0$, this concludes the proof.

Lemma 2 — (Nagell [10]) Let q be a prime, $q \equiv 1 \pmod 3$,

$$q = \frac{q_1^2 + 27\, q_2^2}{4}$$

where q_1, q_2 are natural numbers. Then all the divisors of $q_1\, q_2$ are cubic residues modulo q.

PROOF : See [10].

Lemma 3 — Let x, y be coprime integers. Then $x^2 - xy + y^2$ has no prime divisor $\equiv 2 \pmod 3$.

PROOF : Suppose that P is a prime $\equiv 2 \pmod 3$ and $P \mid (x^2 - xy + y^2)$.
Then

$$P \mid (4x^2 - 4xy + 4y^2) = (x+y)^2 + 3\,(x-y)^2,$$

i.e.,

$$(x+y)^2 + 3\,(x-y)^2 \equiv 0 \pmod P \qquad \ldots (8)$$

Note that

$$(x-y, P) = 1 \qquad \ldots (9)$$

otherwise, since $P \mid (x\,(x-y) + y^2)$, this contradicts the condition $(x, y) = 1$. From (8), (9) we have

$$\left((x+y)\,(x-y)^{-1} \right)^2 \equiv -3 \pmod P$$

or

$$1 = \left(\frac{-3}{P}\right) = (-1)^{\frac{P-1}{2}} \cdot \left(\frac{3}{P}\right) = (-1)^{\frac{P-1}{2}} \cdot (-1)^{\frac{P-1}{2}} \cdot \left(\frac{P}{3}\right)$$

$$= \left(\frac{P}{3}\right) = \left(\frac{3k+2}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{9-1}{8}} = -1,$$

where $\left(\frac{m}{n}\right)$ is Jacobi's symbol.

The contradiction obtained proves the lemma.

Lemma 4 — Let p, q be different primes and let x, y be nonzero integers satisfying $(x, y) = 1$. Suppose, furthermore, that

$$x+y=pq^c\,\gamma\,\alpha^2\,u^3,\quad x^2-xy+y^2=q^{1-c}\,\gamma^2\,\alpha\,\upsilon^3 \qquad \ldots (10)$$

where $c \in \{0, 1\}$, $\alpha, \gamma, u, \upsilon$ are natural numbers. Then

$$\gamma = 1, \qquad \alpha \in \{1, 3\}.$$

PROOF : Suppose that $\gamma > 1$. Then, according to (10), we have

$$\gamma^2 \mid (x^2-xy+y^2) \qquad \text{and} \qquad \gamma \mid (x+y),$$

hence,

$$\gamma^2 \mid (x+y)^2 = x^2+2xy+y^2.$$

This means that $\gamma^2 \mid 3xy$, i.e., $\gamma^2 \mid xy$. According to (10), this contradicts to the condition $(x, y) = 1$. Therefore, $r = 1$ and

$$x+y=pq^c\,\alpha^2\,u^3,\quad x^2-xy+y^2=q^{1-c}\,\alpha\,\upsilon^3.$$

Similarly, we have

$$\alpha \mid (x+y) \qquad \text{and} \qquad \alpha \mid (x^2-xy+y^2).$$

Hence $\alpha \mid 3xy$ or $\alpha \mid 3$ (since $(x, y) = 1$), i.e., $\alpha \in \{1, 3\}$ and lemma is proved.

Lemma 5 — Let p, q be primes, $p \equiv 2 \pmod 3$, $q \equiv 1 \pmod 3$, $4q-p^2 \not\equiv 3 \pmod 9$. Then either

$$\frac{p^2-1}{3} \not\equiv 0 \pmod 3$$

or

$$\frac{q^2-1}{3} \not\equiv 0 \pmod 3.$$

PROOF : Suppose that

$$\frac{p^2-1}{3} \equiv \frac{q^2-1}{3} \equiv 0 \pmod 3.$$

Then $p^2 \equiv q^2 \equiv 1 \pmod 9$. Since $q \equiv 1 \pmod 3$, we have that $q \equiv 1 \pmod 9$. Therefore,

$$4q-p^2 \equiv 4-1=3 \pmod 9.$$

The contradiction obtained proves the lemma.

