Functiones et Approximatio
53.1 (2015), 167–175
doi: 10.7169/facm/2015.53.1.9

ON THE DIOPHANTINE EQUATION $ax^3 + by + c = xyz$

Sivanarayanapandian Subburam, Ravindrananathan Thangadurai

Abstract: Consider the diophantine equation $ax^3 + by + c = xyz$, where a, b and c are positive integers such that $\gcd(a, c) = 1$ and c is square-free. Let (x, y, z) be a positive integral solution of the equation. In this paper, we shall give an upper bound for x,y and z in terms of the given inputs a, b and c. Also, we apply our results to investigate the divisors of the elements of the sequence $\{an^3 + c\}$ in residue classes.

Keywords: Diophantine equations, positive solutions, upper bound for solutions, divisors in residue classes.

1. Introduction

Consider the diophantine equation

$$ax^3 + by + c - xyz = 0, \tag{1}$$

where x, y and z are unknown positive integers and, a, b and c are fixed positive integers such that $\gcd(a, c) = 1$ and c is square-free. This equation has been studied by many authors including Mohanty [4], Utz [10], Mohanty-Ramasamy [5] and [6], Luca-Togbé [3], Togbé [9], Subburam [7], Subburam-Thangadurai [8], etc.. In 1996, Mohanty-Ramasamy in [6] proved that there are only finitely many integral solutions to (1).

Let $N(a, b, c)$ denotes the number of positive integral solutions (x, y, z) of equation (1). By the result of Mohanty-Ramasamy in [6], it is known that $N(a, b, c)$ exists and it is finite. Recently, Subburam-Thangadurai [8] produced upper bounds for x, y and z, where (x, y, z) is a positive integral solution of equation 1 when $a = 1 = c$ and investigated the divisors of the element of the sequence $\{n^3 + 1\}$ in residue classes modulo n. In this paper, we give upper bounds for x, y and z of equation (1) in terms of a, b and c. Also, by an application of this result, we study the divisors of the elements of the sequence $\{an^3 + c\}$ in residue classes modulo n.

2010 Mathematics Subject Classification: primary: 11D25; secondary: 11D45

Theorem 1. *Any positive integral solution* (x, y, z) *of* (1) *satisfies*

$$x \leqslant abc^6\left[a^2b^3c^8(a^2b^2c^{11} + a^2bc^{11} + 1)^3 + 1\right] + c^2,$$

$$y \leqslant ac^6\left[a^2b^3c^8(a^2b^2c^9 + a^2bc^{11} + 1)^3 + 1\right]$$

and

$$z \leqslant ac^3\left\{abc^5\left[a^2b^3c^8(a^2b^2c^9 + a^2bc^{11} + 1)^3 + 1\right] + c\right\}^2 + bc + c^2.$$

From Theorem 1, we write the following corollary.

Corollary 1. *Let* $M = \max\{a, b, c\}$*. Then any positive integral solution* (x, y, z) *of* (1) *satisfies*

$$\max\{x, y, z\} \leqslant 3^9 M^{128}.$$

Theorem 2. *We have*

$$\sum_{n=1}^{\infty} \sum_{\substack{d \mid an^3 + c \\ d \equiv -b \pmod{n}}} 1 = N(a, b, c).$$

In 1984, H. W. Lenstra [2] proved:

For every real number $\alpha > 1/4$*, there exists a constant* $\kappa(\alpha)$ *with the following property. If* r, s *and* N *are integers such that* $0 \leqslant r < s < N$*,* $s > N^{\alpha}$ *and* $\gcd(r, s) = 1$*, then there are at most* $\kappa(\alpha)$ *positive divisors of* N *which are congruent to* r *modulo* s*.*

Also, in the same paper, he showed that if $\alpha > 1/3$, then $\kappa(\alpha) = 11$. In 2007, Coppersmith *et al* [1] showed that if $\alpha > 0.331$, then $\kappa(\alpha) = 32$. From this result, we can prove that if $n > 2^{48} \max\{a, b\}^{48}$ and b are any positive integers, then

$$\sum_{\substack{d \mid an^3 + c \\ d \equiv -b \pmod{n}}} 1 \leqslant 32.$$

As an immediate consequence of Theorems 1 and 2, we get the following corollary.

