ACTA ARITHMETICA
XCVII.4 (2001)

Diophantine equations and class numbers of real quadratic fields

by

Xiaolei Dong and Zhenfu Cao (Harbin)

1. Introduction. Let $\mathbb{Z}$, $\mathbb{N}$, $\mathbb{Q}$, $\mathbb{P}$ be the sets of integers, positive integers, rational numbers and odd prime numbers, respectively. Let $d \in \mathbb{N}$ be a square free number, and $h(d)$ the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$, where d satisfies

$$1 + 4b^2k^{2n} = da^2, \quad a, b, k, n \in \mathbb{N},\ k > 1,\ n > 1. \tag{1}$$

In [17], Lu proved that if $a = b = 1$, then

$$h(d) \equiv 0 \pmod{n}. \tag{2}$$

In [11], Le proved that if $b = 1$, $n > 2$, $2k^n + a\sqrt{d}$ is the fundamental solution of Pell's equation $x^2 - dy^2 = -1$, and $(p, (q-1)q) = 1$ for each odd prime divisor $p \mid n$ and $q \mid k$, then (2) holds, except $(a, d, k, n) = (5, 41, 2, 4)$. Clearly, Le's result cannot imply Lu's result. In [3], we proved that if $b = 1$, $n > 2$, $2k^n + a\sqrt{d}$ is the fundamental solution of Pell's equation $x^2 - dy^2 = -1$, $a \le k^{n/2}$ and $2 \nmid k$, then (2) holds. By Lemma 3 of the present paper, the assumption "$2k^n + a\sqrt{d}$ is the fundamental solution of Pell's equation $x^2 - dy^2 = -1$" in [3] can be omitted.

In this paper, we prove the following further results.

Theorem 1. *If* $b = 1$, $n > 2$, *and one of the following cases holds*, *then* (2) *holds*, *except* $(a, d, k, n) = (5, 41, 2, 4)$:

Case 1: $a \mid^* d$; *the symbol* $a \mid^* d$ *means that every prime divisor of* a *divides* d;

Case 2: $(p, q^2 - 1) = 1$ *for each odd prime divisor* p *of* n *and prime divisor* q *of* a;

Case 3: $a \le 0.5k^{0.4226n}$ *or* $a \le 0.5k^{0.5527n}$ *and* $2 \nmid k$.

2000 *Mathematics Subject Classification*: 11R11, 11R29, 11D41.

Key words and phrases: real quadratic field, class number, Pell's equation, higher degree Diophantine equation, Lucas sequence, cryptographic problem, convergent.

Supported by the National Natural Science Foundation of China and the Heilongjiang Provincial Natural Science Foundation.

Remark. After submitting the paper, we found that a similar, but different as regards Case 2 of Theorem 1, result is contained in the paper of Ping Zhi Yuan [25]. And Yuan [26] also proved that if the equation

$$x^2 - dy^2 = 4q, \quad x, y \in \mathbb{Z},\ (x,y) = 1 \text{ or } 2, \tag{3}$$

has a solution for each prime divisor $q \mid b$, and $a \le 0.9b^{1/2}k^{n/4}$, then (2) holds.

Theorem 2. *Assume that equation* (3) *has a solution for each prime divisor $q \mid b$. If n has a prime factor p, and $a \le 0.5b^{\lambda_1}k^{\lambda_2 n}$, where $\lambda_1 = 2\lfloor\sqrt{p}\rfloor/(2\lfloor\sqrt{p}\rfloor + 1)$, $\lambda_2 = 1 - 1/\sqrt{p}$, then $p \mid h(d)$* (the symbol $\lfloor x \rfloor$ means greatest integer not greater than x).

Corollary 1. *Assume that equation* (3) *has a solution for each prime divisor $q \mid b$. If $a = 1$ and $b > 1$, then* (2) *holds.*

Corollary 2. *Assume that equation* (3) *has a solution for each prime divisor $q \mid b$. If $a \le 0.5b^{2/3}k^{0.29n}$, then* (2) *holds.*

Theorem 3. *Assume that equation* (3) *has a solution for each prime divisor $q \mid b$, and $a \le 0.5b^{2/3}k^{0.4226n}$. If $b = q_1^{2\alpha_1} \ldots q_s^{2\alpha_s}$, $(\alpha_i, q_i) \in \mathbb{N} \times \mathbb{P}$ $(i = 1, \ldots, s)$, and one of the following cases holds*:

1. $s = 1$;
2. $s \ge 2$, $q_1 \equiv 5 \pmod 8$ *and* $q_i \equiv 3 \pmod 4$ $(2 \le i \le s)$,

then (2) *holds*, *except $n = 6$, $k = 2$, $b = 3^2 \cdot 29^2$, $a = 985$, $d = 967441$.*

Clearly, the results are of importance for some cryptographic problems, since Buchmann and Williams [2] set up a key exchange cryptosystem in the class group of a quadratic field.

2. Lemmas. From (1), we see that Pell's equation

$$x^2 - dy^2 = -1, \quad x, y \in \mathbb{N}, \tag{4}$$

has solutions. Assume that $x_0 + y_0\sqrt{d}$ is the fundamental solution of (4).

Lemma 1. *If (x_1, y_1) is a solution of* (4), *and $y_1 \mid^* d$, then $x_1 + y_1\sqrt{d} = x_0 + y_0\sqrt{d}$ is the fundamental solution of* (4).

This lemma is a classical result of C. Størmer [22]. Cf. also M. Ward [24] and L. K. Durst [7]–[9].

Lemma 2. *If (x_1, y_1) is a solution of* (4), *and $x_1 > y_1^2/2$, then $x_1 + y_1\sqrt{d} = x_0 + y_0\sqrt{d}$ is the fundamental solution of* (4).

Proof. Otherwise, we assume $y_1 > y_0$. Then

$$y_0^2x_1^2 - x_0^2y_1^2 = y_0^2x_1^2 - y_1^2(dy_0^2 - 1) = y_0^2(x_1^2 - dy_1^2) + y_1^2 = y_1^2 - y_0^2 > 0.$$

Let

$$y_0^2x_1^2 - x_0^2y_1^2 = y_1^2 - y_0^2 = A \in \mathbb{N}.$$

Then

$$y_0x_1 + x_0y_1 = A_1, \quad y_0x_1 - x_0y_1 = A_2, \quad A = A_1A_2, \quad A_1, A_2 \in \mathbb{N}.$$

Since $(A_1 - 1)(A_2 - 1) \geq 0$, we easily see that

$$x_1 = \frac{A_1 + A_2}{2y_0} \leq \frac{A+1}{2y_0} = \frac{y_1^2 - y_0^2 + 1}{2y_0} \leq \frac{1}{2}y_1^2.$$

This contradicts our assumption. ∎

Lemma 2 yields

Lemma 3. *If a, b, d, k, n satisfy* (1), *and $a < 2\sqrt{b}\,k^{n/2}$, then $2bk^n + a\sqrt{d}$ is the fundamental solution of* (4).

