A note on the divisibility of class numbers of imaginary quadratic fields $\mathbf{Q}(\sqrt{a^2 - k^n})$

By Akiko ITO*)

Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya, Aichi 464-8602, Japan

(Communicated by Heisuke HIRONAKA, M.J.A., Oct. 12, 2011)

Abstract: Let $n > 1$ be an integer, $k > 1$ be an odd integer and $a > 0$ be an even integer. Suppose $a^2 + b^2 d = k^n$, where $d \neq 1, 3$ is a positive odd square-free integer and $\gcd(a, bd) = 1$. In this paper, we describe imaginary quadratic fields $\mathbf{Q}(\sqrt{a^2 - k^n})$ explicitly whose class numbers are divisible by n if $d \equiv 1, 5, 7 \bmod 8$ or $d \equiv 3 \bmod 8$ with $(n, 3) = 1$ under certain conditions.

Key words: Class numbers; imaginary quadratic fields; primitive divisors of Lucas numbers.

1. Introduction. Let $n \geq 3$, and $D \geq 63$ be a square-free integer such that $t^2 D = K^n - x^2$. Here t, K, x are positive integers with $(K, 2x) = 1$. By Mollin [Mo], Murty [Mu1], [Mu2] and Soundararajan [So], it is known that if $K^n < (D+1)^2$, then $n \mid h(-D)$, where $h(-D)$ denotes the class number of imaginary quadratic fields $\mathbf{Q}(\sqrt{-D})$. In this paper, we consider whether $n \mid h(-D)$ is satisfied or not without the condition $K^n < (D+1)^2$. By using a result on the primitive divisors of Lucas numbers, we prove the following.

Theorem 1.1. *Let $n > 1$ be an integer, $k > 1$ be an odd integer and $a > 0$ be an even integer. Suppose $a^2 + b^2 d = k^n$, where $d \neq 1, 3$ is a positive odd square-free integer, $b > 0$ and $gcd(a, bd) = 1$. And assume $b \mid^* d$. The condition $b \mid^* d$ denotes all prime factors of b divide d.*
(1) *If $d \equiv 1, 5, 7 \bmod 8$ and the following conditions* (i), (ii), (iii) *are not satisfied, then $n \mid h(-d)$.*

(i) $(a, b, d, k, n) = (2759646, 1, 341, 377, 5)$,

(ii) $(a, b^2 d, k, n) =$

$$\left(\frac{m}{2} \cdot (2m^2 + \varepsilon \cdot 3), \frac{3m^2 + \varepsilon \cdot 4}{4}, m^2 + \varepsilon, 3\right),$$

where $m > 0$ with $m \equiv 0 \bmod 4$ and $\varepsilon = \pm 1$,

(iii) $$(a, b^2 d, k^n) = \left(\frac{m}{2} \cdot \mid -2m^2 + \varepsilon \cdot 3^{l+1} \mid, 3^{2l} \cdot \frac{3m^2 - \varepsilon \cdot 4 \cdot 3^l}{4}, (m^2 - \varepsilon \cdot 3^l)^3\right),$$

where $m > 0$ with $m \not\equiv 0 \bmod 3$ and $m \equiv 0 \bmod 4$, $l > 0$ and $\varepsilon = \pm 1$. In the case (i)*, we have $5 \nmid h(-341) = 28$ and, in the two cases* (ii) *and* (iii)*, we have $n/3 \mid h(-d)$.*
(2.1) *If $d \equiv 3 \bmod 8$ and $(n, 3) = 1$, then $n \mid h(-d)$ except the case*

$$(a, b, d, k, n) = (22434, 1, 19, 55, 5).$$

In fact, we have $5 \nmid h(-19) = 1$.
(2.2) *If $d \equiv 3 \bmod 8$ and $(n, 3) \neq 1$, then $n/3 \mid h(-d)$.*

The method of the proof of this theorem is based on the result of Cao [Ca2].

Remark 1. If $b = 1$, the condition $b \mid^* d$ is always satisfied. Therefore, this theorem contains the case where $a^2 - k^n < 0$ is square-free.

The above theorem implies that we can describe imaginary quadratic fields $\mathbf{Q}(\sqrt{a^2 - k^n})$ explicitly whose class numbers may not be divisible by n under the conditions when $b \mid^* d$, $2 \mid a$, $2 \nmid k$ and $\gcd(a, bd) = 1$.

