REND. SEM. MAT. UNIV. PADOVA, Vol. 119 (2008)

Integral Points on Certain Elliptic Curves.

HUI LIN ZHU (*) - JIAN HUA CHEN (**)

ABSTRACT - By using algebraic number theory method and p-adic analysis method, we find all integral points on certain elliptic curves

$$y^2 = (x+a)(x^2+bx+c), \quad a,b,c \in \mathbf{Z}, \quad b^2 < 4c.$$

Furthermore, we can find all integer solutions of certain hyperelliptic equations

$$Dy^2 = Ax^4 + Bx^2 + C, \ B^2 < 4AC.$$

As a particular example, we give a complete solution of the equation which was proposed by Zagier

$$y^2 = x^3 - 9x + 28$$

by this method. In Appendix I and Appendix II, we give the computational method of finding the fundamental unit and factorizing quadratic algebraic number in the subring of a totally complex quartic field, respectively.

1. Introduction.

A. Baker [1] developed a method based on linear forms in the logarithms of algebraic numbers, so as to derive an upper bound for the solutions of certain Diophantine equations including elliptic curve. Unfortunately, this upper bound is too large and sometimes beyond the range of computer searching.

Recent results on elliptic logarithm methods [2] [3] [4] have allowed the determination of integral points on certain elliptic curves rank as big as 8, but in order to apply it we need the generators of infinite order of the

(*) Indirizzo dell'A.: School of Mathematical Sciences, Xiamen University, Fujian 361005, China.

E-mail: huilin9200@yahoo.com

(**) Indirizzo dell'A.: School of Mathematics and Statistics, Wuhan University, Wuhan 430072, P.R. China.

E-mail: chenjh_ecc@163.com

The project is supported by the National Natural Science Foundation of China (2001AA141010).

Mordell-Weil group and the torsion group of the elliptic curve, and the rank should not be too high and the canonical heights of the generators should not be too large either. Mathematicians are asking for simpler method. In this paper, we use an elementary method containing algebraic number theory and p-adic analysis to find all integral points on certain elliptic curves.

In section 2, by this method, we find all integral points $(x, y) = (-4, 0)$, $(-1, \pm 6)$, $(9, \pm 26), (764396, \pm 668309460)$ of the equation proposed by Zagier [5]

$$y^2 = x^3 - 9x + 28. \tag{1.1}$$

In section 3, we find all integral points on a class of elliptic curves

$$y^2 = (x + a)(x^2 + bx + c), \quad a, b, c \in \mathbf{Z}, \tag{1.2}$$

where the discriminant of $x^2 + bx + c$, denote as Δ, satisfies $\Delta = b^2 - 4c < 0$. Furthermore, we can find all integer solutions of certain hyperelliptic Diophantine equations

$$Dy^2 = Ax^4 + Bx^2 + C, \quad B^2 < 4AC. \tag{1.3}$$

In section 4, we discuss other cases of equation (1.2) where the discriminant $\Delta \geq 0$.

In Appendix I and Appendix II, we give the computational method of finding the fundamental unit and factorizing quadratic algebraic number in the subring of a totally complex quartic field, respectively.

2. Proof of Main Theorem.

THEOREM 1. *All integral points of the elliptic curve* (1.1) *are* $(x, y) = (-4, 0), (-1, \pm 6), (9, \pm 26), (764396, \pm 668309460)$.

PROOF.

$$y^2 = x^3 - 9x + 28 = (x + 4)(x^2 - 4x + 7).$$

Put $z = x + 4$, then we have

$$x^2 - 4x + 7 = (x + 4)^2 - 12(x + 4) + 39 = z^2 - 12z + 39.$$

Let $d = \gcd(z, z^2 - 12z + 39)$, it is easy to obtain $d|39$. Because

$\Delta = -12 < 0$, we get

$$\begin{cases} z = du^2 \\ z^2 - 12z + 39 = dv^2 \end{cases}, \tag{2.1}$$

where $d = 1, 3, 13, 39, \quad \gcd(u, v) = 1$.

When $d = 1,\ (z-6)^2 + 3 = v^2,\ [v - (u^2 - 6)][v + (u^2 - 6)] = 3,$ it is easy to show that there is no solution in rational integer u, v. So equation (2.1) is equivalent to the following three equations

$$\begin{cases} z = 3u^2 \\ z^2 - 12z + 39 = 3v^2 \end{cases}, \tag{2.2}$$

$$\begin{cases} z = 13u^2 \\ z^2 - 12z + 39 = 13v^2 \end{cases} \tag{2.3}$$

and

$$\begin{cases} z = 39u^2 \\ z^2 - 12z + 39 = 39v^2 \end{cases}. \tag{2.4}$$

In the following, we will discuss the three cases, separately.

CASE 1: We solve equation (2.2). Reducing mod4 to (2.2), we can get that v is even and u is odd. Put $v = 2v_0$, hence we can write (2.2) as

$$\begin{cases} z = 3u^2 \\ z^2 - 12z + 39 = 3(2v_0)^2 \end{cases}.$$

Thus we have

$$(3u^2 - 6)^2 + 3 = 3(2v_0)^2.$$

We use **algebraic number theory method** to factor the equation above(see [6][7][8][9]). In the quadratic algebraic field $\mathbf{Q}(\sqrt{-3})$, we have

$$\left[(3u^2 - 6) + \sqrt{-3}\right]\left[(3u^2 - 6) - \sqrt{-3}\right] = -(\sqrt{-3})^2(2AA')^2,$$

where A, A' are two algebraic integers in the quadratic algebraic field $\mathbf{Q}(\sqrt{-3})$ and $v_0 = AA'$. The class number of $\mathbf{Q}(\sqrt{-3})$ is one and we get

$$(3u^2 - 6) \pm \sqrt{-3} = \pm\sqrt{-3}w^n(2A^2), \tag{2.5}$$

where $w = \dfrac{-1+\sqrt{-3}}{2}$ is a root of unity in $\mathbf{Q}(\sqrt{-3})$ and $w^3 = 1, n = 0, 1$ or 2.

From (2.5), we obtain

$$(3u)^2 \pm 6\sqrt{-3}w^n A^2 = 18 \pm 3\sqrt{-3},$$

$$(3u)^2 \pm 2\sqrt{-3}w^n(\sqrt{-3}A)^2 = 18 \pm 3\sqrt{-3}.$$

Put $A_1 = \sqrt{-3}A$, then we have

$$(3u)^2 - 2\sqrt{-3}w^n A_1^2 = 18 \pm 3\sqrt{-3}, \tag{2.6}$$

or

$$(3u)^2 + 2\sqrt{-3}w^n A_1^2 = 18 \pm 3\sqrt{-3}. \tag{2.7}$$

CASE 1.1: First, we solve equation (2.6). We write equation (2.6) as

$$(3u)^2 - 2\sqrt{-3}A_2^2 = 18 \pm 3\sqrt{-3} = 15 - 6w \text{ or } 21 + 6w, \tag{2.8}$$

where $A_2^2 = A_1^2 w^n$, $\sqrt{-3} = 2w + 1$.