Lemma 4. *If the equation $U^2 - dV^2 = 4$ has an integer solution with $(U, V) = 1$, then the Diophantine equation*

$$4x^{2n} - dy^2 = -1, \quad n > 2, \tag{5}$$

has no solution in positive integers, *except $d = 5$, $x = y = 1$.*

It is Theorem 1 of [3]. The key to the proof of Lemma 4 is using several results on the equations $x^2 + 3 = y^n$, $x^2 + 3 = 4y^n$, $3x^2 + 1 = y^n$ and $1 + 3x^2 = 4y^n$.

Proof. Assume that equation (5) has a positive integer solution x, y. Clearly, the equation $U^2 - dV^2 = 4$ has an integer solution with $(U, V) = 1$ if and only if the equation $U'^2 - dV'^2 = -4$ has an integer solution with $(U', V') = 1$. Let $\varrho = (U_0' + V_0'\sqrt{d})/2$ be the fundamental solution of the equation $U'^2 - dV'^2 = -4$. It is well known that $\varepsilon = \varrho^3$ is the fundamental solution of (4). Hence, from (5) we have

$$2x^n = \frac{\varepsilon^{2m+1} + \overline{\varepsilon}^{2m+1}}{2} = \frac{\varrho^{3(2m+1)} + \overline{\varrho}^{3(2m+1)}}{2}, \quad m \geq 0, \tag{6}$$

where $\overline{\varepsilon}, \overline{\varrho}$ satisfy $\varepsilon\overline{\varepsilon} = \varrho\overline{\varrho} = -1$. From (6),

$$4x^n = (\varrho^{2m+1} + \overline{\varrho}^{2m+1})((\varrho^{2m+1} + \overline{\varrho}^{2m+1})^2 + 3), \tag{7}$$

where $\varrho^{2m+1} + \overline{\varrho}^{2m+1} \in \mathbb{N}$. Since $(\varrho^{2m+1} + \overline{\varrho}^{2m+1}, (\varrho^{2m+1} + \overline{\varrho}^{2m+1})^2 + 3) = 1$ or 3, the latter occurring only for $3 \parallel (\varrho^{2m+1} + \overline{\varrho}^{2m+1})^2 + 3$, we see from (7) that

$$\varrho^{2m+1} + \overline{\varrho}^{2m+1} = 4x_1^n, \quad (\varrho^{2m+1} + \overline{\varrho}^{2m+1})^2 + 3 = x_2^n, \quad x = x_1x_2, \tag{8}$$

or

$$\varrho^{2m+1} + \overline{\varrho}^{2m+1} = x_1^n, \quad (\varrho^{2m+1} + \overline{\varrho}^{2m+1})^2 + 3 = 4x_2^n, \quad x = x_1x_2, \tag{9}$$

or

$$(10)\qquad \varrho^{2m+1}+\overline{\varrho}^{2m+1}=3^{n-1}\cdot 4x_1^n,\ \ (\varrho^{2m+1}+\overline{\varrho}^{2m+1})^2+3=3x_2^n,\ \ x=3x_1x_2,$$

or

$$(11)\qquad \varrho^{2m+1}+\overline{\varrho}^{2m+1}=3^{n-1}x_1^n,\ \ (\varrho^{2m+1}+\overline{\varrho}^{2m+1})^2+3=3\cdot 4x_2^n,\ \ x=3x_1x_2,$$

where $x_1, x_2 \in \mathbb{N}$ with $(x_1, x_2) = 1$. (8) is impossible since Nagell [19] and then Brown [1] proved that the equation $x^2+3 = y^n$ has no integer solutions with $n > 2$. Similarly, from Nagell [18], [19] and Ljunggren [14], [15] we know that the equation $x^2+3 = 4y^n$ $(n > 2)$ has the only positive integer solutions $x = y = 1$ and $n = 3$, $x = 37$, $y = 7$, the equation $3x^2 + 1 = y^n$ has no positive integer solutions with $n > 2$, and the equation $1+3x^2 = 4y^n$ $(n > 2)$ has the only positive integer solution $x = y = 1$. Thus (10) and (11) are impossible, and (9) has the only solution $x = 1$. ∎

Lemma 5. *If $l > 1$, then the only positive integer solutions of the equations*

$$x^2 - 2y^{2l} = \pm 1$$

are $1^2 - 2\cdot 1^{2l} = -1$, $239^2 - 2\cdot 13^4 = -1$.

Proof. It follows from [16], [23] and [4] that the only solutions of the equation $x^2-2y^4 = -1$ in positive integers are $(1, 1)$, $(293, 13)$, the equation $x^2 - 2y^{2l} = -1$ $(2\nmid l,\ l > 1)$ has only the trivial solution $x = y = 1$ and the equation $x^2 - 2y^{2l} = 1$ $(l > 1)$ has no solutions in positive integers. Hence the assertion holds. ∎

Lemma 6. *If $l > 1$ then the Diophantine equation*

$$x^{2l} - 2y^2 = \pm 1$$

have only the trivial solution $x = y = 1$.

Lemma 6 follows directly from two general results in [5] and [6].

Let u_n be the Lucas sequence, i.e. $u_n = (\alpha^n - \beta^n)/(\alpha-\beta)$, where α, β are the two roots of the equation

$$x^2 - Px + Q = 0, \qquad P, Q \in \mathbb{Z},\ (P, Q) = 1.$$

The prime p is called a *primitive prime factor* of u_n if n is the least positive integer with $p \mid u_n$.

Lemma 7. *Let p be a prime, $p\nmid 2Q$. Then*:

(i) *if p is a primitive prime factor of u_n, then $p \mid u_m$ if and only if $n \mid m$;*
(ii) *if $p > 2$, then $p \mid u_{p-(\frac{D}{p})}$, $D = P^2 - 4Q$, $\left(\frac{D}{p}\right)$ is the Legendre symbol.*

Proof. See [13], Theorem 1.7. ∎

It is well known that the simple continued fraction of $\sqrt{d}$ is periodical; we denote it by $\sqrt{d} = [a_0, \overline{a_1, \ldots, a_s}]$, where $a_0 = [\sqrt{d}]$, $a_s = 2a_0$ and $a_i < 2a_0$ for $i = 0, \ldots, s-1$.

LEMMA 8. *If $|L| < \sqrt{d}$ and (X,Y) is a positive integer solution of the equation*

$$(12) \qquad X^2 - dY^2 = L, \quad X, Y \in \mathbb{Z},\ (X,Y) = 1,$$

then X/Y is a convergent of $\sqrt{d}$.

Proof. See [10], Theorem 10.8.2. ∎

LEMMA 9. *For any $j \in \mathbb{Z}$ with $j \geq 0$, let p_j/q_j and r_j be the jth convergent and complete quotient of $\sqrt{d}$ respectively, and let $k_j = (-1)^{j-1}(p_j^2 - dq_j^2)$, $\Delta_j = (-1)^j(p_{j-1}p_j - dq_{j-1}q_j)$. Then*:

(i) $k_j > 0$, $\Delta_j > 0$, $a_{j+1} = [(\Delta_j + \sqrt{d})/k_j]$.

(ii) $k_j = 1$ *if and only if* $a_{j+1} = 2a_0$.