Example. (A.1) For the Case (ii) and (iii) of Theorem 1.1 (1), examples with $n/3 \mid h(-d)$ and $n \nmid h(-d)$ exist.
(A.1.1) For $m = 4$ in Case (ii) of Theorem 1.1 (1), we have

$$(a, b, d, k, n) = \begin{cases} (70, 1, 13, 17, 3) & \text{if } \varepsilon = 1 \\ (58, 1, 11, 15, 3) & \text{if } \varepsilon = -1. \end{cases}$$

2000 Mathematics Subject Classification. Primary 11R11, 11R29, 11D61.
*) Research Fellow of the Japan Society for the Promotion of Science.

doi: 10.3792/pjaa.87.151

In these cases, we have $1 = 3/3 \mid h(-13) = 2$ and $3 \nmid h(-13)$, $1 = 3/3 \mid h(-11) = 1$ and $3 \nmid h(-11)$ respectively.

(A.1.2) For $m = 16$, $l = 2$, $\varepsilon = 1$ in Case (iii) of Theorem 1.1 (1), we have

$$(a, b, d, k, n) = (3880, 9, 183, 247, 3).$$

In this case, we have $1 = 3/3 \mid h(-183) = 8$ and $3 \nmid h(-183)$. For $m = 4$, $l = 2$, $\varepsilon = -1$, $k = 5$ in Case (iii) of Theorem 1.1 (1), we have

$$(a, b, d, k, n) = (118, 9, 21, 5, 6).$$

In this case, we have $2 = 6/3 \mid h(-21) = 4$ and $6 \nmid h(-21)$.

(A.2) For the Case (ii) and (iii) of Theorem 1.1 (1), examples with $n \mid h(-d)$ exist.

(A.2.1) For $m = 12$ in Case (ii) of Theorem 1.1 (1), we have

$$(a, b, d, k, n) = \begin{cases} (1746, 1, 109, 145, 3) & \text{if } \varepsilon = 1 \\ (1710, 1, 107, 143, 3) & \text{if } \varepsilon = -1. \end{cases}$$

In these cases, we have $3 \mid h(-109) = 6$ and $3 \mid h(-107) = 3$ respectively.

(A.2.2) For $m = 32$, $l = 2$, $\varepsilon = 1$ in Case (iii) of Theorem 1.1 (1), we have

$$(a, b, d, k, n) = (32336, 9, 759, 1015, 3).$$

In this case, we have $3 \mid h(-759) = 24$. For $m = 16$, $l = 2, \varepsilon = -1$ in Case (iii) of Theorem 1.1 (1), we have

$$(a, b, d, k, n) = (4312, 9, 201, 265, 3).$$

In this case, we have $3 \mid h(-201) = 12$.

(B.1) For Theorem 1.1 (2.2), an example with $n/3 \mid h(-d)$ and $n \nmid h(-d)$ exists. For the case when $(a, b, d, k, n) = (4, 1, 11, 3, 3)$, we have $3/3 \mid h(-11) = 1$ and $3 \nmid h(-11)$.

(B.2) For Theorem 1.1 (2.2), an example with $n \mid h(-d)$ exists. For the case when $(a, b, d, k, n) = (2, 1, 339, 7, 3)$, we have $3 \mid h(-339) = 6$.

2. Preliminaries.

Lemma 2.1. *Let $k > 1$, y be odd integers and $x > 0$ be an even integer. Suppose $x^2 + y^2 D = k^z$, where $D \neq 1, 3$ is a positive square-free integer,* $\gcd(D, k) = \gcd(x, y) = 1$ *and $z > 1$.*

(1) *If $-D \equiv 3 \bmod 4$, then we have*

$$x + y\sqrt{-D} = \pm(X_1 + Y_1\sqrt{-D})^t,$$
$$z = z_1 t \ (z_1 > 0),$$

where X_1, Y_1, z_1 are integers such that $X_1^2 + DY_1^2 = k^{z_1}$, $\gcd(X_1, Y_1) = 1$ *and $h(-D) \equiv 0 \bmod z_1$.*

(2) *If $-D \equiv 1 \bmod 4$, then we have*

$$x + y\sqrt{-D} = \pm\left(\frac{X_1 + Y_1\sqrt{-D}}{2}\right)^t,$$
$$z = z_1 t \ (z_1 > 0),$$

where X_1, Y_1, z_1 are integers such that $X_1^2 + DY_1^2 = 4k^{z_1}$, $X_1 \equiv Y_1 \bmod 2$ and $h(-D) \equiv 0 \bmod z_1$.