Put $\theta = \sqrt{2\sqrt{-3}}$, θ is an algebraic integer in a totally complex quartic field and satisfies $\theta^2 = 2\sqrt{-3} = 2 + 4w$. Define the subring $R = = \mathbf{Z}[1, \theta, w, \theta w]$.

For simplicity, we denote $\alpha = a + b\theta + cw + d\theta w$ as $\alpha = (a, b, c, d)$ and denote the conjugates of α as the following:

$$\alpha_- = a - b\theta + cw - d\theta w = (a, -b, c, -d),$$

$$\alpha' = a + b\theta' + cw^2 + d\theta' w^2, \quad \alpha'_- = a - b\theta' + cw^2 - d\theta' w^2,$$

where $\theta' = \sqrt{-2\sqrt{-3}}$ is the complex conjugate of θ. And we denote the coefficients of α as $a = (\alpha)_0, b = (\alpha)_1, c = (\alpha)_2, d = (\alpha)_3$. Denote by $|z|$ the complex absolute value of the complex number z and denote $\|\alpha\| = \max(|\alpha|, |\alpha_-|, |\alpha'|, |\alpha'_-|)$ as the greatest absolute value of $\alpha, \alpha_-, \alpha'$ and α'_-.

Because θ is an algebraic number in a totally complex quartic field, according to Dirichlet's unit theorem, there is only one independent fundamental unit in $\mathbf{Q}(\theta)$. By direct computation, the fundamental unit in R (Appendix I) is

$$\varepsilon = 1 + 2\theta + 4w + 2\theta w.$$

From (2.8), we get

$$(3u + \theta A_2)(3u - \theta A_2) = 15 - 6w \text{ or } 21 + 6w.$$

Thus we have

$$3u + \theta A_2 = \pm \alpha \varepsilon^k w^t, \quad u, k, t \in \mathbf{Z}, t = 0, 1, 2. \tag{2.9}$$

If algebraic number ξ in the field $\mathbf{Q}(\theta)$ has $\xi = \alpha\alpha' = \beta\beta'$ and $\beta = \alpha\varepsilon$, where ε is the unit in the field $\mathbf{Q}(\theta)$, we call α and β as relevant factors. Otherwise, we call α, α', β and β' as irrelevant factors. By computation (Appendix II), the irrelevant factors of $15 - 6w$ and $21 + 6w$ are:

$$\alpha_1 = (3, 2, 0, 1), \qquad \alpha_{1-} = (3, -2, 0, -1),$$

$$\alpha_2 = (9, 4, 6, -1), \qquad \alpha_{2-} = (9, -4, 6, -1).$$

Now we use **p-adic analysis method** [10] to solve (2.9). From (2.9), we get

$$3u - \boldsymbol{\theta} A_2 = \pm \boldsymbol{\alpha}_- \boldsymbol{\varepsilon}_-^k w^t, \quad u, k, t \in \mathbf{Z}, t = 0, 1, 2. \tag{2.10}$$

(2.9) $\times$ (2.10), since $\varepsilon\varepsilon_- = 1$, $(3u)^2 - \theta^2 A_2^2 = (\alpha_2\alpha_{2-})(\varepsilon\varepsilon_-)^k \omega^{2t}$, we get $t = 0$.

Because $A_2 \in \mathbf{Q}(\sqrt{-3})$, we put $A_2 = b + dw, \quad b, d \in \mathbf{Z}$, then we have

$$(3u + \theta A_2)_2 = (\pm \alpha \varepsilon^k)_2 = 0.$$

It is the main reason that we take p-adic analysis to solve equations (2.6). To take p-adic analysis, we need to find the prime p from the prime factors of $\gcd((\varepsilon^k)_1, (\varepsilon^k)_2, (\varepsilon^k)_3)$. Here we choose $p = 109$ to take p-adic analysis.

If $\alpha = \alpha_2$ or α_{2-},

$$\varepsilon\varepsilon_- = 1, \quad (3u)^2 - \theta^2 A_2^2 = (\alpha_2\alpha_{2-})(\varepsilon\varepsilon_-)^k = \alpha_2\alpha_{2-} = -(21 + 6w),$$

it leads to contradiction, so $\alpha = \alpha_1$ or α_{1-}.

By direct computation,

$$\varepsilon^6 = (-40223, -45604, -89232, -35828) \equiv -1 (\mathrm{mod}\, 13),$$

$$(\alpha_1\varepsilon)_2 \equiv -1 (\mathrm{mod}\, 13), \quad (\alpha_1\varepsilon^2)_2 \equiv -1 (\mathrm{mod}\, 13), \quad (\alpha_1\varepsilon^3)_2 \equiv -6 (\mathrm{mod}\, 13),$$

$$(\alpha_1\varepsilon^4)_2 \equiv 4 (\mathrm{mod}\, 13), \qquad (\alpha_1\varepsilon^5)_2 \equiv 1 (\mathrm{mod}\, 13).$$

So we assume $k = 6m$, write $k = 108n + s, 0 \le s \le 107$, where actually $s = 0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102$.

By direct computation, we know that only $s = 0$ meets

$$(\alpha_1\varepsilon^s)_2 \equiv 0 (\mathrm{mod}\, 109).$$

In the following, we will prove equation (1.1) has the solutions $(x, y) = = (-1, \pm 6)$ when $s = 0$.

Put $109^r \| n$. Because

$$\varepsilon^{108} \equiv (1, 9374, 0, 8720) (\mathrm{mod}\, 11881 = 109^2),$$

denote

$$\varepsilon^{108} = 1 + 109(0, 86, 0, 80) + 109^2\eta.$$

$$\alpha_1\varepsilon^{108n} = \alpha_1(1+109((0,86,0,80)+109\eta))^n = \alpha_1(1+109n((0,86,0,80)+109\eta)+\cdots),$$

$$0 \equiv (\alpha_1\varepsilon^{108n})_2 \equiv (\alpha_1)_2 + 109n(\alpha_1(0,86,0,80))_2 (\mathrm{mod}\, 109^{r+2}),$$

$$\alpha_1(0,86,0,80) = (-480, 258, 36, 240), \quad 109 \nmid 36,$$

we get $n = 0, u = \pm 1, (x, y) = (-1, \pm 6)$. Similarly, we deal with $\alpha = \alpha_{1-}$ and get $(x, y) = (-1, \pm 6)$.

