Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 632617, 4 pages
http://dx.doi.org/10.1155/2014/632617

Research Article

On the System of Diophantine Equations $x^2 - 6y^2 = -5$ and $x = az^2 - b$

Silan Zhang,[1,2] Jianhua Chen,[1] and Hao Hu[1]

[1] *School of Mathematics and Statistics, Wuhan University, Hubei 430072, China*
[2] *College of Science, Huazhong Agricultural University, Hubei 430070, China*

Correspondence should be addressed to Silan Zhang; 18971077228@163.com

Received 23 March 2014; Accepted 6 June 2014; Published 17 June 2014

Academic Editor: Gustaaf Schoukens

Mignotte and Pethö used the Siegel-Baker method to find all the integral solutions (x, y, z) of the system of Diophantine equations $x^2 - 6y^2 = -5$ and $x = 2z^2 - 1$. In this paper, we extend this result and put forward a generalized method which can completely solve the family of systems of Diophantine equations $x^2 - 6y^2 = -5$ and $x = az^2 - b$ for each pair of integral parameters a, b. The proof utilizes algebraic number theory and p-adic analysis which successfully avoid discussing the class number and factoring the ideals.

1. Introduction

Let $\mathbb{Z}$, $\mathbb{N}$, and $\mathbb{Q}$ be the sets of all integers, positive integers, and rational numbers, and let a, b be the integers. The system of Diophantine equations

$$x^2 - 6y^2 = -5, \qquad x = az^2 - b \tag{1}$$

is a quartic model of an elliptic curve that has been investigated in many papers. Mignotte and Pethő [1] used the Siegel-Baker method to solve (1) for $a = 2$ and $b = 1$; however, their method was complicated as a combination of algebraic and transcendental number theory. In 1998, Cohn [2] gave an elementary proof of the above system of equations for $a = 2$ and $b = 1$. In 2004, Le [3] used a similar elementary method to extend the result of Cohn's work and proposed an effective method solving the system of equations

$$x^2 - Dy^2 = 1 - D, \qquad x = 2z^2 - 1, \tag{2}$$

where $D - 1$ is the power of an odd prime. As an example, solutions of the equations for $D = 6$ and $D = 8$ are given in the paper so as to show the effectiveness of the method.

In this paper, we use algebraic number theory and Skolem's p-adic method [4] to solve (1), and the method is relatively simple. In the proposed method, both the consideration of the class number in the field and the factorization of ideals of integral ring are avoided. Moreover, a faster algorithm proposed in [5] to compute the fundamental unit and the set of nonassociated factors is used.

In order to well interpret the main result, the symbol notation used in this paper is defined as below.

Here, we assume that $m \geq 0$ is an integer and $\varepsilon_0 = 5 + 2\sqrt{6}$ is the fundamental unit in the field $\mathbb{Q}(\sqrt{6})$, and let A denote $(\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m)/(\beta + \overline{\beta})$, where $\beta^2 = \pm\eta\varepsilon_0$ or $\beta^2 = \pm\eta$, with $\eta = 1 + \sqrt{6}$; $\overline{\beta}^2$ denotes the conjugate of β^2 in $\mathbb{Q}(\sqrt{6})$.

The main result of this paper is as follows.

Theorem 1. *Let (x, y, z) be an integral solution of (1). Then z exists only when it satisfies one of the following four equations for $k \in \mathbb{Z}$:*

$$(N1)\ 2az + \theta A = \pm\alpha\varepsilon^k \text{ with } \theta^2 = 2a(1 - \sqrt{-5}),$$
$$(N2)\ 2az + \theta A = \pm\alpha\varepsilon^k \text{ with } \theta^2 = 4a(1 + \sqrt{-5}),$$
$$(N3)\ 2az + \theta A = \pm\alpha\varepsilon^k \text{ with } \theta^2 = 2a(-1 - \sqrt{-5}),$$
$$(N4)\ 2az + \theta A = \pm\alpha\varepsilon^k \text{ with } \theta^2 = 4a(-1 + \sqrt{-5}),$$

where ε is the fundamental unit of the totally complex quartic field of $\mathbb{Q}(\theta)$, α is the nonassociated factor such that $\alpha\alpha_- = 4a(b - \sqrt{-5})$, α_- denotes the relative conjugate of α, and A is referred to above.