Proof. We can prove this in a way similar to the proof of [Ca1, Lemma 1]. (1) Since $x^2 + y^2 D = k^z$, we have

$$(x + y\sqrt{-D})(x - y\sqrt{-D}) = k^z.$$

From $\gcd(D, k) = \gcd(x, y) = 1$, $x + y\sqrt{-D}$ and $x - y\sqrt{-D}$ are coprime integers of $\mathcal{O}_{\mathbf{Q}(\sqrt{-D})}$. Then, we can write

$$(x + y\sqrt{-D}) = A^z$$

for some ideal A of the field $\mathbf{Q}(\sqrt{-D})$. Let $z_1 := \gcd(h(-D), z)$. We can write $z_1 = ih(-D) + jz$ for some $i, j \in \mathbf{Z}$ and we have

$$A^{z_1} = (A^{h(-D)})^i \cdot (A^z)^j \sim (1)^i \cdot (1)^j \sim (1).$$

This implies that A^{z_1} is a principal ideal and we obtain

$$A^{z_1} = (X_1 + Y_1\sqrt{-D})$$

for some X_1, $Y_1 \in \mathbf{Z}$. Since $\gcd(h(-D), z) = z_1$, we have $z = z_1 t$ for some $t \in \mathbf{Z}$. Then, we obtain

$$(x + y\sqrt{-D}) = (A^{z_1})^t = (X_1 + Y_1\sqrt{-D})^t.$$

The assumption $D \neq 1, 3$ implies $\mathcal{O}^\times_{\mathbf{Q}(\sqrt{-D})} = \{\pm 1\}$. Therefore, we have

$$x + y\sqrt{-D} = \pm(X_1 + Y_1\sqrt{-D})^t.$$

(2) We can obtain a proof in a way similar to the above case. Since $-D \equiv 1 \bmod 4$, we have $\mathcal{O}_{\mathbf{Q}(\sqrt{-D})} = \mathbf{Z}[\frac{1+\sqrt{-D}}{2}]$. Then, we obtain

$$A^{z_1} = \left(\frac{X_1 + Y_1\sqrt{-D}}{2}\right)$$

for some X_1, $Y_1 \in \mathbf{Z}$ with $X_1 \equiv Y_1 \bmod 2$. From this and $\mathcal{O}^\times_{\mathbf{Q}(\sqrt{-D})} = \{\pm 1\}$, we have

$$x + y\sqrt{-D} = \pm\left(\frac{X_1 + Y_1\sqrt{-D}}{2}\right)^t.$$

□

Lemma 2.2 (C. Ko [Ko] and V. A. Lebesgue (cf. [Ca2, Lemma 3.7])). *The equation $x^2 - \lambda = y^n$, $n > 1$, $\lambda = \pm 1$ has the only positive integer solution $(x, y, n, \lambda) = (3, 2, 3, 1)$.*

Lemma 2.3 (R. Stanley [St, Theorem 8a, Theorem 14a])**.**
(1) *The equation* $y^2 - 3^m = x^3$, $(x,3) = 1$, $m, y \geq 0$ *has just five integer solutions* $(m,x,y) = (0,-1,0)$, $(0,2,3)$, $(1,1,2)$, $(2,-2,1)$ *and* $(2,40,253)$.
(2) *The equation* $y^2 + 3^m = x^3$, $(x,3) = 1$, m, $y \geq 0$ *has just three integer solutions* $(m,x,y) = (0,1,0)$, $(4,13,46)$ *and* $(5,7,10)$.

A *Lucas pair* is a pair (A,B) of algebraic integers such that $A+B$ and AB are non-zero coprime rational integers and A/B is not a root of unity. Given a Lucas pair (A,B), the corresponding sequence of Lucas numbers is defined by

$$u_n = u_n(A,B) = \frac{A^n - B^n}{A - B},$$

where $n \in \mathbf{N} \cup \{0\}$. Let (A,B) be a Lucas pair. A prime number p is a *primitive divisor of the Lucas number* $u_n(A,B)$ if p divides u_n but does not divide $(A-B)^2 u_1 \cdots u_{n-1}$. We say that a Lucas number is an *n-defective Lucas number* if $u_n(A,B)$ has no primitive divisor.