Case 1.2: Second, we solve equation (2.7). Let $\theta = \sqrt{-2\sqrt{-3}}$, $w = \dfrac{-1+\sqrt{-3}}{2}$, $R = \mathbf{Z}[1, \theta, w, \theta w]$, we have $\theta^2 = -2 - 4w$. We use the similar method above and get

$$3u + \theta A_2 = \pm\alpha\varepsilon^k w^t, \quad u, k, t \in \mathbf{Z}.$$

By computation, the fundamental unit in R is

$$\varepsilon = (3, 0, 4, 2),$$

the irrelevant factors of $15 - 6w$ and $21 + 6w$ in R are:

$$\alpha_1 = (3, 1, 0, -1), \qquad \alpha_{1-} = (3, -1, 0, 1);$$

$$\alpha_2 = (3, 1, 6, -1), \qquad \alpha_{2-} = (3, -1, 6, 1);$$

$$\alpha_3 = (3, 5, -6, 1), \qquad \alpha_{3-} = (3, -5, -6, -1);$$

$$\alpha_4 = (3, 7, -12, -1), \qquad \alpha_{4-} = (3, -7, -12, 1).$$

We can get $t = 0$ by the same method with Case1.1. Because $\varepsilon\varepsilon_- = 1, \alpha_2\alpha_{2-} = -(15 - 6w), \alpha_3\alpha_{3-} = -(15 - 6w)$, it results in contradiction, then $\alpha = \alpha_1, \alpha_{1-}, \alpha_4$ or α_{4-}.

If $\alpha = \alpha_1$,

$$\varepsilon^6 = (49009, -9776, 89232, 35828) \equiv -1 (\mathrm{mod}\, 13),$$

$$(\alpha_1\varepsilon)_2 \equiv -1 (\mathrm{mod}\, 13), \ (\alpha_1\varepsilon^2)_2 \equiv -1 (\mathrm{mod}\, 13), \ (\alpha_1\varepsilon^3)_2 \equiv -6 (\mathrm{mod}\, 13),$$

$$(\alpha_1\varepsilon^4)_2 \equiv -4 (\mathrm{mod}\, 13), \quad (\alpha_1\varepsilon^5)_2 \equiv 1 (\mathrm{mod}\, 13).$$

So we assume $k = 6m$, write $k = 108n + s, 0 \le s \le 107$, where actually $s = 0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 78, 84, 90, 96, 102$. By direct computation, we know that only $s = 0$ meets

$$(\alpha_1 \varepsilon^s)_2 \equiv 0 (\mathrm{mod}\, 109).$$

Put $109^r \| n$. Because

$$\varepsilon^{108} \equiv (1, 654, 0, 3161) (\mathrm{mod}\, 11881 = 109^2),$$

denote

$$\varepsilon^{108} = 1 + 109(0, 6, 0, 29) + 109^2 \eta.$$

$$\alpha_1 \varepsilon^{108n} = \alpha_1 (1 + 109((0, 6, 0, 29) + 109\eta))^n = \alpha_1 (1 + 109n((0, 6, 0, 29) + 109\eta) + \cdots),$$

$$0 \equiv (\alpha_1 \varepsilon^{108n})_2 \equiv (\alpha_1)_2 + 109n(\alpha_1 (0, 6, 0, 29))_2 (\mathrm{mod}\, 109^{r+2}),$$

$$\alpha_1 (0, 6, 0, 29) = (138, 18, -36, 87), \quad 109 \nmid 36,$$

we get $n = 0, u = \pm 1, (x, y) = (-1, \pm 6)$. Similarly, we deal with $\alpha = \alpha_{1-}$ and get $(x, y) = (-1, \pm 6)$. Similarly, we deal with $\alpha = \alpha_{1-}, \alpha_4$ and α_{4-}, so we get $(x, y) = (-1, \pm 6)$.

CASE 2: We solve equation (2.3). By taking modula 8, we can get that v is even and u is odd. It can be written as

$$[(13u^2 - 6) + \sqrt{-3}][(13u^2 - 6) - \sqrt{-3}] = (-1 + 2\sqrt{-3})(-1 - 2\sqrt{-3})(2AA')^2.$$

We have

$$(13u^2 - 6) \pm \sqrt{-3} = \pm 2(-1 + 2\sqrt{-3}) w^n A^2,$$

where $w = \dfrac{-1 + \sqrt{-3}}{2}$ is a root of unity in $\mathbf{Q}(\sqrt{-3})$ and $w^3 = 1$, $n = 0, 1$ or $2, u \in \mathbf{Z}, A, A'$ are two algebraic integer in $\mathbf{Z}[w]$ and $v = 2AA'$. Let $A_1 = (-1 + 2\sqrt{-3})A$, we can get

$$(13u)^2 - 2(-1 - 2\sqrt{-3}) w^n A_1^2 = 78 \pm 13\sqrt{-3} = 65 - 26w \text{ or } 91 + 26w, \tag{2.11}$$

or

$$(13u)^2 + 2(-1 - 2\sqrt{-3}) w^n A_1^2 = 78 \pm 13\sqrt{-3} = 65 - 26w \text{ or } 91 + 26w. \tag{2.12}$$

CASE 2.1: First, we solve equation (2.11). Let $A_2^2 = w^n A_1^2, \theta = \sqrt{-2 - 4\sqrt{-3}}$, then $\theta^2 = -6 - 8w$. θ is an algebraic integer in a totally complex quartic field. We define a subring $R = \mathbf{Z}[1, \theta, w, \theta w]$.

From (2.11), we get

$$13u + \theta A_2 = \pm\alpha\varepsilon^k w^t, \quad u,k,t \in \mathbf{Z},\ t = 0,1,2. \tag{2.13}$$

By computation, the fundamental unit in R is

$$\varepsilon = (11,3,4,4),$$

the irrelevant factors of $65 - 26w$ and $91 + 26w$ in R are:

$$\begin{aligned}
\alpha_1 &= (13,4,0,3), & \alpha_{1-} &= (13,-4,0,-3);\\
\alpha_2 &= (1,4,10,1), & \alpha_{2-} &= (1,-4,10,-1);\\
\alpha_3 &= (3,1,4,-3), & \alpha_{3-} &= (3,-1,4,-3);\\
\alpha_4 &= (1,3,10,1), & \alpha_{4-} &= (1,-3,10,-1);\\
\alpha_5 &= (17,3,14,7), & \alpha_{4-} &= (17,-3,14,-7).
\end{aligned}$$

We can get $u = \pm 1, (x,y) = (9,\pm 26)$ by p-adic analysis method similar to Case 1.

CASE 2.2: Second, we solve equation (2.12). Let $A_2^2 = w^t A_1^2, \theta = = \sqrt{2+4\sqrt{-3}}$, then $\theta^2 = 6 + 8w$. θ is an algebraic integer in a totally complex quartic field. We define a ring $R = \mathbf{Z}[1,\theta,w,\theta w]$.