Corollary 2. *Let* $M = \max\{a, b, c\}$*. Then we have*

$$\sum_{\substack{d \mid an^3 + c \\ d \equiv -b \pmod{n}}} 1 = 0 \qquad \text{and} \qquad \sum_{m=1}^{\infty} \sum_{\substack{d \mid am^3 + c \\ d \equiv -b \pmod{m}}} 1 \leqslant 3^8 M^{128},$$

where n *is any integer with* $n > 3^4 M^{66}$*.*

2. Preliminaries

Let (x, y, z) be any positive integral solution of equation (1). In this section, we shall prove some lemmas which are useful to prove the main results.

Lemma 1. *If* $\gcd(c, x) = 1$*, then* $\gcd(b, x) = 1$.

Proof. If $\gcd(b, x) = d$ for some integer d, then, by equation (1), we see that $d \mid c$ and hence $d \mid \gcd(x, c) = 1$. This proves the lemma. ■

Lemma 2. *Let* $\gcd(x, c) = d$*. Then we get the positive integers* $x_1 = x/d$*,* $y_1 = \gcd(b, d)y/d$ *and* $z_1 = zd/\gcd(b, d)$ *with* $\gcd(x_1, c/d) = \gcd(ad^2, c/d) = 1$*, such that* $(X, Y, Z) = (x_1, y_1, z_1)$ *satisfies the equation*

$$ad^2X^3 + \frac{b}{\gcd(b, d)}Y + \frac{c}{d} = XYZ. \tag{2}$$

Proof. Let $d = \gcd(x, c)$. Then by letting

$$x_1 = \frac{x}{d} \qquad \text{and} \qquad c_1 = \frac{c}{d},$$

from (1), we get,

$$ax_1x^2 + \frac{by}{d} + c_1 = x_1yz.$$

Therefore

$$\frac{by}{d} = x_1yz - ax_1x^2 - c_1.$$

Since $x_1yz - ax_1x^2 - c_1$ is an integer, by/d is a positive integer. Therefore $d \mid by$. This implies that

$$\frac{d}{\gcd(b, d)} \mid y.$$

Let $d_1 = \gcd(b, d)$ and $y_1 = \gcd(b, d)y/d$. So, the tuple (x_1, y_1, z_1) satisfies

$$ad^2x_1^3 + \frac{b}{d_1}y_1 + c_1 = x_1y_1z_1,$$

where $z_1 = zd/\gcd(b, d)$. Since $\gcd(a, c) = 1$ and c is square-free, we have $\gcd(ad^2, c_1) = 1$ and c_1 is square-free. ■

In the above lemma, if we include the condition $c \mid b$, then we have the following result. This gives the converse part also.

Lemma 3. *Consider equation* (1) *with* $c \mid b$*. Let* $\gcd(x, c) = d$*. Then we get the positive integers* x_1, y *and* z *with* $\gcd(ad^2, c/d) = \gcd(x_1, c/d) = 1$*, such that* $(X, Y, Z) = (x_1, y, z)$ *satisfy the equation*

$$ad^2X^3 + \frac{b}{d}Y + \frac{c}{d} = XYZ. \tag{3}$$

Conversely, if (x, y, z) *is a positive integral solution of equation* (3)*, for some divisor* d *of* c *such that* $\gcd(x, c/d) = 1$*, then* (dx, y, z) *is a positive solution of equation* (1).