3. Proof of the Theorem

We shall carry out the proof by contradiction. Let (3) be solvable in nonzero integers x, y, z. Among all the triples (x, y, z) satisfying (3) choose that for which $|z|$ has the minimal value. Obviously, in this case we have $(x, y) = (y, z) = (z, x) = 1$. Since, according to Lemma 3, $x^3 - xy + y^2$ has no prime divisor $\equiv 2 \pmod 3$, from (3) we find that $x + y \equiv 0 \pmod p$. Without loss of generality we can assume that z is a positive integer. Then it follows from the relation

$$pqz^3 = (x+y) \cdot \frac{(x+y)^2 + 3(x-y)^2}{4}$$

that the numbers $x+y$ and $x^2 - xy + y^2$ are also positive integers.

Using prime factorization of the numbers $x+y$ and $x^2 - xy + y^2$, we can write them in the form

$$x + y = pq^c \gamma \alpha^2 u^3, \quad x^2 - xy + y^2 = q^{1-c} \gamma^2 \alpha \upsilon^3,$$

where $c \in \{0, 1\}$, $\alpha, \gamma, u, \upsilon$ are positive integers.

According to Lemma 4, we find that

$$x + y = pq^c \alpha^2 u^3, \quad x^2 - xy + y^2 = q^{1-c} 2 = \alpha \upsilon v, \qquad \ldots (11)$$

where $c \in \{0, 1\}$, $\alpha \in \{1, 3\}$.

Rewrite the second relation of (11) in the form

$$\frac{(x+y)^2 + 3(x-y)^2}{4} = q^{1-c} \alpha \upsilon^3$$

or

$$\frac{\alpha^3 p^2 q^{2c} u^6 + \frac{3}{\alpha} \cdot (x-y)^2}{4} = q^{1-c} \upsilon^3. \qquad \ldots (12)$$

Obviously, $(\upsilon, pq) = 1$ if $c = 1$.

Therefore for proving the theorem only 4 cases remain:

$$(i) \begin{cases} c = 1, \\ \alpha = 1; \end{cases} \quad (ii) \begin{cases} c = 1, \\ \alpha = 3; \end{cases} \quad (iii) \begin{cases} c = 0, \\ \alpha = 1; \end{cases} \quad (iv) \begin{cases} c = 0, \\ \alpha = 3. \end{cases}$$

First let us consider (i). From (12) we have

$$\frac{p^2 q^2 u^6 + 3(x-y)^2}{4} = \upsilon^3$$

or

$$\frac{pqu^3+\sqrt{-3}\,(x-y)}{2}\cdot\frac{pqu^3-\sqrt{-3}\,(x-y)}{2}=\upsilon^3. \qquad \ldots (13)$$

Since the fundamental theorem of arithmetic is valid in the ring $\mathbf{Z}[\rho]$, from (13) we obtain that there exist integers a and b such that

$$\frac{pqu^3+\sqrt{-3}\,(x-y)}{2}=\zeta\left(\frac{a+b\sqrt{-3}}{2}\right)^3, \qquad \ldots (14)$$

where

$$\zeta\in\left\{1,\frac{1\pm\sqrt{-3}}{2}\right\},\quad \upsilon=\frac{a^2+3b^2}{4}\text{ and }(a,\,b)\in\{1,\,2\}.$$

According to Lemma 5, either $\frac{p^2-1}{3}\not\equiv 0 \pmod 3$ or $\frac{q^2-1}{3}\not\equiv 0 \pmod 3$.

If $p\neq 2$, then define the number s as follows:

$$s=\begin{cases} p & \text{if } \dfrac{p^2-1}{3}\not\equiv 0 \pmod 3,\\[2ex] q & \text{if } \dfrac{q^2-1}{3}\not\equiv 0 \pmod 3.\end{cases}$$

Next, raise both sides of (14) to the power $\frac{s^2-1}{3}$, according to Lemma 1, obtain

$$4^{\frac{s^2-1}{3}}\left(\sqrt{-3}\,(x-y)\right)^{\frac{s^2-1}{3}}\equiv\zeta^{\frac{s^2-1}{3}} \pmod s.$$

Here we have used that $(a^2+3b^2,pq)=(\upsilon,pq)=1$. Hence,

$$\zeta^{\frac{s^2-1}{3}}\equiv w \pmod s,$$

where w is a rational integer. Taking into account that $\zeta^3=\pm 1$, $\frac{s^2-1}{3}\not\equiv 0 \pmod 3$, we get a unique possible case $\zeta=1$.