From (2.12), we get

$$13u + \theta A_2 = \pm\alpha\varepsilon^k w^t, \quad u,k,t \in \mathbf{Z},\ t = 0,1,2. \tag{2.14}$$

By computation, the fundamental unit in R is

$$\varepsilon = (3,1,2,0),$$

but there are no irrelevant factors of $65 - 26w$ and $91 + 26w$ in R, so there is no solution.

CASE 3: We solve equation (2.4). It can be written as

$$[(39u^2-6)+\sqrt{-3}][(39u^2-6)-\sqrt{-3}] = (-6+\sqrt{-3})(-6-\sqrt{-3})(AA')^2.$$

We have

$$(39u^2-6) \pm \sqrt{-3} = \pm(-6+\sqrt{-3})w^n A^2,$$

where $w = \dfrac{-1+\sqrt{-3}}{2}$ is a root of unity in $\mathbf{Q}(\sqrt{-3})$ and $w^3 = 1$, $n = 0,1$ or $2, u \in \mathbf{Z}, A, A'$ are two algebraic integers in $\mathbf{Z}[w]$ and $v = AA'$.

Let $A_1 = (-6+\sqrt{-3})A$, we get

$$(39u)^2-(-6-\sqrt{-3})w^nA_1^2 = 234 \pm 39\sqrt{-3} = 195-78w \text{ or } 273+78w, \tag{2.15}$$

or

$$(39u)^2+(-6-\sqrt{-3})w^nA_1^2 = 234 \pm 39\sqrt{-3} = 195-78w \text{ or } 273+78w. \tag{2.16}$$

CASE 3.1: First, we solve (2.15). Let $A_2^2 = w^nA_1^2$, $\theta = \sqrt{-6-\sqrt{-3}}$, then $\theta^2 = -7-2w$. θ is an algebraic integer in a totally complex quartic field. We define a subring $R = \mathbf{Z}[1, \theta, w, \theta w]$.

From (2.15), we get

$$39u + \theta A_2 = \pm\alpha\varepsilon^k w^t, \quad u, k, t \in \mathbf{Z}. \tag{2.17}$$

By computation, the fundamental unit in R is

$$\varepsilon = (2, 1, -1, 1),$$

the irrelevant factors of $195-78w$ and $273+78w$ in R are:

$$\alpha_1 = (0, 5, 0, -2), \quad \alpha_{1-} = (0, -5, 0, 2);$$
$$\alpha_2 = (6, 7, 24, 2), \quad \alpha_{2-} = (6, -7, 24, -2);$$
$$\alpha_3 = (9, 4, -3, -1), \quad \alpha_{3-} = (9, -4, -3, 1).$$

We can get $u = 0, 140$, so $(x, y) = (-4, 0), (764396, \pm 668309460)$ by p-adic analysis method similar to Case 1.

CASE 3.2: Second, we solve equation (2.16). Let $A_2^2 = w^tA_1^2, \theta = \sqrt{6+\sqrt{-3}}$, then $\theta^2 = 7+2w$. θ is an algebraic integer in a totally complex quatic field. We can define a ring $R = \mathbf{Z}[1, \theta, w, \theta w]$.

We get

$$39u + \theta A_2 = \pm\alpha\varepsilon^k w^t, \quad u, k, t \in \mathbf{Z}, t = 0, 1, 2.$$

By computation, we know that the fundamental unit in R is

$$\varepsilon = (5, 2, 3, 1),$$

the irrelevant factors of $195-78w$ and $273+78w$ in R are:

$$\alpha_1 = (0, 5, 0, -2), \quad \alpha_{1-} = (0, -5, 0, 2);$$
$$\alpha_2 = (6, 1, 24, 8), \quad \alpha_{2-} = (6, -1, 24, -8);$$
$$\alpha_3 = (12, 5, 9, 7), \quad \alpha_{3-} = (12, -5, 9, -7).$$

We can get there is no solution by p-adic analysis.

Theorem 1 has been proved.

3. Method Discussion.

By using algebraic number theory and p-adic analysis method, we can find all integral points on certain elliptic curves

$$y^2 = (x+a)(x^2+bx+c), \quad a,b,c \in \mathbf{Z},$$

where the discriminant of x^2+bx+c, denote as Δ, satisfies $\Delta = b^2-4c < 0$. Furthermore, we can solve all integer solutions of certain hyperelliptic equations

$$Dy^2 = Ax^4+Bx^2+C, \quad B^2 < 4AC.$$

Now we give the complete solution of equation (1.2). Put $z = x+a$, from (1.2), we get

$$x^2+bx+c = z^2+(b-2a)z+(a^2-ab+c),$$

$$\begin{cases} z = du^2 \\ z^2+(b-2a)z+(a^2-ab+c) = dv^2 \end{cases}, \tag{3.1}$$

where $d = \gcd(z, z^2+(b-2a)x+(a^2-ab+c))$, so $d|(a^2-ab+c)$. Actually, when d has a square factor, we can extract it to u and v. For some cases of d, we can solve the equations by elementary method. Next we use algebraic number theory method and p-adic analysis method to solve all integral points on certain elliptic curves (1.2).

From (3.1), we have

$$d^2u^4+(b-2a)du^2+(a^2-ab+c) = dv^2.$$

It can be written as the form of equation (1.3)

$$Dy^2 = Ax^4+Bx^2+C, \quad B^2 < 4AC,$$

where $u = x, v = y, A = d^2, B = (b-2a)d, C = a^2-ab+c, D = d$.

Equation (1.3) can be written as

$$D_1y^2 = x_1^4+B_1x_1^2+C_1, \tag{3.2}$$

where $D_1 = A^3D, B_1 = AB, C_1 = A^3C, x_1 = Ax$ and $B_1^2 < 4C_1$. So we have

$$4D_1y^2 = (2x_1^2+B_1)^2+(4C_1-B_1^2).$$

Let $f = 4C_1-B_1^2 = lg^2 > 0$ (l is square-free positive integer), we have

$$4D_1y^2 = (2x_1^2+B_1)^2+lg^2. \tag{3.3}$$

We factorize equation (3.3) in complex quadratic field $\mathbf{Q}(\sqrt{-g})$ to get

$$(2x_1^2 + B_1 + l\sqrt{-g}) = (KLM^2), \tag{3.4}$$

where K is the common divisor of ideals $(2x_1^2 + B_1 + l\sqrt{-g})$ and $(2x_1^2 + B_1 - l\sqrt{-g})$, L is the ideal factorization of $4D_1$ and $N(L) = 4D_1$.