Remark 1. Lemma 2 suggests that we can always take a positive solution (x, y, z) of equation (1) with $\gcd(x, c) = 1$. In this case, if the solution (x, y, z) satisfies $x \leqslant f_1(a, b, c)$, $y \leqslant f_2(a, b, c)$ and $z \leqslant f_3(a, b, c)$ for some polynomial functions f_i's in a, b and c with positive coefficients, then, in the general case, the solution (x', y', z') of equation (1) satisfies $x' \leqslant cf_1(ac^2, b, c)$, $y' \leqslant cf_2(ac^2, b, c)$ and $z' \leqslant cf_3(ac^2, b, c)$.

Remark 2. Since $y|(ax^3 + c)$ and $(xz - b)|(ax^3 + c)$, an upper bound of x gives immediately upper bounds for y and z via $y \leqslant ax^3 + c$ and $z \leqslant ax^2 + c + b$.

Lemma 4. *Assume that* $\gcd(x, c) = 1$. *Then there exist positive integers l and r with $xl = by + c$, such that $(X, Y, Z) = (l, y, r)$ satisfy the equation*

$$cX^3 + abc^2Y + ac^3 = XYZ. \tag{4}$$

Proof. Since $\gcd(x, c) = 1$, by Lemma 1, we have $\gcd(x, b) = 1$. As $ax^3 + by + c = xyz$, we see that $x \mid (by + c)$ and $y \mid (ax^3 + c)$. Therefore, let $l = (by + c)/x$. Then $y \mid (xl - c)$. As, $y \mid (ax^3 + c)$, we have $y \mid (cl^3 + ac^3)$. Therefore $y \mid (cl^3 + abc^2y + ac^3)$. Also, as $l \mid (by + c)$, we conclude that $l \mid (cl^3 + abc^2y + ac^3)$.

Let $\lambda = \gcd(l, y)$. Then, as $y \mid (xl - c)$, we have $\lambda \mid c$ and hence $\lambda \mid \gcd(y, c)$. Since $\gcd(x, c) = 1$ and $\lambda \mid \gcd(y, c)$, we get $\lambda \mid a$. Hence $\lambda \mid \gcd(a, c) = 1$. Therefore $\gcd(l, y) = 1$. Then there exists a positive integer r such that

$$cl^3 + abc^2y + ac^3 = lyr.$$

This proves the lemma. ∎

Lemma 5. *Assume that* $\gcd(x, c) = 1$. *Then there exists a positive integral solution $(l(x), y, l(z))$ of equation* (4) *satisfying the following;*

(i) $xl(x) = by + c$.
(ii) *If* $cl(x) \geqslant x$, *then* $l(z) > b$.
(iii) *If* $ax \geqslant l(x)$, *then* $z > b$.
(iv) *If* $x \geqslant (ac + 2)/(2a - 1)$ *and* $l(x) \geqslant x + 2$, *then* $z \leqslant ab$.
(v) *If* $l(x) \geqslant c + 2$ *and* $x \geqslant l(x) + 2$, *then* $l(z) \leqslant abc^2$.

Proof. By Lemma 4, there exist positive integers $l(x)$ and $l(z)$ such that

$$cl(x)^3 + abc^2y + ac^3 = l(x)yl(z)$$

and

$$xl(x) = by + c.$$

This proves (i).

Since $xl(x) = by + c$ and $x \leqslant cl(x)$, we have $c \leqslant cl(x)^2 - by$. Suppose that $l(z) \leqslant b$. Then we get,

$$c \leqslant cl(x)^2 - by \leqslant cl(x)^2 - l(z)y = -(abc^2y + ac^3)/l(x) < 0,$$

which is a contradiction. This proves (ii).

Since $xl(x) = by + c$ and $ax \geqslant l(x)$, we have $c \leqslant ax^2 - by$. Suppose that $z \leqslant b$. Then we get

$$c \leqslant ax^2 - by \leqslant ax^2 - zy = -(by + c)/x < 0,$$

which is a contradiction. This proves (iii).