As the application to the theorem, we give the following corollary.

Corollary 2. *The system of* (1) *for* $a = 2$ *and* $b = 1$ *has exactly six integral solutions:* $(x, y, z) = (16561, \pm 6761, \pm 91)$, $(71, \pm 29, \pm 6)$, $(17, \pm 7, \pm 3)$, $(7, \pm 3, \pm 2)$, $(1, \pm 1, \pm 1)$, *and* $(-1, \pm 1, 0)$.

2. Proof of the Theorem

Before the proof of the theorem, Lemma 3 is needed.

Lemma 3. *If* m, ε_0, β, *and* $\overline{\beta}$ *are defined as before, then* $A = (\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m)/(\beta + \overline{\beta})$ *is an algebraic number in the field* $\mathbb{Q}(\sqrt{-5})$.

Proof. Rewriting A, we have

$$A = \frac{\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m}{\beta + \overline{\beta}} = \frac{\left(\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m\right)\left(\beta + \overline{\beta}\right)}{\left(\beta + \overline{\beta}\right)^2} = \frac{\beta^2\varepsilon_0^m + \overline{\beta}^2\overline{\varepsilon_0}^m + \beta\overline{\beta}\left(\varepsilon_0^m + \overline{\varepsilon_0}^m\right)}{\beta^2 + \overline{\beta}^2 + 2\beta\overline{\beta}}. \tag{3}$$

Since $\beta^2 + \overline{\beta}^2$, $\beta^2\varepsilon_0^m + \overline{\beta}^2\overline{\varepsilon_0}^m$, and $\varepsilon_0^m + \overline{\varepsilon_0}^m$ are all rational integers and $\beta\overline{\beta} = \sqrt{-5}$, then clearly A is an algebraic number. Thus, the lemma is proven. □

Proof of Theorem. There are four separate cases in consideration during the proof. Since the process is very similar in each case, some details will be omitted for simplicity. Now we prove the theorem.

After rewriting the first equation of (1), factorization in the field $\mathbb{Q}(\sqrt{6})$ yields

$$\left(x + \sqrt{6}y\right)\left(x - \sqrt{6}y\right) = \left(1 + \sqrt{6}\right)\left(1 - \sqrt{6}\right). \tag{4}$$

Then we have

$$\begin{aligned} \left(x + \sqrt{6}y\right) &= \pm\eta\varepsilon_0^n, \\ \left(x - \sqrt{6}y\right) &= \pm\overline{\eta\varepsilon_0}^n, \quad \text{with } n \in \mathbb{Z}. \end{aligned} \tag{5}$$

Adding (5), we get

$$2x = \pm\left(\eta\varepsilon_0^n + \overline{\eta\varepsilon_0}^n\right). \tag{6}$$

The solution of (6) is split into four cases.

Case 1. Assume that $n = 2m + 1$ is odd and $2x = \eta\varepsilon_0^n + \overline{\eta\varepsilon_0}^n$. Then

$$2x = \eta\varepsilon_0^{2m+1} + \overline{\eta\varepsilon_0}^{2m+1} = \left(\beta + \overline{\beta}\right)^2\left(\frac{\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m}{\beta + \overline{\beta}}\right)^2 - 2\beta\overline{\beta}, \quad \text{with } \beta^2 = \eta\varepsilon_0. \tag{7}$$