We suppose the ideal classes in $\mathbf{Q}(\sqrt{-g})$ are $I_1, I_2, \cdots, I_h$ and their representatives are $J_1, J_2, \cdots, J_h$. There is no loss of generality by assuming that $KL \sim I_1^{-1}, M \sim I_2^{-1}$. From (3.4), we have

$$J_1 J_2^2 (2x_1^2 + B_1 + l\sqrt{-g}) = J_1 KL (J_2 M)^2. \tag{3.5}$$

Since $J_1 KL$ and $J_2 M$ are principle ideals, $J_1 J_2^2$ is a principle ideal. Let $J_1 KL = S_1, J_2 M = S_2, J_1 J_2^2 = S_3$, we have

$$S_3(2x_1^2 + B_1 + l\sqrt{-g}) = S_1 S_2^2. \tag{3.6}$$

Suppose the conjugation of S_3 is S_3', and $S_3 S_3' = a$. From (3.6), we get

$$2ax_1^2 + B_2 = S' S_2^2, \tag{3.7}$$

where $B_2 = a(B_1 + l\sqrt{-g}), S' = S_1 S_3' \in \mathbf{Q}(\sqrt{-g})$ is an algebraic number in $\mathbf{Q}(\sqrt{-g})$. From (3.7), we obtain

$$2ax_1^2 - S' S_2^2 = -B_2,$$

$$(2ax_1)^2 - 2aS' S_2^2 = -2aB_2. \tag{3.8}$$

REMARK 1. As long as $2aS'$ in (3.8) has a square factor $\beta \in \mathbf{Q}(\sqrt{-g})$, we put $\theta^2 = \dfrac{2aS'}{\beta^2}, S_2' = \beta S_2$. Define the subring $R = \mathbf{Z}[1, \theta, w, \theta w]$. θ is an algebraic integer in a totally complex quartic field. We choose the basis $1, \theta, w, \theta w$ in order that $\|\theta\|$ and $\|\varepsilon\|$ in the subring R is by far least and p which we choose to take p-adic analysis is the smallest possible.

From (3.8), we have

$$2ax_1 + \theta S_2' = \pm w^t \varepsilon^k \alpha, \tag{3.9}$$

where w is a root of unity, ε is a fundamental unit in the subring R, α is an irrelevant factor of $-2aB_2$ in $\mathbf{Q}(\theta)$(the irrelevant factors α of $-2aB_2$ are finite).

Since $S_2 \in \mathbf{Q}(\sqrt{-g})$, we put $S_2' = b + d\theta^2,\ b, d \in \mathbf{Z}$. From (3.9), we get

$$2ax_1 + b\theta + d\theta^3 = \pm w^t \varepsilon^k \alpha. \tag{3.10}$$

From (3.10), we have

$$2ax_1 - b\theta - d\theta^3 = \pm w^t \varepsilon_-^k \alpha_-. \tag{3.11}$$

(3.10) $\times$ (3.11), we get $t = 0$. The coefficient of θ^2 is 0 in the left of (3.10), so

$$(2ax_1 + b\theta + d\theta^3)_2 = (\pm\varepsilon^k\alpha)_2 = 0. \tag{3.12}$$

From equation (3.12), we know there must be another equation corresponding to the unknown k. Finally we solve it directly by p-adic analysis method.

In [11][12], Ljunggren and Tzanakis proved that solving equation (1.3) is equivalent to solve the integer solutions of a class of quartic Thue equation

$$p(x, y) = Ax^4 + Bx^3y + Cx^2y^2 + Dxy^3 + Ey^4 = \pm m,$$

where $p(x, 1) = 0$ has two real roots and a couple of complex roots. Suppose θ is a root of $p(x, 1) = 0$, then by Dirichlet's unit theorem there are two independent fundamental units $\varepsilon_1, \varepsilon_2$ in $Q(\theta)$. It is complicate to compute them. In [6], Ljunggren's method need compute a relative unit in a quartic field. Obviously, their methods are not easy.

REMARK 2. It is necessary to point out that the method works theoretically. Our computations involved can be carried out successfully but in very exceptional cases. The first point is that there is no control on the size and the computation time of the fundamental unit ε, even though we find a proper θ in order that $R = \mathbf{Z}[1, \theta, w, \theta w]$ is a domain. The second point, is that computing a set of representative of ideal class group of an imaginary field can take a lot of time. That is to say, we can not multiply the examples at will. But in fact, many equations can be solved by this method. We compute all integral points on another elliptic curve which Don.Zagier proposed

$$y^2 = x^3 - 30x + 133 \tag{3.13}$$

are: (x, y)=$(-7, 0), (-3, \pm 4), (2, \pm 9), (6, \pm 13), (5143326, \pm 116644498677)$. Many famous problems are the examples of equation (3.2), for example[13][2][14]:

$$\left(\frac{x(x-1)}{2}\right)^2 = \frac{y(y-1)}{2}, \tag{3.14}$$

$$6y^2 = x^3 + 5x + 6 = (x + 1)(x^2 - x + 6), \tag{3.15}$$

$$31y^2 = x^3 - 1, \tag{3.16}$$

$$y^2 = (x + 337)(x^2 + 337^2). \tag{3.17}$$

4. Other Cases' Discussion.

When the discriminant $\Delta = b^2 - 4c = 0$ in equation (1.2), we have $c = \frac{b^2}{4}$, then b is even and c is a square number. Let $b = 2l,\ l \in \mathbf{Z}$, then $c = l^2$, so

$$y^2 = (x + a)(x^2 + 2lx + l^2) = (x + a)(x + l)^2. \tag{4.1}$$

So $x + a$ is a square number. Put $x + a = m^2, m \in \mathbf{Z}$, then we get

$$y^2 = m^2(x + l)^2. \tag{4.2}$$

Thus we get the solution

$$\begin{cases} x = m^2 - a^2 \\ y = \pm m(m^2 - a + l) \end{cases}. \tag{4.3}$$

When the discriminant $\Delta = b^2 - 4c > 0$ in equation (1.2), we have $c < \frac{b^2}{4}$, then $x^2 + bx + c = 0$ has two different real roots x_1 and x_2. Especially when $\Delta = b^2 - 4c = n^2,\ \ n \in \mathbf{N}$, we have $x_1 = \frac{-b - n}{2}$ and $x_2 = \frac{-b + n}{2}$. Hence equation (1.2) can be written as

$$y^2 = (x + a)\Big(x - \frac{-b - n}{2}\Big)\Big(x - \frac{-b + n}{2}\Big). \tag{4.4}$$

We can refer to Pell Equation's method in Zagier [5]. When $\Delta = b^2 - 4c$ is not a square number, we refer to linear forms in the logarithms of algebraic number[1] and elliptic logarithm method [2].

Appendix I

Find a fundamental unit in $R = \mathbf{Z}[1, \theta, w, \theta w]$, where $\theta = \sqrt[4]{-12}, w = \frac{-1 + \sqrt{-3}}{2}$.