Lemma 2.4 (Y. Bilu, G. Hanrot and P. M. Voutier [BHV])**.** *For any integer $n > 30$, every Lucas number is no n-defective. Further, for any positive integer $n \leq 30$, all n-defective Lucas numbers are explicitly determined.*

All n-defective $(n > 1)$ Lucas numbers are given in [BHV, Table 1, 3] and [Mou, Theorem 4.1]. By [BHV, Remark 1.1, Proposition 2.1(i) and Corollary 2.2], we also obtain the following (cf. [Ca2, Lemma 3.4]).

Lemma 2.5. *If p is a primitive divisor of the Lucas number $u_n(A,B)$, then $n \equiv \pm 1 \mod p$.*

We use these results for the proof of Theorem 1.1 mainly.

3. Proof of Theorem 1.1.

Case 1 ($d \equiv 1 \mod 4$)**.** By Lemma 2.1 (1), we have

$$a + b\sqrt{-d} = \pm(x_1 + y_1\sqrt{-d})^r, \quad n = z_1 r,$$

where x_1, y_1, z_1 are integers such that $x_1^2 + y_1^2 d = k^{z_1}$, $gcd(x_1, y_1 d) = 1$, $z_1 > 0$ and $h(-d) \equiv 0 \mod z_1$. If r is even, we can write $r = 2r'$ $(r' \in \mathbf{Z})$. We have

$$a + b\sqrt{-d} = \pm(\alpha^2 - d\beta^2) \pm 2\alpha\beta\sqrt{-d},$$

where $(x_1 + y_1\sqrt{-d})^{r'} = \alpha + \beta\sqrt{-d}$ $(\alpha,\ \beta \in \mathbf{Z})$. This is a contradiction with $2 \nmid b$. Then, we obtain $2 \nmid r$. Let $\varepsilon := |x_1| + |y_1| \cdot \sqrt{-d}$ and $\overline{\varepsilon} := |x_1| - |y_1| \cdot \sqrt{-d}$. Then, we have

$$b = \left|\frac{\overline{\varepsilon}^r - \varepsilon^r}{\overline{\varepsilon} - \varepsilon}\right| \cdot |y_1|.$$

Let

$$b_1 := \left|\frac{\overline{\varepsilon}^r - \varepsilon^r}{\overline{\varepsilon} - \varepsilon}\right|.$$

By $b = b_1 \cdot |y_1|$ and $b \mid^* d$, we have $b_1 \mid^* d$. We obtain that $\frac{\overline{\varepsilon}^r - \varepsilon^r}{\overline{\varepsilon} - \varepsilon}$ satisfies the definition of the r-th Lucas number. We have

$$b_1 = \left|\binom{r}{1}|x_1|^{r-1} + \binom{r}{3}|x_1|^{r-3} \cdot (|y_1| \cdot \sqrt{-d})^2 + \cdots + \binom{r}{r}(|y_1| \cdot \sqrt{-d})^{r-1}\right|.$$

For any prime number q with $q \mid b_1$, we have $q \mid d$ by $b_1 \mid^* d$. Then, we obtain $b_1 \equiv r x_1^{r-1} \equiv 0 \mod q$. Since $(x_1, y_1 d) = 1$, we have $q \nmid x_1$, that is, $q \mid r$. By Lemma 2.5, this implies that $\frac{\overline{\varepsilon}^r - \varepsilon^r}{\overline{\varepsilon} - \varepsilon}$ has no primitive divisors. By Lemma 2.4, [BHV, Table 1, 3] and [Mou, Theorem 4.1], we have $r = 1, 3, 5$. For $r = 5$, we obtain $(2|x_1|, -4y_1^2 d) = (12, -1364)$, that is, $(a,b,d,k,n) = (2759646, 1, 341, 377, 5)$. For $r = 3$, we obtain (I) $(2|x_1|, -4y_1^2 d) = (m, -4-3m^2)$, (II) $(2|x_1|, -4y_1^2 d) = (m, 4-3m^2)$ with $m > 1$, (III) $(2|x_1|, -4y_1^2 d) = (m, 4 \cdot 3^l \cdot \varepsilon - 3m^2)$ with $m > 0$, $m \not\equiv 0 \mod 3$, $l > 0$, $\varepsilon = \pm 1$ and $(\varepsilon, k, m) \neq (1,1,2)$. For the case (I), we have $m^2 + 1 = k^{z_1}$. By Lemma 2.2, we get $z_1 = 1$, that is, $n = 3$. Since $a + b\sqrt{-d} = \pm(x_1 + y_1\sqrt{-d})^3$ and $y_1^2 d = 1 + \frac{3}{4}m^2$, we obtain $b_1 = 1$, that is, $b^2 d = y_1^2 d = 1 + \frac{3}{4}m^2$. By $a = \pm x_1(x_1^2 - 3y_1^2 d)$, $|x_1| = \frac{m}{2} > 0$, we obtain $a = \frac{m}{2}(2m^2 + 3)$. For the case (II), (III), we can obtain a, $b^2 d$, k^{z_1} in a way similar to the case (I) by using Lemma 2.2. Since a is even and