Since

$$\left(\beta + \overline{\beta}\right)^2 = 34 + 2\sqrt{-5} = \left(1 - \sqrt{-5}\right)\left(3 + \sqrt{-5}\right)^2, \quad \beta\overline{\beta} = \sqrt{-5}, \tag{8}$$

by inserting (7) and the second equation of (1) into (6), we get

$$2az^2 - \theta^2A^2 = 2\left(b - \sqrt{-5}\right), \tag{9}$$

where $\theta^2 = 1 - \sqrt{-5}$ and $A = (3 + \sqrt{-5})((\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m)/(\beta + \overline{\beta}))$. We multiply both sides of the equation by $2a$ to obtain

$$(2az)^2 - \theta^2A^2 = 4a\left(b - \sqrt{-5}\right) = \alpha\alpha_-. \tag{10}$$

Without loss of generality, we also denote $\theta^2 = 2a(1 - \sqrt{-5})$ and $A = (3 + \sqrt{-5})((\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m)/(\beta + \overline{\beta}))$. Factoring (9) in the field $\mathbb{Q}(\theta)$, we have

$$(N1)\ 2az + \theta A = \pm\alpha\varepsilon^k, \quad \text{with } \theta^2 = 2a\left(1 - \sqrt{-5}\right),\ k \in \mathbb{Z}. \tag{11}$$

Case 2. In another case, when $n = 2m$ is even and $2x = \eta\varepsilon_0^n + \overline{\eta\varepsilon_0}^n$, then

$$2x = \eta\varepsilon_0^{2m} + \overline{\eta\varepsilon_0}^{2m} = \left(\beta + \overline{\beta}\right)^2\left(\frac{\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m}{\beta + \overline{\beta}}\right)^2 - 2\beta\overline{\beta}, \quad \text{with } \beta^2 = \eta. \tag{12}$$

Similarly, we have

$$(2az)^2 - \theta^2A^2 = 4a\left(b - \sqrt{-5}\right) = \alpha\alpha_-, \tag{13}$$

where $\theta^2 = 4a(1 + \sqrt{-5})$ and $A = (\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m)/(\beta + \overline{\beta})$. Furthermore, we know that z satisfies

$$(N2)\ 2az + \theta A = \pm\alpha\varepsilon^k \quad \text{with } \theta^2 = 4a\left(1 + \sqrt{-5}\right),\ k \in \mathbb{Z}. \tag{14}$$

Case 3. Consider $n = 2m + 1$ is odd and $2x = -(\eta\varepsilon_0^n + \overline{\eta\varepsilon_0}^n)$. By the same consideration, we deduce that z satisfies

$$(N3)\ 2az + \theta A = \pm\alpha\varepsilon^k \quad \text{with } \theta^2 = 2a\left(-1 - \sqrt{-5}\right),\ k \in \mathbb{Z}, \tag{15}$$

where $A = (3 - \sqrt{-5})((\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m)/(\beta + \overline{\beta}))$.

Case 4. Consider $n = 2m$ is even and $2x = -(\eta\varepsilon_0^n + \overline{\eta\varepsilon_0}^n)$. Similarly, we know that z satisfies

$$(N4)\ 2az + \theta A = \pm\alpha\varepsilon^k \quad \text{with } \theta^2 = 4a\left(-1 + \sqrt{-5}\right),\ k \in \mathbb{Z}, \tag{16}$$

where $A = (\beta\varepsilon_0^m + \overline{\beta}\overline{\varepsilon_0}^m)/(\beta + \overline{\beta})$.

Thus, we complete the proof of the theorem. □

3. Proof of the Corollary

Remark 4. The method of the proof of the corollary is a special instance of general procedure for the computation of integral points on some quartic model of elliptic curves. The method is relatively simple, because it avoids the use of class number and ideal factorization in imaginary quartic fields.

Before the proof, we give the following lemma.