If $\varepsilon = a + b\theta + cw + d\theta w$ is a fundamental unit in R, where $a, b, c, d \in \mathbf{Z}$, then $\varepsilon_- = a - b\theta + cw - d\theta w$ is a conjugate of ε. So we have

$$\varepsilon\varepsilon_- = (a + b\theta + cw + d\theta w)(a - b\theta + cw - d\theta w)$$

$$= (a^2 - 2b^2 + 8bd - c^2 - 2d^2) + (2ac - 4b^2 + 4bd - c^2 + 2d^2)w = F + Gw.$$

$$N(\varepsilon) = N(\varepsilon_-) = N(F + Gw) = (F + Gw)(F + Gw^2) = F^2 - FG + G^2 = \pm 1.$$

Thus we get

$$FG \pm 1 = F^2 + G^2 \geq 2|FG|.$$

From $FG > 0, FG = 0, FG < 0,$ we obtain $(F, G) = (\pm 1, \pm 1),\ (\pm 1, 0),$ $(0, \pm 1)$, where

$$(*) \qquad \begin{cases} F = a^2 - 2b^2 + 8bd - c^2 - 2d^2 \\ G = 2ac - 4b^2 + 4bd - c^2 + 2d^2 \end{cases}.$$

There is no loss of generation of assuming $c \neq 0$, otherwise $c = 0$ is the easier condition. From

$$G = 2ac - 4b^2 + 4bd - c^2 + 2d^2,$$

we have $a = \dfrac{c^2 + W}{2c}$, where $W = 4b^2 - 4bd - 2d^2 + G$. Then we obtain

$$\Big(\frac{c^2 + W}{2c}\Big)^2 - 2b^2 + 8bd - c^2 - 2d^2 = F.$$

Thus we have

$$3c^4 + c^2(8b^2 - 32bd + 8d^2 - 2W + 4F) - W^2 = 0.$$

We regard this equation as a quadratic equation with one unknown $c_1 = c^2$, then

$$c_1 = c^2 = \frac{-B \pm \sqrt{B^2 + 12W^2}}{6},\ \text{where } B = 8b^2 - 32bd + 8d^2 - 2W + 4F.$$

We limit the ranges of b and d to find the integers a, b, c, d which meet $(*)$. We suppose $|b| \leq 5, |d| \leq 5$, then in the ranges we search $c_1 = c^2$. If there exist two integers b_0 and d_0 to get $c_1 = c_0^2, c_0 \in \mathbf{Z}$, we can compute a_0 from $a = \dfrac{c^2 + W}{2c}$. If a_0 is an integer, we have already found a unit in R. If we can not find a, b, c, d in the ranges, we should extend the ranges of b and d till we find a unit $\varepsilon_0 = a_0 + b_0\theta + c_0 w + d_0\theta w$.

Now we will compute the fundamental unit $\varepsilon = a + b\theta + cw + d\theta w$ from $\varepsilon_0 = a_0 + b_0\theta + c_0 w + d_0\theta w$, where $a, b, c, d \in \mathbf{Z}$. If $\|\varepsilon_0\|$ is not the least, we have $\varepsilon_0 = \pm\varepsilon^t, |t| \geq 2$.

Denote

$$\begin{pmatrix} \varepsilon \\ \varepsilon_- \\ \varepsilon' \\ \varepsilon'_- \end{pmatrix} = \begin{pmatrix} 1 & \theta & w & \theta w \\ 1 & -\theta & w & -\theta w \\ 1 & \theta' & w^2 & \theta' w^2 \\ 1 & -\theta' & w^2 & -\theta' w^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \triangleq M \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

then

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = M^{-1} \begin{pmatrix} \varepsilon \\ \varepsilon_- \\ \varepsilon' \\ \varepsilon'_- \end{pmatrix}.$$

From $M^{-1} = \dfrac{1}{4w+2} \begin{pmatrix} 1+w & 1+w & w & w \\ \dfrac{1+w}{\theta} & -\dfrac{1+w}{\theta} & \dfrac{w}{\theta'} & -\dfrac{w}{\theta'} \\ 1 & 1 & -1 & -1 \\ \dfrac{1}{\theta} & -\dfrac{1}{\theta} & -\dfrac{1}{\theta'} & \dfrac{1}{\theta'} \end{pmatrix}$, we obtain

$$\begin{cases} a = \dfrac{1}{4w+2}[(1+w)\varepsilon + (1+w)\varepsilon_- + w\varepsilon' + w\varepsilon'_-] \\ b = \dfrac{1}{4w+2}\Big[\dfrac{1+w}{\theta}\varepsilon + \Big(-\dfrac{1+w}{\theta}\Big)\varepsilon_- + \dfrac{w}{\theta'}\varepsilon' + \Big(-\dfrac{w}{\theta'}\Big)\varepsilon'_-\Big] \\ c = \dfrac{1}{4w+2}(\varepsilon + \varepsilon_- - \varepsilon' - \varepsilon'_-) \\ d = \dfrac{1}{4w+2}\Big(\dfrac{\varepsilon}{\theta} - \dfrac{\varepsilon_-}{\theta} - \dfrac{\varepsilon'}{\theta'} + \dfrac{\varepsilon'_-}{\theta'}\Big) \end{cases}.$$

From $\begin{cases} \varepsilon_0 = \pm\varepsilon^t \\ \varepsilon_{0-} = \pm\varepsilon_-^t \\ \varepsilon'_0 = \pm\varepsilon'^t \\ \varepsilon'_{0-} = \pm\varepsilon'^t_- \end{cases}$ (where $|t| \geq 2$), we get $\begin{cases} \varepsilon = \pm\varepsilon_0^{1/t} \\ \varepsilon_- = \pm\varepsilon_{0-}^{1/t} \\ \varepsilon' = \pm\varepsilon_0'^{1/t} \\ \varepsilon'_- = \pm\varepsilon_{0-}'^{1/t} \end{cases}$, thus we obtain

$$\begin{aligned} |a| &\leq \Big|\frac{1}{4w+2}\Big|(|1+w\|\varepsilon| + |1+w\|\varepsilon_-| + |w\|\varepsilon'| + |w\|\varepsilon'_-|) \\ &= \Big|\frac{1}{4w+2}\Big|(|1+w\|\varepsilon_0|^{1/t} + |1+w\|\varepsilon_{0-}|^{1/t} + |w\|\varepsilon'_0|^{1/t} + |w\|\varepsilon'_{0-}|^{1/t}) \\ &\leq 4\Big|\frac{1}{4w+2}\Big|\,\|\varepsilon_0\|^{1/2}, \end{aligned}$$

$$|b| \le \Big|\frac{1}{4w+2}\Big|\Big(\Big|\frac{1+w}{\theta_0}\Big||\varepsilon| + \Big|\frac{1+w}{\theta_0}\Big||\varepsilon_-| + \Big|\frac{w}{\theta_0'}\Big||\varepsilon'| + \Big|\frac{w}{\theta_0'}\Big||\varepsilon_-'|\Big)$$