If $p=2$ let us show that $\zeta=1$ as well. If $\zeta=\frac{1\pm\sqrt{-3}}{2}$, then raising both sides of (14) to the power $\frac{q^2-1}{3}$, we see that $q\equiv 1 \pmod 9$. Furthermore, from (14) we have

$$16qu^3 = a^3 - 9ab^2 \pm 9b(a^2 - b^2). \quad \ldots (15)$$

Since $q \equiv 1 \pmod 9$, (15) implies that $a^3 \equiv -2u^3 \pmod 9$, i.e., $a \equiv u \equiv 0 \pmod 3$. We have a contradiction with $(x, y) = (y, z) = (z, x) = 1$. Therefore, $\zeta = 1$.

Further, from (14) we find

$$a(a - 3b)(a + 3b) = 4pqu^3,$$

where $(a, b) \in \{1, 2\}$, $a \not\equiv 0 \pmod 3$. Recall that $z = u\upsilon = \dfrac{a^2 + 3b^2}{4} \cdot u$.

Next, we have

$$a = \sigma_1 X^3, \quad a - 3b = \sigma_2 Y^3, \quad a + 3b = \sigma_3 Z^3,$$

where $\sigma_1, \sigma_2, \sigma_3, X, Y, Z$ are integers, $\sigma_1, \sigma_2, \sigma_3 = 4p \cdot q \cdot 2^{3\beta}$, $\beta \in \{0, 1\}$, $u = 2^\beta XYZ$. All this means that

$$\sigma_2 Y^3 + \sigma_3 Z^3 = 2\sigma_1 X^3.$$

Ranging over the all possible values for $\sigma_1, \sigma_2, \sigma_3, \beta$ we easily get a contradiction either with the fact that p is not a cubic residue modulo q or with the minimum of the value z in eq. (3) for which we have

$$z = \frac{a^2 + 3b^2}{4} \cdot 2^\beta XYZ.$$

(*ii*) If $c = 1$, $\alpha = 3$, then it follows from (12) that

$$\frac{x - y + 3\sqrt{-3}\, pqu^3}{2} = \zeta \left(\frac{a + b\sqrt{-3}}{2} \right)^3,$$

where a, b are integers, $\zeta \in \left\{1, \dfrac{1 \pm \sqrt{-3}}{2}\right\}$.

Next, arguing as in case (*i*), we arrive at a contradiction.

(*iii*) $c = 0$, $\alpha = 1$. According to (11), we have

$$x+y=pu^3, \quad \frac{(x+y)^2+3(x-y)^2}{4} = q\upsilon^3, \quad z=u\upsilon,$$

where u, υ are integers. It follows from (12) that

$$\frac{p^2u^6+(x-y)^2}{4} = q\upsilon^3.$$

This means that there exist nonzero integers q_1, q_3, a, b such that

$$\frac{pu^3+\sqrt{-3}(x-y)}{2} = \frac{q_1+\sqrt{-3}\,q_3}{2}\cdot\left(\frac{a+b\sqrt{-3}}{2}\right)^3, \qquad \text{... (16)}$$

$$q = \frac{q_1^2+3q_3^2}{4}.$$

Then

$$8pu^3 = q_1(a^3-9ab^2) - 9q_3(a^2b-b^3),$$

whence it follows that $q_1^2 \equiv p^2 \pmod 9$. This means that

$$3q_3^2 = 4q-q_1^2 \equiv 4q-p^2 \not\equiv 3 \pmod 9,$$

i.e., $q_3^2 \not\equiv 1 \pmod 3$. Therefore, $q_3 \equiv 0 \pmod 3$. We set $q_3 = 3q_2$, where q_2 is an integer. Then

$$q = \frac{q_1^2+27q_2^2}{4}.$$

From (16) we have

$$\frac{pu^3+\sqrt{-3}(x-y)}{2} = \frac{q_1+3\sqrt{-3}\,q_2}{2}\cdot\left(\frac{a+b\sqrt{-3}}{2}\right)^3.$$