Lemma 5. *For any integer $m \neq 0$ and $i > 1$, one has $V_p(p^i \binom{m}{i}) > V_p(p \binom{m}{1})$, where $V_p(\cdot)$ denotes the standard p-adic valuation and p is an odd prime.*

Proof. We know

$$\begin{aligned} & V_p\left(p^i \binom{m}{i}\right) - V_p\left(p \binom{m}{1}\right) \\ &= i - 1 + V_p\binom{m}{i} - V_p\binom{m}{1} \\ &= i - 1 + V_p\left(\frac{(m-1)\cdots(m-i+1)}{i!}\right) \\ &= i - 1 + V_p\left((m-1)\cdots(m-i+1)\right) - V_p(i!) \\ &\geq i - 1 - V_p(i!) \\ &= i - 1 - \left(\left[\frac{i}{p}\right] + \left[\frac{i}{p^2}\right] + \cdots\right) \\ &\geq i - 1 - \frac{i}{p-1} \\ &\geq \left(\frac{p-2}{p-1}\right) i - 1 > 0, \quad \text{with } i > 1. \end{aligned} \tag{17}$$

Therefore, for $i > 1$, the p-adic valuation of the term of $p^i \binom{m}{i}$ exceeds the p-adic valuation of the term of $p \binom{m}{1}$. Thus, we complete the proof of Lemma 5. □

To complete the proof of the corollary, the fundamental unit in the totally complex quartic field $\mathbb{Q}(\theta)$ is computed. Furthermore, nonassociated factor of $2 - 2\sqrt{-5}$ in the ring of integers of $\mathbb{Q}(\theta)$ is also calculated. The idea of computation of fundamental unit and nonassociated factorization stems from Zhu and Chen [5, 6] and Buchmann's work [7], which offered a fast implementation scheme. Results are obtained via MATHEMATICA 7.0, which are listed in Table 1.

Proof of Corollary. Case 1. Substituting $a = 2$ and $b = 1$ into (9), we know that z satisfies

$$4z^2 - \theta^2 A^2 = 2 - 2\sqrt{-5} = \alpha\alpha_{-}. \tag{18}$$

Equation *(N1)* is reduced to

$$(N5)\ 2z + \theta A = \pm\alpha\varepsilon^k \quad \text{with } \theta^2 = 1 - \sqrt{-5},\ k \in \mathbb{Z}. \tag{19}$$

From Table 1, we get $\varepsilon = 11 + 2\theta - 6\theta^2 - 4\theta^3$ and $\alpha = 6 + 4\theta - \theta^3$. From Lemma 3, we know that A is an element in the field $\mathbb{Q}(\sqrt{-5})$. If we expand $2z + \theta A$ in the basis $1, \theta, \theta^2$, and θ^3 of $\mathbb{Q}(\theta)$, we obtain $2z + \theta A = a + b\theta + c\theta^2 + d\theta^3$ $(a, b, c, d \in \mathbb{Q})$; then, from Lemma 3, we also know that $c = 0$. In short, we denote this fact by $(2z + \theta A)_2 = 0$.

To use the p-adic analysis, a suitable prime p is needed. Here, we take $p = 7$. A straightforward computation shows that

$$\varepsilon^8 \equiv 1 \pmod 7. \tag{20}$$

Since $(\alpha\varepsilon^0)_2 \equiv 0 \pmod 7$, $(\alpha\varepsilon^7)_2 \equiv 0 \pmod 7$, and $(\alpha\varepsilon^i)_2 \not\equiv 0 \pmod 7$ $(i = 2, \ldots, 6)$, we get $k \equiv 0, 7 \pmod 8$.

(i) Let $k \equiv 0 \pmod 8$; since $\varepsilon^8 \equiv 1 \pmod 7$, we obtain $\varepsilon^8 = 1 + 7\xi$; then

$$\begin{aligned} \pm(2z + \theta A) = \alpha(1 + 7\xi)^m &= \alpha + 7\binom{m}{1}(\alpha\xi) \\ &+ 7^2\binom{m}{2}(\alpha\xi^2) + \cdots + 7^m\binom{m}{m}(\alpha\xi^m), \end{aligned} \tag{21}$$

with $k = 8m$. So we have

$$\pm(2z + \theta A)_2 = \left(\alpha + 7\binom{m}{1}(\alpha\xi) + \cdots + 7^m\binom{m}{m}(\alpha\xi^m)\right)_2. \tag{22}$$

From Lemma 5 and $(\alpha\xi)_2 = (-30 + 30\theta + 60\theta^2 + 30\theta^3)_2 \not\equiv 0 \pmod 7$, we get $m = 0$ and $z = \pm 3$ by working modulo 7^{r+2} on formula (13), where $7^r \| m$.