$$= \Big|\frac{1}{4w+2}\Big|\Big(\Big|\frac{1+w}{\theta_0}\Big||\varepsilon_0|^{1/t} + \Big|\frac{1+w}{\theta_0}\Big||\varepsilon_{0-}|^{1/t} + \Big|\frac{w}{\theta_0'}\Big||\varepsilon_0'|^{1/t} + \Big|\frac{w}{\theta_0'}\Big||\varepsilon_{0-}'|^{1/t}\Big)$$

$$\le 2\Big|\frac{1}{4w+2}\Big|\Big(\Big|\frac{1}{\theta_0}\Big| + \Big|\frac{1}{\theta_0'}\Big|\Big)\|\varepsilon_0\|^{1/2},$$

$$|c| \le 4\Big|\frac{1}{4w+2}\Big|\|\varepsilon_0\|^{1/2}, \qquad |d| \le 2\Big|\frac{1}{4w+2}\Big|\Big(\Big|\frac{1}{\theta_0}\Big| + \Big|\frac{1}{\theta_0'}\Big|\Big)\|\varepsilon_0\|^{1/2}.$$

If we can not find integers a, b, c, d in the ranges, then $\varepsilon_0 = a_0 + + b_0\theta + c_0 w + d_0\theta w$ is just the fundamental unit.

If we can find integers a_0', b_0', c_0', d_0', then we get a unit $\varepsilon_1 = = a_0' + b_0'\theta + c_0' w + d_0'\theta w$ whose absolute value $\|\varepsilon_1\|$ is smaller than $\|\varepsilon_0\|$. We use the same method for ε_1 till we find the fundamental unit. By computation, the fundamental unit of the subring $R = \mathbf{Z}[1, \theta, w, \theta w]$ is $\varepsilon = 1 + 2\theta + 4w + 2\theta w$.

The method of computation here is more effective than the ones in [15][16].

Appendix II

Factorize the quadratic algebraic number $\xi = 15 - 6w$ and $\xi' = 21 + 6w$ in $R = \mathbf{Z}[1, \theta, w, \theta w]$, where $w = \dfrac{-1+\sqrt{-3}}{2}$, $\theta = \sqrt[4]{-12}$.

Let $\xi = 15 - 6w = 21 + 6w^2 = \pm\alpha\alpha_-$, $\xi' = 21 + 6w = 15 - 6w^2 = \pm\alpha'\alpha_-'$. The factorization is only defined "up to multiplication by units". If there are two factors $\alpha_1 = (a_1, b_1, c_1, d_1)$ and $\alpha_2 = (a_2, b_2, c_2, d_2)$ which meet above condition, and $\dfrac{\alpha_1}{\alpha_2}$ is an algebraic integer and is a unit $\varepsilon = \dfrac{\alpha_1}{\alpha_2} (N(\varepsilon) = \pm 1)$, then they are relevant algebraic numbers. We have

$$N(\xi) = N(\xi') = (15 - 6w)(21 + 6w) = 351 = \alpha\alpha_-\alpha'\alpha_-',$$

and we have an important inequality[10]

$$\|\alpha\| \le |N(\xi)|^{1/4}\sqrt{\|\varepsilon\|},$$

where ε is the fundamental unit in a totally complex quartic field $\mathbf{Q}(\theta)$. In the following, we will give a simple proof for above inequality.

By a logarithmic mapping l, we can establish the relation between ξ and the fundamental unit ε. That is to say, from $n = r_1 + 2r_2 = = 1 \times 0 + 2 \times 2 = 4$, we suppose

$$\eta_1 = l(\varepsilon) = (2\log|\varepsilon|, 2\log|\varepsilon'|), \quad \eta_2 = (2, 2),$$

$$l(\alpha) = (2\log|\alpha|, 2\log|\alpha'|) = x_1\eta_1 + x_2\eta_2 = x_1 l(\varepsilon) + x_2\eta_2,$$

so we have

$$\begin{cases} 2\log|\alpha| = 2x_1\log|\varepsilon| + 2x_2 \\ 2\log|\alpha'| = 2x_1\log|\varepsilon'| + 2x_2 \end{cases},$$

where ε and ε' are ε's conjugates whose absolute values are different, α and α' are α's conjugates whose absolute values are different. Hence we obtain

$$2\log|\alpha| + 2\log|\alpha'| = [2(x_1\log|\varepsilon|) + 2x_2] + [2(x_1\log|\varepsilon'|) + 2x_2] =$$

$$= x_1\log|\varepsilon\varepsilon'|^2 + 4x_2 = 4x_2\,.$$

So we have

$$x_2 = \frac{1}{4}\log|\alpha|^2|\alpha'|^2 = \frac{1}{4}\log|N(\alpha)| = \frac{1}{4}\log|N(\xi)|.$$

Therefore we get

$$|\alpha| = |x_2||\varepsilon^{x_1}| = |N(\xi)|^{1/4}|\varepsilon^{x_1}|.$$

Put $x_1 = m_1 + y_1, |y_1| \le \frac{1}{2}, m_1 \in \mathbf{Z}$. From $\alpha = \tilde{\alpha}\varepsilon^{m_1}$, we have $\tilde{\alpha} = \alpha\varepsilon^{-m_1}$, then

$$|\tilde{\alpha}| \le |N(\xi)|^{1/4}\max\left(\frac{1}{\sqrt{|\varepsilon|}}, \sqrt{|\varepsilon|}\right) = |N(\xi)|^{1/4}\|\varepsilon_0\|,$$

where ε_0 is the fundamental unit in $R = \mathbf{Z}[1, \theta, w, \theta w]$. Because we factorize the quadratic algebraic number ξ in the subring R, the α's that we will find are stable under multiplication by powers of ε and actually we compute a set of representatives $\tilde{\alpha}$ modulo this action.

REMARK 3. If there is a factorization of ξ, then up to changing α by a relevant integer, the important inequality is fulfilled. Of course it is clear the inequality does not work for any algebraic integer "relevant" to α.