(iii) *Let $f = s - 1$ if $2 \mid s$ and $f = 2s - 1$ if $2 \nmid s$. Then $p_f + q_f\sqrt{d}$ is the fundamental solution of the equation*

$$(13) \qquad x^2 - dy^2 = 1, \quad x, y \in \mathbb{N}.$$

(iv) *For any $m \in \mathbb{N}$, $k_{ms+i} = k_i$ $(i = 0, \ldots, s-1)$.*

(v) *If* $1 < |L| < \sqrt{d}$, $2d \not\equiv 0 \pmod{|L|}$ *and equation* (12) *has a solution* (X,Y), *then equation* (12) *has at least two positive solutions such that* $X < p_f$ *and* $Y < q_f$.

Proof. See [12], Lemma 5. ∎

LEMMA 10. *If $(l,p) \in \mathbb{N} \times \mathbb{P}$, $l > 1$, then the Diophantine equation*

$$(14) \qquad x^2 - 2^{2l-1}p^{2\alpha}y^{2l} = 1, \quad x, y, \alpha \in \mathbb{N},$$

has no solutions, *except* $17^2 - 2^5 \cdot 3^2 \cdot 1^6 = 1, 114243^2 - 2^3 \cdot 239^2 \cdot 13^4 = 1.$

Proof. Assume that equation (14) has a solution. Then

$$(15) \qquad x \pm 1 = 2y_1^{2l}, \quad x \mp 1 = 2^{2l-2}p^{2\alpha}y_2^{2l}, \quad y = y_1y_2,$$

or

$$(16) \qquad x \pm 1 = 2p^{2\alpha}y_1^{2l}, \quad x \mp 1 = 2^{2l-2}y_2^{2l}, \quad y = y_1y_2,$$

where $y_1, y_2 \in \mathbb{N}$ with $(y_1, y_2) = 1$. From (15), we get

$$y_1^{2l} - 2(2^{l-2}p^\alpha y_2^l)^2 = \pm 1,$$

which is impossible by Lemma 6. From (16), we get

$$(17) \qquad (p^\alpha y_1^l)^2 - 2^{2l-3}y_2^{2l} = \pm 1.$$

If $l = 2$, then (17) gives $p = 239$, $\alpha = 1$, $y_1 = 1$, $y_2 = 13$ by Lemma 5. This gives a solution $l = 2$, $p = 239$, $\alpha = 1$, $x = 114243$, $y = 13$ of equation (14). If $l > 2$, then considering the equality (17) mod 8 we obtain $(p^\alpha y_1^l)^2 - 2^{2l-3}y_2^{2l} = 1$, and so

$$p^\alpha y_1^l \pm 1 = 2y_3^{2l}, \quad p^\alpha y_1^l \mp 1 = 2^{2l-4}y_4^{2l}, \quad y_2 = y_3y_4,$$

where $y_3, y_4 \in \mathbb{N}$ with $(y_3, y_4) = 1$. Hence,

$$y_3^{2l} - 2(2^{l-3}y_4^l)^2 = \pm 1,$$

which is impossible, except $l = 3$, $y_3 = y_4 = 1$ by Lemma 6. This gives another solution of (14): $l = 3$, $p = 3$, $\alpha = 1$, $x = 17$, $y = 1$. ∎

LEMMA 11. *If $c, l \in \mathbb{N}$ with $l > 1$, and c is only divisible by primes of the form $4m + 3$, then the Diophantine equation*

$$x^2 - 2^{2l-1}c^2y^{2l} = 1, \qquad x, y \in \mathbb{N}, \tag{18}$$

has no solutions, except $l = c = 3$, $x = 17$, $y = 1$ and $l = 2$, $c = 239$, $x = 114243$, $y = 13$.

Proof. Assume that equation (18) has a solution. From (18), we have

$$x \pm 1 = 2c_1^2y_1^{2l}, \qquad x \mp 1 = 2^{2l-2}c_2^2y_2^{2l}, \qquad y = y_1y_2, \qquad c = c_1c_2,$$

and so

$$c_1^2y_1^{2l} - 2^{2l-3}c_2^2y_2^{2l} = \pm 1. \tag{19}$$

If $c_2 = 1$, then (19) has only two exceptional solutions by the same argument as in the proof of Lemma 10. If $c_2 > 1$, then from the assumption we know that (19) gives $c_1^2y_1^{2l} - 2^{2l-3}c_2^2y_2^{2l} = 1$, and so

$$c_1y_1^l \pm 1 = 2c_3^2y_3^{2l}, \qquad c_1y_1^l \mp 1 = 2^{2l-4}c_4^2y_4^{2l}, \qquad y_2 = y_3y_4, \qquad c_2 = c_3c_4. \tag{20}$$

If $c_1 = 1$, then (19) is impossible by Lemma 6. If $c_1 > 1$, then "$c_1y_1^l - 1 = 2^{2l-4}c_4^2y_4^{2l}$" is impossible. So (20) gives

$$c_3^2y_3^{2l} - 2^{2l-5}c_4^2y_4^{2l} = -1. \tag{21}$$

Thus, $c_4 = 1$, $l = 3$. But by Lemma 5, (21) also is impossible. ∎

3. Proof of Theorem 1. From Lu's result, we may assume that $b = 1$, $a > 1$. We see from (1) that

$$(2k^n + 1)^2 - da^2 = 4k^n. \tag{22}$$

Using the properties of the real quadratic field $\mathbb{Q}(\sqrt{d})$ (e.g. see Nagell [20] where the same idea is used in the case of imaginary quadratic fields, or Lemma 8.9 in Narkiewicz's book [21]), we deduce from (22) that

$$n = Z_1t, \qquad \frac{2k^n + 1 + a\sqrt{d}}{2} = \eta\left(\frac{X_1 + Y_1\sqrt{d}}{2}\right)^t, \qquad t \in \mathbb{N}, \tag{23}$$

where η is some unit of $\mathbb{Q}(\sqrt{d})$, t is the maximal positive integer T such that the ideal generated by $(2k^n + 1 + a\sqrt{d})/2$ is the Tth power of a principal ideal, X_1, Y_1, Z_1 are non-zero integers with

$$X_1^2 - dY_1^2 = 4k^{Z_1}, \qquad (X_1, Y_1) = 1, \qquad Z_1 \in \mathbb{N}, \qquad h(d) \equiv 0 \pmod{Z_1}. \tag{24}$$

Lemma 4 implies that ε, the fundamental solution of Pell's equation $x^2 - dy^2 = -1$, is the fundamental unit (except the case $d = 5$ which is excluded by the assumption $k > 1$ in (1)) of $\mathbb{Q}(\sqrt{d})$ and thus $\eta = \pm\varepsilon^{2s}$, $s \in \mathbb{Z}$. (23) gives

$$\frac{2k^n + 1 + a\sqrt{d}}{2} = \pm\varepsilon^{2s}\left(\frac{X_1 + Y_1\sqrt{d}}{2}\right)^t. \tag{25}$$

If $t = 1$, then the theorem is proved. Otherwise, $t > 1$. If $2 \mid t$, then $t = 2t_1$, $t_1 \in \mathbb{N}$. Define the integers U, V by

$$\varepsilon^s\left(\frac{X_1 + Y_1\sqrt{d}}{2}\right)^{t_1} = \frac{U + V\sqrt{d}}{2}, \qquad \overline{\varepsilon}^s\left(\frac{X_1 - Y_1\sqrt{d}}{2}\right)^{t_1} = \frac{U - V\sqrt{d}}{2},$$

where $\overline{\varepsilon} = x_0 - y_0\sqrt{d}$ with $\varepsilon\overline{\varepsilon} = -1$. Clearly, U, V satisfy

$$U^2 - dV^2 = (-1)^s 4k^{Z_1 t_1} = (-1)^s 4k^{n/2}, \qquad (U, V) = 1. \tag{26}$$