(ii) When $k \equiv 7 \pmod 8$, we have

$$\begin{aligned} \pm(2z + \theta A) = \alpha\varepsilon^{-1}(1 + 7\xi)^m &= \alpha\varepsilon^{-1} + 7\binom{m}{1}(\alpha\varepsilon^{-1}\xi) \\ &+ \cdots + 7^m\binom{m}{m}(\alpha\varepsilon^{-1}\xi^m), \end{aligned} \tag{23}$$

with $k = -1 + 8m$. So we have

$$\begin{aligned} \pm(2z + \theta A)_2 = \Big(\alpha\varepsilon^{-1} &+ 7\binom{m}{1}(\alpha\varepsilon^{-1}\xi) \\ &+ \cdots + 7^m\binom{m}{m}(\alpha\varepsilon^{-1}\xi^m)\Big)_2. \end{aligned} \tag{24}$$

Similar deduction shows that $m = 0$ and $z = \pm 68$.

Case 2. Secondly, we similarly consider the following equation:

$$(N6)\ 2z + \theta A = \pm\alpha\varepsilon^k, \quad \text{with } \theta^2 = 2 + 2\sqrt{-5},\ k \in \mathbb{Z}. \tag{25}$$

From Table 1, we get $\varepsilon = -49 - 20\theta + 3\theta^2 + (7/2)\theta^3$ and $\alpha = 2 + \theta$. By the same argument we choose $p = 23$ and $\varepsilon^{11} \equiv 1 \pmod{23}$. Similarly we have $k \equiv 0, 1 \pmod{11}$; then we can deduce $z = \pm 1$ and $z = \pm 91$, respectively.

Case 3. Consider the following equation:

$$(N7)\ 2z + \theta A = \pm\alpha\varepsilon^k \quad \text{with } \theta^2 = -1 - \sqrt{-5},\ k \in \mathbb{Z}. \tag{26}$$

Table 1: Associated number field.

θ^2	Integral basis	Fundamental unit	Nonassociated factor of $2-2\sqrt{-5}$
$1-\sqrt{-5}$	$1,\theta,\theta^2,\theta^3$	$11+2\theta-6\theta^2-4\theta^3$	$6+4\theta-\theta^3$
$2+2\sqrt{-5}$	$1,\theta,\frac{1}{2}\theta^2,\frac{1}{4}\theta^3$	$-49-20\theta+3\theta^2+\frac{7}{2}\theta^3$	$2+\theta$
$-1-\sqrt{-5}$	$1,\theta,\theta^2,\theta^3$	$-85+34\theta+30\theta^2+38\theta^3$	$4+\theta^3$
$-2+2\sqrt{-5}$	$1,\theta,\frac{1}{2}\theta^2,\frac{1}{4}\theta^3$	$1-2\theta-\theta^2-\frac{1}{2}\theta^3$	$12-\theta$

Table 2: Positive z-value of the solution.

	$a=1$	$a=2$	$a=3$	$a=4$	$a=5$	$a=6$	$a=7$	$a=8$	$a=9$	$a=10$
$b=1$	$z=0$	$z=0,1,2,3,6,91$	$z=0$	$z=0$	$z=0$	$z=0$	$z=0$	$z=0,1,3$	$z=0$	$z=0$
$b=2$	$z=1,3$	NS	$z=1$	NS	NS	NS	NS	NS	$z=1$	NS
$b=3$	$z=2$	$z=1,59$	NS	$z=1$	$z=2$	NS	NS	NS	NS	$z=1,83$
$b=4$	NS	NS	$z=1,5$	NS	$z=1$	NS	NS	NS	NS	NS
$b=5$	$z=2$	NS	$z=2$	$z=1$	NS	$z=1$	NS	NS	NS	NS
$b=6$	NS	NS	NS	NS	$z=1$	NS	$z=1,5$	NS	NS	NS
$b=7$	$z=0$	$z=0,2$	$z=0$	$z=0$	$z=0$	$z=0,1,2$	$z=0$	$z=0,1$	$z=0$	$z=0$
$b=8$	$z=1,3,5,41$	NS	NS	NS	NS	NS	$z=1$	NS	$z=1$	NS
$b=9$	$z=4$	$z=1,2,29$	NS	$z=2$	$z=4$	NS	NS	$z=1$	NS	$z=1$
$b=10$	$z=3,9$	NS	$z=1,3$	NS	NS	NS	NS	NS	$z=1,3$	NS