Now, we put $y = (xl(x) - c)/b$ in $ax^3 + by + c = xyz$. Then we get,

$$z = \left(\frac{ax^2 + l(x)}{xl(x) - c}\right) b.$$

Therefore, to prove (iv), it is enough to prove that if

$$x \geqslant \frac{ac + 2}{2a - 1} \qquad \text{and} \qquad l(x) \geqslant x + 2,$$

then,

$$\left(\frac{ax^2 + l(x)}{xl(x) - c}\right) \leqslant a.$$

Suppose that $(ax^2 + l(x))/(xl(x) - c) > a$. Then $l(x) < (ax^2 + ac)/(ax - 1)$. Since $x \geqslant (ac + 2)/(2a - 1)$, we have $(ax^2 + ac)/(ax - 1) \leqslant x + 2$. Hence, $l(x) < x + 2$ which is a contradiction. Therefore,

$$\left(\frac{ax^2 + l(x)}{xl(x) - c}\right) \leqslant a.$$

Now, we shall assume that

$$l(x) \geqslant c + 2 \text{ and } x \geqslant l(x) + 2.$$

We prove that $l(z) \leqslant abc^2$. Putting $by = l(x)x - c$ in

$$cl(x)^3 + abc^2y + ac^3 = l(x)yl(z),$$

we get,

$$l(z) = \left(\frac{l(x)^2 + acx}{xl(x) - c}\right) bc.$$

Therefore, to prove (v), it is enough to prove that

$$\left(\frac{l(x)^2 + acx}{xl(x) - c}\right) \leqslant ac.$$

Assume that $(l(x)^2 + acx)/(xl(x) - c) > ac$. Then, we get,

$$x < (l(x)^2 + c)/(l(x) - 1).$$

Since $x \geqslant l(x) + 2$, we get

$$l(x) + 2 < (l(x)^2 + c)/(l(x) - 1)$$

and hence

$$l(x) < c + 2,$$

a contradiction. Hence (v) follows. This proves the lemma. ■

Lemma 6. *For any non-zero integers x, a and c, we have*

$$\gcd(ax^2 + x - 1, x^2 - x - c) \qquad \textit{divides} \quad \left|a^2c^2 - 3ac - a - c\right|$$

and

$$\gcd(ax^2 + x + 1, x^2 + x - c) \qquad \textit{divides} \quad \left|a^2c^2 + 3ac + a - c\right|.$$

Proof. Let $d = \gcd(ax^2+x-1, x^2-x-c)$. Then $d \mid (ax^2+x-1)$ and $d \mid (x^2-x-c)$. It is clear that if $q \mid A$ and $q \mid B$ for any integers q, A and B, then $q \mid A - B$. From this argument, we have the first assertion. To get the second assertion, replace x by $-x$ and a by $-a$ in the first assertion and get the result. ■

3. Proof of Theorem 1

Proof. Let (x, y, z) be any positive integral solution of equation (1). By Remark 1, it is enough to assume that $\gcd(x, c) = 1$. Therefore, by Lemma 1, we have $\gcd(x, b) = 1$.

Case 1: $z \leqslant ab$. Since $ax^3 + c = (xz - b)y$, we get $(xz - b) \mid (ax^3 + c)$. Since

$$z^3(ax^3 + c) = (xz - b)(az^2x^2 + abxz + ab^2) + (cz^3 + ab^3),$$

we see that $(xz - b) \mid (cz^3 + ab^3)$. Therefore

$$(xz - b) \leqslant (cz^3 + ab^3).$$

From this, we observe that

$$x \leqslant cz^2 + ab^3 + b \leqslant ab^3 + ca^2b^2 + b. \tag{5}$$

and

$$y \leqslant a(ab^3 + ca^2b^2 + b)^3 + c. \tag{6}$$

Case 2: $z > ab$, $l(x) \geqslant c + 2$ and $x \geqslant l(x) + 2$. Then, by Lemma 5, we have $l(z) \leqslant abc^2$. Therefore, by replacing a by c, b by abc^2 and c by ac^3 in Case 1, we get,