So, by (25), we get

$$\frac{1 + 2k^n + a\sqrt{d}}{2} = \left(\frac{U + V\sqrt{d}}{2}\right)^2 = \frac{(U^2 + dV^2)/2 + UV\sqrt{d}}{2}. \tag{27}$$

From (26) and (27), we have $1 + 2k^n = U^2 - (-1)^s 2k^{n/2}$, and so

$$(k^{n/2})^2 + (k^{n/2} + (-1)^s)^2 = U^2. \tag{28}$$

From (28), we know that $(k^{n/2}, k^{n/2} + (-1)^s, |U|)$ is a primitive Pythagorean triple such that

$$k^{n/2} = 2AB, \qquad k^{n/2} + (-1)^s = A^2 - B^2, \qquad |U| = A^2 + B^2, \tag{29}$$

or

$$k^{n/2} = A^2 - B^2, \qquad k^{n/2} + (-1)^s = 2AB, \qquad |U| = A^2 + B^2, \tag{30}$$

where $A, B \in \mathbb{N}$, $A > B$, $2 \mid AB$ and $(A, B) = 1$. (29) gives

$$(A + B)^2 - 2A^2 = -(-1)^s, \qquad (A - B)^2 - 2B^2 = (-1)^s,$$

and $A = k_1^{n/2}$ or $B = k_1^{n/2}$ since $k^{n/2} = 2AB$, $(A, B) = 1$. Hence

$$(A + B)^2 - 2k_1^{2\cdot n/2} = -(-1)^s, \qquad \text{or} \qquad (A - B)^2 - 2k_1^{2\cdot n/2} = (-1)^s.$$

This implies that (29) is impossible, except $A = 2$, $B = 1$, $n = 4$, $k = 2$, $|U| = 5$, by Lemma 5. So $(a, d, k, n) = (5, 41, 2, 4)$ is an exception. For (30), we have

$$(A - B)^2 - 2B^2 = -(-1)^s,$$

and $A - B = k_1^{n/2}$ from $k^{n/2} = (A - B)(A + B)$, $(A - B, A + B) = 1$. Hence,

$$k_1^{2\cdot n/2} - 2B^2 = -(-1)^s.$$

This implies that (30) is impossible by Lemma 6.

If $2\nmid t$, then t has an odd prime factor p. We first consider the proof of Case 3. When $a \leq 0.5k^{\lambda n}$, $\lambda = 1 - 1/\sqrt{p}$, we can prove from (23) and (24) that no prime p can divide t (for a similar argument see the proof of Lemma 12 later). Hence, $a > 0.5k^{\lambda n}$, $\lambda = 1 - 1/\sqrt{p}$. Notice that $((X_1 + Y_1\sqrt{d})/2)^p \in \mathbb{Z}[\sqrt{d}]$ when $p = 3$ and $2\nmid k$, and (25) is impossible if $((X_1 + Y_1\sqrt{d})/2)^p \in \mathbb{Z}[\sqrt{d}]$. Thus, we have $\lambda > 0.4226$ since $p \geq 3$ and $\lambda > 0.5527$ if $2\nmid k$. This contradicts our assumption.

Now, we consider the proof of Cases 1 and 2. Since p is an odd prime, there exist $u, v \in \mathbb{Z}$ with

$$2s = up + v, \qquad |v| < p/2. \tag{31}$$

Let

$$\varrho = \pm\varepsilon^u\left(\frac{X_1 + Y_1\sqrt{d}}{2}\right)^{t/p}, \qquad \overline{\varrho} = \pm\overline{\varepsilon}^u\left(\frac{X_1 - Y_1\sqrt{d}}{2}\right)^{t/p}. \tag{32}$$

Then there exist $X, Y \in \mathbb{Z}$ with

$$\varrho = (X + Y\sqrt{d})/2, \qquad \overline{\varrho} = (X - Y\sqrt{d})/2, \tag{33}$$

and

$$X^2 - dY^2 = (-1)^u 4k^{n/p}, \qquad (X, Y) = 1. \tag{34}$$

Hence, (25) gives

$$2k^n + 1 + a\sqrt{d} = 2\varepsilon^v\varrho^p, \qquad 2k^n + 1 - a\sqrt{d} = 2\overline{\varepsilon}^v\overline{\varrho}^p. \tag{35}$$

First, we prove

Conclusion 1. *If Case* 1 *holds*, *then* (35) *is impossible.*

Proof. From Lemma 1, $\varepsilon = 2k^n + a\sqrt{d}$. Hence we see from (35) that

$$2k^n + 1 \equiv 2(2k^n)^v\varrho^p \pmod{a}. \tag{36}$$

Let $\varrho^p = (X_p + Y_p\sqrt{d})/2$. Clearly, $X_p, Y_p \in \mathbb{Z}$, $(X_p, Y_p) = 1$. We deduce from (36) that $0 \equiv (2k^n)^v \cdot Y_p \pmod{a}$, and so

$$a \mid Y_p \tag{37}$$

since $(2k, a) = 1$. Notice that

$$\frac{\varrho^p - \overline{\varrho}^p}{\varrho - \overline{\varrho}} = \frac{1}{2^{p-1}}\left(\binom{p}{1}X^{p-1} + \binom{p}{3}X^{p-3}(Y\sqrt{d})^2 + \dots\right) \equiv \frac{p}{2^{p-1}}X^{p-1} \pmod{d}. \tag{38}$$

Thus $((\varrho^p - \overline{\varrho}^p)/(\varrho - \overline{\varrho}), d) = 1$ or p. So

$$\left(\frac{\varrho^p - \overline{\varrho}^p}{\varrho - \overline{\varrho}}, a\right) = 1 \text{ or } p \tag{39}$$

since $a \mid^* d$. If $p \mid a$, then from (38) we see that $p \| (\varrho^p - \overline{\varrho}^p)/(\varrho - \overline{\varrho})$. Hence from (37), (39) and $Y_p = Y(\varrho^p - \overline{\varrho}^p)/(\varrho - \overline{\varrho})$ we get $|Y| \geq a/c$, with $c = 1$

if $p \nmid a$ or $c = p$ if $p \mid a$. So

$$\frac{|X| + |Y|\sqrt{d}}{2} > \frac{a\sqrt{d}}{2c}. \tag{40}$$

If $v \leq 0$, then from (35) we have $\varrho > |\overline{\varrho}|$ and so $X > 0, Y > 0$. Hence, from (40), the first equality of (35), and (31), we get

$$\begin{aligned}\frac{a\sqrt{d}}{2c} < \varrho = \left(\frac{\varepsilon^{-v}(1+\varepsilon)}{2}\right)^{1/p} &< (\varepsilon^{(p-1)/2} \cdot \varepsilon)^{1/p} = \varepsilon^{1/2+1/(2p)} \\ &< (4k^n + 1)^{1/2+1/(2p)}.\end{aligned} \tag{41}$$

Also, by (1) (notice $b = 1$), we have

$$k^n/c < \sqrt{1 + 4k^{2n}}/(2c) = a\sqrt{d}/(2c). \tag{42}$$

From (41) and (42), we get $k^n < c(4k^n + 1)^{1/2+1/(2p)}$. Then we have

$$(4k^n + 1)^{1/2+1/(2p)}((4k^n + 1)^{1/2-1/(2p)} - 4c) < 1. \tag{43}$$

Clearly, (43) is impossible, except $k = 2$, $n = p = 3$, if $c = 1$. When $k = 2$, $n = p = 3$, from (1) and $b = 1$ we get $d = 257, a = 1$. This contradicts our assumption $a > 1$. If $c = p$, then from (1) we have $p \equiv 1 \pmod 4$ since $p \mid a$. Hence, we see that (43) is impossible if $n > p$ or $p > 5$ or $k > 3$. But $n = p = 5$, $k = 2$ and $n = p = 5$, $k = 3$ do not satisfy (1) ($b = 1$) and $p \mid a$.