"NS" refers to "no solution."

We also have $\varepsilon=-85+34\theta+30\theta^2+38\theta^3$, $\alpha=4+\theta^3$, $p=5$, and $\varepsilon^4\equiv 1(\mathrm{mod}\,5)$. Direct deductions show that $z=\pm 2$ and $z=\pm 11798$.

Case 4. The final equation is

$$(N8)\ 2z+\theta A=\pm\alpha\varepsilon^k \quad \text{with } \theta^2=-2+2\sqrt{-5},\ k\in\mathbb{Z}. \tag{27}$$

It corresponds to $\varepsilon=1-2\theta-\theta^2-(1/2)\theta^3$, $\alpha=12-\theta$, $p=13$, and $\varepsilon^5\equiv 1(\mathrm{mod}\,13)$. A similar deduction yields $z=0$ and $z=\pm 6$.

All in all, if (x,y,z) is an integral solution of (1),

$$\pm z=3,68,1,91,2,11798,0,6. \tag{28}$$

Substituting (24) into the system of Diophantine equations (1), we get all integral solutions, namely, $(x,y,z)=(16561,\pm 6761,\pm 91)$, $(71,\pm 29,\pm 6)$, $(17,\pm 7,\pm 3)$, $(7,\pm 3,\pm 2)$, $(1,\pm 1,\pm 1)$, and $(-1,\pm 1,0)$.

This completes the proof of the corollary. □

Remark 6. Like before, we can solve a family of systems of Diophantine equations (1). As a direct application of this theorem, systems of equations with parameters $1\le a\le 10$ and $1\le b\le 10$ are solved and results are listed in Table 2. For simplicity, we only list the positive z-value of solutions (x,y,z).

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is partly supported by the Fundamental Research Funds for the Central Universities (no. 2662014QC010) and National Natural Science Foundation of China (61202305).

References

[1] M. Mignotte and A. Pethő, "On the system of Diophantine equations $x^2-6y^2=-5$ and $x=2z^2-1$," *Mathematica Scandinavica*, vol. 76, no. 1, pp. 50–60, 1995.

[2] J. H. E. Cohn, "The Diophantine system $x^2-6y^2=-5, x=2z^2-1$," *Mathematica Scandinavica*, vol. 82, no. 2, pp. 161–164, 1998.

[3] M. H. Le, "On the Diophantine system $x^2-Dy^2=1-D$ and $x=2z^2-1$," *Mathematica Scandinavica*, vol. 95, no. 2, pp. 171–180, 2004.

[4] H. Brandt and Th. Skolem, *Diophantische Gleichungen. (Erg. d. Math. u. ihrer Grenzgebiete, 5. H. 4)*, Verlag Julius Springer, Berlin, Germany, 1938.

[5] H. L. Zhu and J. H. Chen, "Integral points on certain elliptic curves," *Rendiconti del Seminario Matematico della Università di Padova*, vol. 119, pp. 1–20, 2008.

[6] H. Zhu and J. Chen, "Integral points on $y^2=x^3+27x-62$," *Journal of Mathematical Study*, vol. 42, no. 2, pp. 117–125, 2009.

[7] J. Buchmann, "The computation of the fundamental unit of totally complex quartic orders," *Mathematics of Computation*, vol. 48, no. 177, pp. 39–54, 1987.