$$y < c(c(abc^2)^3 + ac^5(abc^2)^2 + abc^2)^3 + ac^3.$$

Thus, we get,

$$y \leqslant ac^3[a^2b^3c^4(a^2b^2c^5 + a^2bc^7 + 1)^3 + 1]. \tag{7}$$

Since $xl(x) = by + c$, we get,

$$x \leqslant abc^3[a^2b^3c^4(a^2b^2c^5 + a^2bc^7 + 1)^3 + 1] + c. \tag{8}$$

Therefore, by Remark 2, we get

$$z \leqslant a\left\{abc^3[a^2b^3c^4(a^2b^2c^5 + a^2bc^7 + 1)^3 + 1] + c\right\}^2 + b + c. \tag{9}$$

Case 3: $z > ab$ and, $l(x) < c + 2$ or $x < l(x) + 2$. Suppose that

$$l(x) < c + 2.$$

Then, by Remark 2, we have

$$y \leqslant c(c + 2)^3 + ac^3.$$

Since $x \leqslant by + c$, we have

$$x \leqslant b[c(c + 2)^3 + ac^3] + c.$$

Next we shall assume that $x < l(x) + 2$. By Lemma 4, there exists a positive integral solution $(l(x), y, l(z))$ of equation (4) satisfying $xl(x) = by + c$. Since $z > ab$, by Lemma 5, we conclude that either

$$x < \frac{ac + 2}{2a - 1} \qquad \text{or} \qquad l(x) < x + 2.$$

Consider the case $l(x) - 2 < x < l(x) + 2$. Suppose that $x = l(x)$. Since $xl(x) = by + c$, we get $x^2 = by + c$. Hence, $y = (x^2 - c)/b$. Put this y in $ax^3 + by + c = xyz$. Then we have

$$z = \frac{bx(ax + 1)}{x^2 - c}.$$

Since $\gcd(x, c) = 1$, $\gcd(x, x^2 - c) = 1$. Hence $x^2 - c \leqslant b(ax + 1)$. That is, $x(x - ab) \leqslant b + c$. If $x > ab$, then $x \leqslant b + c$. Otherwise $x \leqslant ab$. Hence, $x \leqslant \max\{b + c, ab\}$.

Suppose that $x = l(x) + 1$. Since $xl(x) = by + c$, $by + c = x(x - 1)$ and so $y = (x^2 - x - c)/b$ and putting this value in equation (1), we get

$$z = \frac{b(ax^2 + x - 1)}{x^2 - x - c}. \tag{10}$$

By Lemma 6, we see that

$$\gcd(ax^2 + x - 1, x^2 - x - c) \qquad \text{divides} \quad \left|a^2c^2 - 3ac - a - c\right|.$$

Therefore, by equation (10), we get,

$$x^2 - x - c \leqslant b\left|a^2c^2 - 3ac - a - c\right|.$$

Thus, we get,

$$x^2 - x - c \leqslant |a^2bc^2 - 3abc - ab - cb|.$$

Hence, we arrive at,

$$x \leqslant |a^2bc^2 - 3abc - ab - cb| + c.$$

Suppose that $l(x) = x + 1$. Since $xl(x) = by + c$, $by + c = x(x + 1)$ and so $y = (x^2 + x - c)/b$. Put this value of y in equation (1), we get

$$z = \frac{b(ax^2 + x + 1)}{x^2 + x - c}.$$

By Lemma 6, we get,

$$x^2 + x - c \leqslant b \left|a^2c^2 + 3ac + a - c\right|.$$

Therefore, we get

$$x \leqslant [b|a^2c^2 + 3ac + a - c| + c]^{1/2}.$$

By Remarks 1 and 2, and equations (10), (11) and (12), we get the bounds. This proves the theorem. ■