If $v > 0$, then from (35) we find that $\varrho < 1$ and $|\overline{\varrho}| = (|X| + |Y|\sqrt{d})/2$. Hence, from (40), the second equality of (35), and (31), we also get (41). Thus (35) is impossible. ■

Next, we prove

Conclusion 2. *If Case* 2 *holds*, *then* (35) *is impossible.*

Proof. It is well known that

$$2k^n + a\sqrt{d} = \varepsilon^l, \quad 2 \nmid l \in \mathbb{N}, \tag{44}$$

since $(2k^n, a)$ is a solution of Pell's equation $x^2 - dy^2 = -1$. Hence, from (35), we have

$$1 + \varepsilon^l = 2\varepsilon^v \varrho^p, \quad 1 + \overline{\varepsilon}^l = 2\overline{\varepsilon}^v \overline{\varrho}^p. \tag{45}$$

In (45), if $p \mid l$, then from (44) we have

$$a = \frac{\varepsilon'^p - \overline{\varepsilon}'^p}{\varepsilon' - \overline{\varepsilon}'} \cdot y_0', \tag{46}$$

where

$$x_0' + y_0'\sqrt{d} = \varepsilon' = \varepsilon^{l/p}, \quad x_0' - y_0'\sqrt{d} = \overline{\varepsilon}' = \overline{\varepsilon}^{l/p}.$$

Clearly, every prime factor $q \neq p$ of $(\varepsilon'^p - \overline{\varepsilon}'^p)/(\varepsilon' - \overline{\varepsilon}')$ is a primitive prime factor of $(\varepsilon'^p - \overline{\varepsilon}'^p)/(\varepsilon' - \overline{\varepsilon}')$. From Lemma 7(ii), we see that $q \mid u_{q-(\frac{D}{q})}$,

$D = 4dy_0'^2$. Hence, from Lemma 7(i), we get $p \mid q - \left(\frac{D}{q}\right)$. But $q \neq p$, $p \nmid q^2 - 1$, a contradiction. Therefore, from (46), we have

$$\frac{\varepsilon'^p - \overline{\varepsilon}'^p}{\varepsilon' - \overline{\varepsilon}'} = 1 \text{ or } p \tag{47}$$

since if $p \mid (\varepsilon'^p - \overline{\varepsilon}'^p)/(\varepsilon' - \overline{\varepsilon}')$ then $p \parallel (\varepsilon'^p - \overline{\varepsilon}'^p)/(\varepsilon' - \overline{\varepsilon}')$. However, (47) is impossible.

If $p \nmid l$, then there are $s, t \in \mathbb{Z}$ such that

$$v = sp + tl, \qquad |t| < p/2. \tag{48}$$

Let

$$\varrho_1 = \varepsilon^s \varrho = \frac{X' + Y'\sqrt{d}}{2}, \qquad \overline{\varrho}_1 = \overline{\varepsilon}^s \overline{\varrho} = \frac{X' - Y'\sqrt{d}}{2},$$

where $X', Y' \in \mathbb{Z}$ with

$$X'^2 - dY'^2 = (-1)^{s+u} 4k^{n/p}, \qquad (X', Y') = 1. \tag{49}$$

And let $\varepsilon_1 = \varepsilon^l$, $\overline{\varepsilon}_1 = \overline{\varepsilon}^l$. Then from (45) we get

$$1 + \varepsilon_1 = 2\varepsilon_1^t \varrho_1^p, \qquad 1 + \overline{\varepsilon}_1 = 2\overline{\varepsilon}_1^t \overline{\varrho}_1^p. \tag{50}$$

By the same argument as in the proof for Conclusion 1, (50) gives

$$a \,\Big|\, Y' \frac{\varrho_1^p - \overline{\varrho}_1^p}{\varrho_1 - \overline{\varrho}_1},$$

and we see that every prime factor $q \neq p$ of a satisfies $q \nmid (\varrho_1^p - \overline{\varrho}_1^p)/(\varrho_1 - \overline{\varrho}_1)$ since $p \nmid q^2 - 1$. Hence, it can be shown that $|Y'| \geq a/c$, with $c = 1$ if $p \nmid a$ or $c = p$ if $p \mid a$. So (50) is impossible by a similar method as in the proof of Conclusion 1. ■

So Theorem 1 is proved. ■

4. Proof of Theorem 2. From (1), we have

$$(2bk^n + 1)^2 - da^2 = 4bk^n. \tag{51}$$

Using the properties of the real quadratic field $\mathbb{Q}(\sqrt{d})$, we deduce from (51) that

$$\left[\frac{2bk^n + 1 + a\sqrt{d}}{2}\right]\left[\frac{2bk^n + 1 - a\sqrt{d}}{2}\right] = [b][k]^n, \tag{52}$$

and the ideals $[(2bk^n + 1 + a\sqrt{d})/2]$ and $[(2bk^n + 1 - a\sqrt{d})/2]$ are coprime. Our assumption about the solvability of (3) implies that each prime divisor of the ideal $[b]$ is a principal ideal. So we infer from (52) that

$$\left[\frac{2bk^n + 1 + a\sqrt{d}}{2}\right] = \left[\frac{x_1 + y_1\sqrt{d}}{2}\right] A^n \tag{53}$$

by unique factorization of ideals in $\mathbb{Q}(\sqrt{d})$, where $x_1, y_1 \in \mathbb{Z}$ satisfy

$$x_1^2 - dy_1^2 = 4b, \quad (x_1, y_1) = 1 \text{ or } 2,$$

$A\overline{A} = [k]$, $\overline{A}$ is the conjugate ideal of A. Let z_1 be the least positive integer such that A^{z_1} is a principal ideal. We have

$$h(d) \equiv 0 \pmod{z_1}, \quad n = z_1 t, \quad t \in \mathbb{N}. \tag{54}$$

Clearly, it suffices to prove the following

LEMMA 12. *No prime p satisfying the assumption of Theorem 2 can divide t.*

Proof. Assume that $p \mid t$. Let $A^{z_1 t/p} = [(X_1 + Y_1\sqrt{d})/2]$, where $X_1, Y_1 \in \mathbb{Z}$ satisfy