If

$$\begin{pmatrix} \alpha \\ \alpha_- \\ \alpha' \\ \alpha'_- \end{pmatrix} = \begin{pmatrix} 1 & \theta & w & \theta w \\ 1 & -\theta & w & -\theta w \\ 1 & \theta' & w^2 & \theta' w^2 \\ 1 & -\theta' & w^2 & -\theta' w^2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = M \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

then

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = M^{-1} \begin{pmatrix} \alpha \\ \alpha_- \\ \alpha' \\ \alpha'_- \end{pmatrix}.$$

We get

$$\begin{cases} a = \dfrac{1}{4w+2}[(1+w)\alpha + (1+w)\alpha_- + w\alpha' + w\alpha'_-] \\ b = \dfrac{1}{4w+2}\Big[\Big(\dfrac{1+w}{\theta}\Big)\alpha + \Big(-\dfrac{1+w}{\theta}\Big)\alpha_- + \dfrac{w}{\theta'}\alpha' + \Big(-\dfrac{w}{\theta'}\Big)\alpha'_-\Big] \\ c = \dfrac{1}{4w+2}(\alpha + \alpha_- - \alpha' - \alpha'_-) \\ d = \dfrac{1}{4w+2}\Big(\dfrac{\alpha}{\theta} - \dfrac{\alpha_-}{\theta} - \dfrac{\alpha'}{\theta'} + \dfrac{\alpha'_-}{\theta'}\Big) \end{cases},$$

$$\begin{cases} |a| \le \Big|\dfrac{1}{2w+1}\Big|\Big(|1+w| + |w|\Big)\|\alpha\| \le \dfrac{2}{\sqrt{3}}\sqrt[4]{351}\sqrt{\|\varepsilon\|} = 13.5294\cdots \\ |b| \le \Big|\dfrac{1}{2w+1}\Big|\Big(\Big|\dfrac{1+w}{\theta}\Big| + \Big|\dfrac{w}{\theta'}\Big|\Big)\|\alpha\| \le \dfrac{2}{\sqrt{3}}\dfrac{\sqrt[4]{351}}{\sqrt[4]{12}}\sqrt{\|\varepsilon\|} = 7.26913\cdots \\ |c| \le \Big|\dfrac{2}{2w+1}\Big|\|\alpha\| \le \dfrac{2}{\sqrt{3}}\sqrt[4]{351}\sqrt{\|\varepsilon\|} = 13.5294\cdots \\ |d| \le \Big|\dfrac{1}{2w+1}\Big|\Big(\Big|\dfrac{1}{\theta}\Big| + \Big|\dfrac{1}{\theta'}\Big|\Big)\|\alpha\| \le \dfrac{1}{\sqrt{3}}\dfrac{2}{\sqrt[4]{12}}\sqrt[4]{351}\sqrt{\|\varepsilon\|} = 7.26913\cdots \end{cases}.$$

In the range of

$$|a| \le 13, |b| \le 7, |c| \le 13, |d| \le 7,$$

there are some $a, b, c, d \in \mathbf{Z}$ satisfying

$$\pm\xi = \pm(15 - 6w) = \alpha\alpha_- = (a + b\theta + cw + d\theta w)(a - b\theta + cw - d\theta w)$$

$$= (a+cw)^2 - \theta^2(b+dw)^2 = (a^2+2acw+c^2w^2) - (4w+2)(b^2+2bdw+d^2w^2)$$
$$= (a^2 - 2b^2 + 8bd - c^2 - 2d^2) + (2ac - 4b^2 + 4bd - c^2 + 2d^2)w = F + Gw.$$

If there are two factors $\alpha_1 = (a_1, b_1, c_1, d_1)$ and $\alpha_2 = (a_2, b_2, c_2, d_2)$ which meet above condition, and $\dfrac{\alpha_1}{\alpha_2}$ is an algebraic integer and is a unit. We should filter one of them(for example α_2) and remain another(for example α_1). We do the procedure till all remained factors α of ξ are irrelevant.

By computation, we get the irrelevant factors of $\xi = 15 - 6w$ and $\xi' = 21 + 6w$ factoring in the subring R are:

$$\alpha_1 = (3, 2, 0, 1), \quad \alpha_1' = (3, -2, 0, -1),$$
$$\alpha_2 = (9, 4, 6, -1), \quad \alpha_2' = (9, -4, 6, 1).$$

Acknowledgments. We express our gratitude to everyone who takes part in discussion of this paper in School of Mathematics and Statistics in Wuhan University. Especially, we thank Dr. Jing-bo Xia for his kind help. The first author express his gratitude to Guo-tai Deng, Yong-wei Yu and Wen-bo Wang for their help in programming. Finally, we thank the referee Professor Ph. Satgé for his valuable suggestions and Giovanni Gerotto for his patient work.

REFERENCES

[1] A. Baker, *Linear forms in the logarithms of algebraic number I*, Mathematika, **13** (1966), pp. 204–216; II: ibid, **14** (1967), pp. 102–107; III: ibid, **14** (1967), pp. 220-228; IV: ibid, **15** (1968), pp. 204–216.

[2] R. J. Stroeker - N. Tzanakis, *Solving Elliptic Diophantine Equations by Estimating Linear Forms in Elliptic Logarithms*, Acta Arith., **29**(2) (1994), pp. 177–196.

[3] R. J. Stroeker - N. Tzanakis, *On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an Improvement*, Experimental Mathemetics, 8(2) (1999), pp. 135–149.

[4] R. J. Stroeker - N. Tzanakis, *Computing All Integer Solutions of a Genus* 1 *Equation*, Math. Comp., **72** (2003), pp. 1917–1933.

[5] D. Zagier, *Large Integral Point on Elliptic Curves*, Math. Comp., **48**(177) (1987), pp. 425–536.

[6] W. Ljunggren, *A Diophantine Problem*, Jour London Math. Soc., **3**(2) (1971), pp. 385–391.

[7] J. H. Chen, *A Note on the Diophantine Equation* $x^2 + 1 = dy^4$, Abh. Math. Sem. Univ. Hamburg, **64** (1994), pp. 1–10.

[8] K. Q. Feng, *Algebraic Number Theory*, Science Press, 2000 (Chinese).

[9] L. G. Hua, *Introduction to Number Theory*, Science Press, 1979 (Chinese).

[10] R. J. STROEKER - N.TZANAKIS, *On the Application of skolem's p-adic Method to the solution of Thue Equations*, Journal of Number Theory, **29** (1988), pp. 166–195.
[11] W. LJUNGGREN, *Solution complete de quelquls equations du sixieme, degre a deux indeterminees*, Arch. Math., **48**(7) (1946), pp. 26–29.
[12] N. TZANAKIS, *On the Diophantine equation* $x^2 - dy^4 = k$, Acta Arith., **46**(3) (1986), pp. 257–269.
[13] L. J. MORDELL, *Diophantine Equations*, London: Academic Press, 1969.
[14] Z. F. CAO - S. Z. MU - X. L. DONG, *A New Proof of a Conjecture of Antoniadis*, Jour Number Theory, **83** (2000), pp. 185–193.
[15] J. BUCHMANN, *A generalization of Voronoi's unit algorithm (I II)*, Jour. Number Theory, **20** (1985), pp. 177–209.
[16] J. BUCHMANN, *The Computation of the Fundamental Unit of Totally Comples Quartic Orders*, Math. Comp., **48**(177) (1987), pp. 39–54.

Manoscritto pervenuto in redazione l'8 gennaio 2006