4. Proof of Theorem 2

Let n be any positive integer. Let d be a positive divisor of $an^3 + c$ such that $d \equiv -b \pmod{n}$. Then there exists a positive integer m such that $d = mn - b$. Since $(mn-b) \mid (an^3+c)$, there is a positive integer y such that $an^3+c = (mn-b)y$ which in turn satisfies $an^3 + by + c = myn$. That is, for a positive divisor d of $an^3 + c$ with $d \equiv -b \pmod{n}$, we get a positive integral solution (n, y, m) of (1). Indeed, for any two distinct positive divisors d_1 and d_2, $d_1 \equiv -b \pmod{n}$ and $d_2 \equiv -b \pmod{n}$, of $an^3 + c$, we get distinct positive integral solutions of (1). Therefore, we get,

$$\sum_{n=1}^{\infty} \sum_{\substack{d \mid an^3 + c \\ d \equiv -b \pmod{n}}} 1 \leqslant N(a, b, c).$$

For the other inequality, let (n, y, z) be a positive integral solution of (1). Then we see that $(nz - b)$ divides $an^3 + c$ and $nz - b$ is positive as y and $an^3 + c$ are positive. By letting $d = nz - b$, we get a positive divisor of $an^3 + c$ which is $\equiv -b \pmod{n}$. Thus, we get,

$$N(a, b, c) \leqslant \sum_{n=1}^{\infty} \sum_{\substack{d \mid an^3 + c \\ d \equiv -b \pmod{n}}} 1.$$

These inequalities prove the theorem.

References

[1] D. Coppersmith, N. Howgrave-Graham, S.V. Nagaraj, *Divisors in residue classes, constructively*, Math. Comp. **77**(261) (2008), 531–545.

[2] H.W. Lenstra, *Divisors in residue classes*, Math. Comp. **42** (165) (1984), 331–340.

[3] F. Luca, A. Togbé, *On the positive integral solution of the diophantine equation $x^3 + by + 1 - xyz = 0$*, Bull. Malays. Math. Sci. Soc. **31**(2) (2008), 129–134.

[4] S.P. Mohanty, *On the diophantine equation $x^3 + y + 1 - xyz = 0$*, Math. Student **45** (1977), no. 4, (1979) 13–16.

[5] S.P. Mohanty, A.M.S. Ramasamy, *On the positive solution of the diophantine equation $x^3 + by + 1 - xyz = 0$*, Bull. Malays. Math. Sci. Soc. **7**(2) (1984), 23–28.

[6] S.P. Mohanty, A.M.S. Ramasamy, *On the positive solution of the diophantine equation $ax^3 + by + c - xyz = 0$*, J. Indian Math. Soc. (N.S.) **62** (1996), 210–214.

[7] S. Subburam, *On the positive integral solutions of the diophantine equation $x^3 + by + 1 - xyz = 0$*, Ramanujan J. **32**(2) (2013), 203–219.

[8] S. Subburam, R. Thangadurai, *On the diophantine equation $x^3+by+1 = xyz$*, C. R. Math. Rep. Acad. Sci. Canada **36**(1), (2014), 15–19.

[9] A. Togbé, *On the positive integral solutions of the diophantine equation $x^3 + by + 4 - xyz = 0$*, Afr. Diaspora J. Math. **8**(1) (2009), 81–89.

[10] W.R. Utz, *Positive solutions of the diophantine equation $x^3+2y+1-xyz = 0$*, Internat. J. Math. Math. Sci. **5**(2) (1982), 311–314.

Addresses: Sivanarayanapandian Subburam: Institute of Mathematical Sciences, C. I. T. Campus, Taramani, Chennai, 600 113, India;
Ravindrananathan Thangadurai: Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad 211019, India.

E-mail: ssubburam@imsc.res.in, thanga@hri.res.in

Received: 7 November 2014; **revised:** 4 March 2015