$$X_1^2 - dY_1^2 = \pm 4k^{n/p}, \quad (X_1, Y_1) = 1 \text{ or } 2. \tag{55}$$

Since Pell's equation

$$x^2 - dy^2 = -1, \quad x, y \in \mathbb{N}, \tag{56}$$

has a solution by (1), we see from (55) that the equations

$$X^2 - dY^2 = 4k^{n/p}, \quad X, Y \in \mathbb{N},\ (X, Y) = 1 \text{ or } 2, \tag{57}$$

and

$$X^2 - dY^2 = -4k^{n/p}, \quad X, Y \in \mathbb{N},\ (X, Y) = 1 \text{ or } 2, \tag{58}$$

have solutions X, Y respectively. Without loss of generality, we may assume that X_1, Y_1 is a solution of (57). Let ε be the fundamental solution of Pell's equation (56), and let

$$\left(\frac{X_1 + Y_1\sqrt{d}}{2}\right)^i = \frac{U_i + V_i\sqrt{d}}{2^{l_i}}, \quad i = 1, \ldots, r,$$

and

$$\varepsilon\left(\frac{X_1 + Y_1\sqrt{d}}{2}\right)^i = \frac{U_i' + V_i'\sqrt{d}}{2^{l_i}}, \quad i = 1, \ldots, r,$$

where $U_i, V_i, U_i', V_i' \in \mathbb{Z}$ with

$$U_i^2 - dV_i^2 = 4^{l_i} k^{in/p}, \quad (U_i, V_i) = 1,\ l_i = 0 \text{ or } 1,$$

and

$$U_i'^2 - dV_i'^2 = -4^{l_i} k^{in/p}, \quad (U_i', V_i') = 1,\ l_i = 0 \text{ or } 1.$$

Since $a \le 0.5b^{\lambda_1}k^{\lambda_2 n}$, from (1) we have $\sqrt{d} > 2bk^n/a \ge 4b^{1-\lambda_1}k^{n(1-\lambda_2)}$. So $4^{l_r}k^{rn/p} \le 4k^{rn/p} \le 4k^{n(1-\lambda_2)} < 4b^{1-\lambda_1}k^{n(1-\lambda_2)} < \sqrt{d}$ for $r = \lfloor p(1-\lambda_2)\rfloor$. By Lemmas 8 and 9(v), $\sqrt{d}$ has $4r$ convergents $p_{s_i^{(j)}}/q_{s_i^{(j)}}$ ($j = 1, \ldots, 4$, $i = 1, \ldots, r$) such that

$$k_{s_i^{(j)}} = 4^{l_i} k^{in/p}, \quad 2 \nmid s_i^{(j)}, \quad 0 < s_i^{(j)} < f, \quad j = 1, \ldots, 4,\ i = 1, \ldots, r,$$

where $f = 2s-1$, $2\nmid s$ since Pell's equation (56) has a solution. From Lemma 9(iv), we know that $\sqrt{d}$ has $2r$ convergents $p_{t_i^{(j)}}/q_{t_i^{(j)}}$ ($j=1,2,\ i=1,\dots,r$) such that

$$k_{t_i^{(j)}} = 4^{l_i}k^{in/p}, \quad 2\nmid t_i^{(j)}, \quad 0 < t_i^{(j)} < s, \quad j=1,2,\ i=1,\dots,r.$$

Therefore, by Lemma 9(i), we have

$$a_{t_i^{(j)}+1} = \left\lfloor \frac{\Delta_{t_i^{(j)}} + \sqrt{d}}{k_{t_i^{(j)}}} \right\rfloor > \frac{\sqrt{d}}{4^{l_i}k^{in/p}}, \quad j=1,2,\ i=1,\dots,r.$$

Since ε is the fundamental solution of Pell's equation (56), we have $\varepsilon = p_{s-1}+q_{s-1}\sqrt{d}$. Notice that $p_0 = a_0$, $p_1 = a_0a_1+1$, and $p_{j+2} = a_{j+2}p_{j+1}+p_j$ for $j \ge 0$. We have

$$\begin{aligned}(59)\qquad p_{s-1} &> \prod_{j=0}^{s-1} a_j \ge a_0 \prod_{i=1}^{r}\prod_{j=1}^{2} a_{t_i^{(j)}+1} > a_0\left(\prod_{i=1}^{r}\frac{\sqrt{d}}{4^{l_i}k^{in/p}}\right)^2\\ &\ge \frac{a_0d^r}{2^{4r}k^{r(r+1)n/p}} > a_0\cdot\frac{(4b^{1-\lambda_1}k^{n(1-\lambda_2)})^{2r}}{2^{4r}k^{r(r+1)n/p}}\\ &= a_0b^{2r(1-\lambda_1)}k^{n(2r(1-\lambda_2)-r(r+1)/p)}.\end{aligned}$$

Since $a_0 = \lfloor\sqrt{d}\rfloor$, $n(1-\lambda_2) > 1$, we have $a_0 > \sqrt{d}-1 > 2b^{1-\lambda_1}k^{n(1-\lambda_2)}$. Hence, (59) gives

$$(60)\quad p_{s-1} > 2b^{(2r+1)(1-\lambda_1)}k^{n((2r+1)(1-\lambda_2)-r(r+1)/p)} = 2b^{(2r+1)(1-\lambda_1)}k^{ng(r)},$$

where $g(r) = (2r+1)(1-\lambda_2) - r(r+1)/p$. Clearly, $g(r) \ge p(1-\lambda_2)^2$ since $r = \lfloor p(1-\lambda_2)\rfloor$. We have $g(r) \ge 1$ and $(2r+1)(1-\lambda_1) = 1$ since $\lambda_2 = 1-1/\sqrt{p}$, and so from (60) we conclude that $p_{s-1} > 2bk^n$. On the other hand, by (1), we see that $2bk^n \ge p_{s-1}$, a contradiction. ■

5. Proof of corollaries. Clearly, it suffices to prove Corollary 2. We deduce from (54) that if $t=1$ then Corollary 2 holds. Now, we assume that $t>1$, and so there is a prime p such that $p\,|\,t$. The proof of Lemma 12 shows that if $a \le 0.5b^{\lambda_1}k^{\lambda_2 n}$, then "$p\,|\,t$" is impossible. Also, $\lambda_1 \ge 2/3$, $\lambda_2 > 0.29$ since $p \ge 2$. Hence, if $a \le 0.5b^{2/3}k^{0.29n}$ then (2) holds. The proof is complete.