Multiply both sides of the last relation by $27q_2^3$ and consider the equation obtained as a congruence modulo $q=\frac{q_1^2+27q_2^2}{4}$. After elementary transformations, we get

$$\frac{27q_2^3pu^3+27\sqrt{-3}(x-y)q_2^3}{2} \equiv \frac{q_1+3\sqrt{-3}\,q_2}{2}\left(\frac{3q_2a+3q_2b\sqrt{-3}}{2}\right)^3$$

$$\equiv \frac{q_1 + 3\sqrt{-3}\, q_2}{2} \cdot \left(\frac{3q_2 a + q_1 b - b(q_1 - 3\sqrt{-3}\, q_2)}{2} \right)^3$$

$$\equiv \frac{q_1 + 3\sqrt{-3}\, q_2}{2} \cdot \left(\frac{3q_2 a + q_1 b}{2} \right)^3 \pmod{q},$$

whence it follows that

$$8 \cdot 27\, q_2^3\, u^3 \cdot p \equiv q_1 (3q_2 a + q_1 b)^3 \pmod{q}.$$

Since $x + y = pu^3$, $u \not\equiv 0 \pmod{q}$, we note that $pX^3 \equiv q_1 \pmod{q}$, where X is an integer. According to Lemma 2, there exists an integer Y such that $Y^3 \equiv q_1 \pmod{q}$. Thus,

$$pX^3 \equiv Y^3 \pmod{q}, \qquad (Y, q) = 1,$$

whence it follows that p is a cubic residue modulo q and this contradicts the hypothesis of the theorem.

(*iv*) $c = 0$, $\alpha = 3$. In this case, it follows from (11) and (12) that

$$x + y = 9pu^3, \quad \frac{(x-y)^2 + 27p^2u^6}{4} = q\upsilon^3.$$

This implies that there exist integers q_1, q_3, a, b for which

$$\frac{x - y + 3pu^3\sqrt{-3}}{2} = \frac{q_1 + \sqrt{-3}\, q_3}{2} \cdot \left(\frac{a + b\sqrt{-3}}{2} \right)^3,$$

$$q = \frac{q_1^2 + 3q_3^2}{4}.$$

Therefore,

$$3 \cdot 8pu^3 = q_1 (3a^2 b - 3b^3) + q_3 (a^3 - 9ab^2),$$

whence it follows that either $a \equiv 0 \pmod 3$ or $q_3 \equiv 0 \pmod 3$.

If $a \equiv 0 \pmod 3$, then $x - y \equiv 0 \pmod 3$ and taking into account that $x + y \equiv 0 \pmod 3$, we arrive at a contradiction with $(x, y) = 1$. Therefore, $q_3 \equiv 0 \pmod 3$. Set $q_3 = 3q_2$, where q_2 is an integer. Then

$$q = \frac{q_1^2 + 27q_2^2}{4},$$

$$\frac{x-y+3pu^3\sqrt{-3}}{2} = \frac{q_1+3\sqrt{-3}\,q_2}{2}\cdot\left(\frac{a+b\sqrt{-3}}{2}\right)^3.$$

Multiply both sides of the last relation by $27q_2^3$ and consider the equation obtained as a congruence modulo $q = \frac{q_1^2 + 27q_2^2}{4}$. Just as in case (iii), it is easy to show that

$$8\cdot 27\,pu^3 \equiv q_2(3aq_2+bq_1)^3 \pmod{q}.$$

Whence, taking into account that $(x+y, q) = 1$ or $(u, q) = 1$, according to Lemma 2, we obtain that p is a cubic residue modulo q. This contradicts the hypothesis of the theorem.

The contradictions obtained prove the theorem.

REFERENCES

1. L. E. Dickson, *History of the Theory of Numbers*, vol. 2, New York, 1934.
2. L. J. Mordell, *Diophantine equations*. Academic Press (London), 1969.
3. B. N. Delone and D. K. Faddeev. The Theory of Irrationalities of the Third Degree, Vol. 10. *Translations of Mathematical Monographs, American Math. Soc.*, Providence, Rhode Island (1964).
4. J. W. S. Cassels, The rational solutions of the diophantine equation $Y^2 = X^3 - D$. *Acta Math.*, **82** (1950), 243-73.
5. E. Selmer, The diophantine equation $ax^3+by^3+cz^3 = 0$. *Acta Math.*, **85** (1951), 203-362.
6. E. Selmer, The diophantine equation $ax^3+by^3+cz^3 = 0$, Completion of the tables. *Acta Math.*, **92** (1954), 191-97.
7. Ph. Satge, Un analogue du calcul de Heegner. *Invent. Math.*, **87** (1987), 425-39.
8. D. Zagier, G. Kramarz, Numerical investigations related to the L-series of certain elliptic curves. *J. Indian Math. Soc.*, **52** (1987), 51-69.
9. J. Gebel, A. Petho, G. Zimmer, On Mordell's equation. *Compositio Math.*, **110**(3) (1998), 335-67.
10. T. Nagell, Sur les restes et les non-restes cubiques. *Ark. mat.*, **1**(39) (1952), 579-86.