6. Proof of Theorem 3. From (52), we get

$$(61)\qquad \left[\frac{2bk^n+1+a\sqrt{d}}{2}\right] = \left[\frac{x_2+y_2\sqrt{d}}{2}\right]^2 A^n,$$

and (54), where $x_2, y_2 \in \mathbb{Z}$ with

$$(62)\qquad x_2^2 - dy_2^2 = 4\sqrt{b}, \quad (x_2,y_2) = 1 \text{ or } 2.$$

Let $A^{z_1} = [(X_2 + Y_2\sqrt{d})/2]$, where $X_2, Y_2 \in \mathbb{Z}$ satisfy

$$X_2^2 - dY_2^2 = \pm 4k^{z_1}, \qquad (X_2, Y_2) = 1 \text{ or } 2. \tag{63}$$

We deduce from (61) that

$$\frac{2bk^n + 1 + a\sqrt{d}}{2} = \eta\left(\frac{x_2 + y_2\sqrt{d}}{2}\right)^2 \left(\frac{X_2 + Y_2\sqrt{d}}{2}\right)^t, \qquad t \in \mathbb{N}, \tag{64}$$

where η is some unit of $\mathbb{Q}(\sqrt{d})$ with $N(\eta) = 1$. Since Pell's equation (56) has a solution, we have $\eta = \pm\varepsilon_1^{2m}$, where ε_1 is the fundamental unit of $\mathbb{Q}(\sqrt{d})$ with $N(\varepsilon_1) = -1$, $m \in \mathbb{Z}$. Hence, (64) gives

$$\frac{2bk^n + 1 + a\sqrt{d}}{2} = \pm\varepsilon_1^{2m}\left(\frac{x_2 + y_2\sqrt{d}}{2}\right)^2 \left(\frac{X_2 + Y_2\sqrt{d}}{2}\right)^t. \tag{65}$$

If $t = 1$, then the theorem is proved. If $2 \mid t$, then $t = 2t_1$, $t_1 \in \mathbb{N}$. Assume that

$$\varepsilon_1^m\left(\frac{x_2 + y_2\sqrt{d}}{2}\right)\left(\frac{X_2 + Y_2\sqrt{d}}{2}\right)^{t_1} = \frac{U + V\sqrt{d}}{2},$$

where $U, V \in \mathbb{Z}$ satisfy

$$U^2 - dV^2 = (-1)^m(\pm 1)^{t_1} 4\sqrt{b}\, k^{z_1 t_1} = (-1)^{m'} 4\sqrt{b}\, k^{n/2}, \qquad (U, V) = 1 \text{ or } 2. \tag{66}$$

So from (65) we get

$$\frac{1 + 2bk^n + a\sqrt{d}}{2} = \left(\frac{U + V\sqrt{d}}{2}\right)^2 = \frac{(U^2 + dV^2)/2 + UV\sqrt{d}}{2}. \tag{67}$$

From (66) and (67), we have

$$1 + 2bk^n = U^2 - (-1)^{m'} 2\sqrt{b}\, k^{n/2},$$

and so

$$(\sqrt{b}\, k^{n/2})^2 + (\sqrt{b}\, k^{n/2} + (-1)^{m'})^2 = U^2. \tag{68}$$

From (68), we know that $(\sqrt{b}\, k^{n/2}, \sqrt{b}\, k^{n/2} + (-1)^{m'}, |U|)$ is a primitive Pythagorean triple such that

$$\sqrt{b}\, k^{n/2} = 2AB, \qquad \sqrt{b}\, k^{n/2} + (-1)^{m'} = A^2 - B^2, \qquad |U| = A^2 + B^2, \tag{69}$$

or

$$\sqrt{b}\, k^{n/2} = A^2 - B^2, \qquad \sqrt{b}\, k^{n/2} + (-1)^{m'} = 2AB, \qquad |U| = A^2 + B^2, \tag{70}$$

where $A, B \in \mathbb{N}$, $A > B$, $2 \mid AB$ and $(A, B) = 1$.

First, we consider (69). We have

$$(A + B)^2 - 2A^2 = -(-1)^{m'}, \qquad (A - B)^2 - 2B^2 = (-1)^{m'}. \tag{71}$$

If $A = k_1^{n/2}$, $k_1 \in \mathbb{N}$, then (71) gives

$$(A+B)^2 - 2k_1^{2\cdot n/2} = -(-1)^{m'}.$$

This implies that $2 \mid m'$, $n = 4$, $k_1 = 13$, $A + B = 239$ by Lemma 5. So $A = 169, B = 70$. This implies $\sqrt{b}\, k^2 = 2^2 \cdot 5 \cdot 7 \cdot 13^2$ and $|U| = 33461$. Hence, from (67) we see that $a = UV \geq 33461$. But $33461 > 0.5 \cdot 35^{4/3} \cdot 26^{0.4226\cdot 4}$, a contradiction.

If $2B = k_2^{n/2}$, $k_2 \in \mathbb{N}$, then (71) gives $2 \mid m'$ and

$$(A-B)^2 - 2(2^{l-1}(k_2/2)^l)^2 = 1, \quad l = n/2 > 1. \tag{72}$$

Clearly, (72) gives

$$(A-B) \pm 1 = 2u^2, \quad (A-B) \mp 1 = 4v^2, \quad uv = 2^{l-2}(k_2/2)^l,$$

where $u, v \in \mathbb{N}$ with $(u, v) = 1$. And so

$$u^2 - 2v^2 = \pm 1, \quad u = u_1^l, \quad v = 2^{l-2}v_1^l, \quad k_2 = 2u_1v_1,$$

i.e.

$$u_1^{2l} - 2(2^{l-2}v_1^l)^2 = \pm 1.$$

This implies that $u_1 = 2^{l-2}v_1 = 1$ by Lemma 6. So $l = 2$, $k_2 = 2$, $A - B = 3$, $B = 2$. This implies $\sqrt{b}\, k^2 = 2^2 \cdot 5$ and $|U| = 29$. Hence $n = 4$, $a = 29$, $b = 25$, $k = 2$. But $29 > 0.5 \cdot 25^{2/3} \cdot 2^{0.4226\cdot 4}$, a contradiction.

By a similar method, if $2A = k_1^{n/2}$ or $B = k_2^{n/2}$, then from (71) and the assumption of the theorem, we also get a contradiction.

If $2^\lambda A \neq k_1^{n/2}$ and $2^\lambda B \neq k_2^{n/2}$, where $\lambda = 0$ or 1, notice (71); then from $2AB = q_1^{\alpha_1} \dots q_s^{\alpha_s} k^{n/2}$ we get

$$\begin{aligned} 2^\lambda A &= (q_1^{\alpha_1})^{1-\lambda}(q_2^{\alpha_2} \dots q_s^{\alpha_s})^\lambda k_1^{n/2}, \\ 2^{1-\lambda} B &= (q_1^{\alpha_1})^{\lambda}(q_2^{\alpha_2} \dots q_s^{\alpha_s})^{1-\lambda} k_2^{n/2}, \\ & \qquad k = k_1k_2, \quad k_1, k_2 \in \mathbb{N}, \quad \lambda = 0 \text{ or } 1. \end{aligned} \tag{73}$$

Clearly, if $\lambda = 0$, then (71) and (73) give $2 \mid m'$ and

$$(A-B)^2 - 2(2^{l-1}q_2^{\alpha_2} \dots q_s^{\alpha_s}(k_2/2)^l)^2 = 1, \quad l = n/2 > 1. \tag{74}$$

By Lemmas 10 and 11, we infer from (74) that

$$l = 2, \quad q_2^{\alpha_2} \dots q_s^{\alpha_s} = 239, \quad A - B = 114243, \quad k_2 = 26 \tag{75}$$

or

$$l = 3, \quad q_2^{\alpha_2} \dots q_s^{\alpha_s} = 3, \quad A - B = 17, \quad k_2 = 2. \tag{76}$$

From (73) and (75), we see that $B = 80782, A = 5^2 \cdot 29 \cdot 269 = q_1^{\alpha_1}k_1^l$, which is impossible. From (76) and (73), we find that $n = 6$, $k = 2$, $b = 3^2 \cdot 29^2$, and $a = 985$, $d = 967441$. This is an exceptional case.

If $\lambda = 1$, then (71) and (73) give $2 \nmid m'$ and

$$(A+B)^2 - 2(2^{l-1}q_2^{\alpha_2} \dots q_s^{\alpha_s}(k_1/2)^l)^2 = 1, \quad l = n/2 > 1.$$

This implies that

$$l = 2, \quad q_2^{\alpha_2} \ldots q_s^{\alpha_s} = 239, \quad A + B = 114243, \quad k_1 = 26 \tag{77}$$

or

$$l = 3, \quad q_2^{\alpha_2} \ldots q_s^{\alpha_s} = 3, \quad A + B = 17, \quad k_1 = 2. \tag{78}$$

From (73) and (77), we get $A = 80782$, $B = 33461$, and so $n = 4$, $k = 26$, $b = (33461 \cdot 239)^2$, $|U| = 7645370045$, $7645370045^2 + 4 \cdot 33461 \cdot 239 \cdot 26^2 = dV^2$. Since $a = UV$ by (67), we have $a = 7645370045|V|$. If $|V| = 1$, then from Corollary 2 we know that (2) holds since $7645370045 < 0.5 \cdot (33461 \cdot 239)^{4/3} \cdot 26^{0.29 \cdot 4}$. If $|V| > 1$, then $|V| \geq 29$ since $5 \nmid dV^2, 13 \nmid dV^2, 17 \nmid dV^2$. But $a \geq 7645370045 \cdot 29 > 0.5 \cdot (33461 \cdot 239)^{4/3} \cdot 26^{0.4226 \cdot 4}$, which contradicts our assumption.

Next, we consider (70). We have

$$(A - B)^2 - 2B^2 = -(-1)^{m'}, \quad (A + B)^2 - 2A^2 = (-1)^{m'}. \tag{79}$$

From $\sqrt{b}\, k^{n/2} = (A - B)(A + B)$, $(A - B, A + B) = 1$, we get

$$A - B = b_1 k_1^{n/2}, \quad A + B = b_2 k_2^{n/2}, \quad \sqrt{b} = b_1 b_2, \quad k = k_1 k_2,$$

where $b_1, b_2, k_1, k_2 \in \mathbb{N}$ with $(b_1, b_2) = (k_1, k_2) = 1$. Substituting these into (79), we have

$$b_1^2 k_1^{2l} - 2B^2 = -(-1)^{m'}, \quad b_2^2 k_2^{2l} - 2A^2 = (-1)^{m'}, \quad l = n/2 > 1,$$

which is impossible since $q_1 \mid b_i$ ($i = 1$ or 2) and the Legendre symbol $\left(\frac{\pm 2}{q_1}\right)$ equals -1.

Now, if $2 \nmid t$ and $t > 1$, then there is an odd prime p such that $p \mid t$. From the proof of Lemma 12, we get $a > 0.5 b^{\lambda_1} k^{\lambda_2 n}$, where $\lambda_1 \geq 2/3$, $\lambda_2 > 0.4226$ since $p \geq 3$. This contradicts our assumption. ∎

Acknowledgements. The authors would like to thank the referee for his valuable suggestions.

References

[1] E. Brown, *Diophantine equations of the form $x^2 + D = y^n$*, J. Reine Angew. Math. 274/275 (1975), 385–389.

[2] J. Buchmann and H. C. Williams, *Quadratic fields and cryptography*, in: Number Theory and Crypography, J. H. Loxton (ed.), Cambridge Univ. Press, 1990, 9–25.

[3] Z. F. Cao, *Diophantine equations and divisibility of class numbers of real quadratic fields*, Acta Math. Sinica 37 (1994), 625–631.

[4] —, *A study of some Diophantine equations*, J. Harbin Inst. Tech. 1988, no. 3, 1–7; MR 90k:11026.

[5] —, *On the Diophantine equation $x^{2n} - \mathcal{D}y^2 = 1$*, Proc. Amer. Math. Soc. 98 (1986), 11–16.

[6] Z. F. Cao, *On the Diophantine equation* $x^p - y^p = \mathcal{D}z^2$, Dongbei Shuxue 2 (1986), 219–227; MR 88b: 11013.
[7] L. K. Durst, *Exceptional real Lehmer sequences*, Pacific J. Math. 9 (1959), 437–441.
[8] —, *Exceptional real Lucas sequences*, ibid. 11 (1961), 489–494.
[9] —, *The growth of Sylvester's cyclotomic numbers*, Duke Math. J. 29 (1962), 447–454.
[10] L.-K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.
[11] M. H. Le, *Divisibility of the class number of the real quadratic field* $\mathbb{Q}\left(\sqrt{\frac{1+4k^{2n}}{a^2}}\right)$, Acta Math. Sinica 33 (1990), 565–574 (in Chinese).
[12] —, *On the generalized Ramanujan–Nagell equation* $x^2 - D = 2^{n+2}$, Trans. Amer. Math. Soc. 334 (1992), 809–825.
[13] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. 31 (1930), 419–448.
[14] W. Ljunggren, *Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positive Diskriminante*, Acta Math. 75 (1943), 1–21.
[15] —, *Über die Gleichungen* $1 + Dx^2 = 2y^2$ *und* $1 + Dx^2 = 4y^n$, Norske Vid. Selsk. Forh., Trondheim 15, 30 (1942), 115–118.
[16] —, *Zur Theorie der Gleichung* $x^2+1 = Dy^4$, Avh. Norske Vid. Akad. Oslo 5 (1942), 1–27.
[17] H. W. Lu, *The divisibility of the class number of some real quadratic fields*, Acta Math. Sinica 28 (1985), 756–762 (in Chinese).
[18] T. Nagell, *Des équations indéterminées* $x^2+x+1 = y^n$ *et* $x^2+x+1 = 3y^n$, Norsk. Mat. For. Skr. (I) 1921, no. 2, 1–14.
[19] —, *Sur l'impossibilité de quelques équations à deux indéterminées*, ibid. 1923, no. 13, 65–82.
[20] —, *Über die Klassenzahl imaginär-quadratischer Zahlkörper*, Abh. Math. Sem. Hamburg 1 (1922), 140–150.
[21] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 1990.
[22] C. Størmer, *Quelques théorèmes sur l'équation de Pell* $x^2 - Dy^2 = \pm 1$ *et leurs applications*, Videnskabs-Selskabets Skrifter 1897, no. 2, 1–48; Nyt Tidsskrift for Mat. 19 B (1908), 1–7.
[23] —, *L'équation* $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\frac{\pi}{4}$, Bull. Soc. Math. France 27 (1899), 160–170.
[24] M. Ward, *The intrinsic divisors of Lehmer numbers*, Ann. of Math. (2) 62 (1955), 230–236.
[25] Ping Zhi Yuan, *The divisibility of the class numbers of real quadratic fields*, Acta Math. Sinica 41 (1998), 525–530.
[26] P. Yuan, *Some basic problems in Diophantine equations*, Ph.D. thesis, Sichuan University, 1997.

Department of Mathematics
Harbin Institute of Technology
Harbin 150001, P.R. China
E-mail: zfcao@hope.hit.edu.cn

Received on 23.11.1998
and in revised form on 19.7.2000 (3520)