$$a = \frac{m}{2} \cdot (2m^2 + \varepsilon \cdot 3) \quad \text{or} \quad \frac{m}{2} \cdot |-2m^2 + \varepsilon \cdot 3^{l+1}|,$$

we have $m \equiv 0 \mod 4$. Therefore, the condition $(\varepsilon, k, m) \neq (1,1,2)$ of the case (III) is not needed. For $r = 1$, we have $n = z_1$. From this and $h(-d) \equiv 0 \mod z_1$, we obtain $n \mid h(-D)$.

Case 2 ($d \equiv 7 \mod 8$)**.** We use the following result.

Lemma 3.1 (Y. Kishi [Ki] and A. Ito [It])**.**
(1) *If $d \equiv 3 \mod 8$, for any integer $s > 0$,*

$$\left(\frac{u + v\sqrt{-d}}{2}\right)^s \in \mathbf{Z}[\sqrt{-d}] \Leftrightarrow 3 \mid s,$$

where $u \equiv v \equiv 1 \mod 2$.
(2) *If $d \equiv 7 \mod 8$, for any integer $s > 0$,*

$$\left(\frac{u+v\sqrt{-d}}{2}\right)^s \notin \mathbf{Z}[\sqrt{-d}],$$

where $u \equiv v \equiv 1 \bmod 2$.

Proof. The statement (1) is contained in [Ki, p.190]. The proof is easy. To show (2), it is enough to show that

$$\frac{1}{2}\left\{\left(\frac{u+v\sqrt{-d}}{2}\right)^s + \left(\frac{u-v\sqrt{-d}}{2}\right)^s\right\} \notin \mathbf{Z}$$

for any integer $s > 0$. The following argument is contained in [It], but we reproduce it here for the convenience of readers. Since $-d \equiv 1 \bmod 8$, we can consider $\sqrt{-d} \in \mathbf{Z}_2^\times$, where $\mathbf{Z}_2^\times$ denotes the unit group of the ring $\mathbf{Z}_2$ of 2-adic integers. Then, to show the above statement is equivalent to show that

$$\frac{1}{2}\left\{\left(\frac{u+v\sqrt{-d}}{2}\right)^s + \left(\frac{u-v\sqrt{-d}}{2}\right)^s\right\} \notin \mathbf{Z}_2.$$

Since $\sqrt{-d} \equiv 1 \bmod 2\mathbf{Z}_2$ and v is odd, we have $v\sqrt{-d} \equiv 1,\ 3 \bmod 4\mathbf{Z}_2$. By checking four cases $(u, v\sqrt{-d}) = (\bar{1},\bar{1}),\ (\bar{1},\bar{3}),\ (\bar{3},\bar{1}),\ (\bar{3},\bar{3})$, where $u = \bar{j}$ denotes $u \equiv j \bmod 4\mathbf{Z}_2$, we obtain $\frac{u+v\sqrt{-d}}{2} \not\equiv \frac{u-v\sqrt{-d}}{2} \bmod 2\mathbf{Z}_2$. Then, we have

$$\left(\frac{u+v\sqrt{-d}}{2}\right)^s + \left(\frac{u-v\sqrt{-d}}{2}\right)^s \equiv 1 \bmod 2\mathbf{Z}_2,$$

that is,

$$\frac{1}{2}\left\{\left(\frac{u+v\sqrt{-d}}{2}\right)^s + \left(\frac{u-v\sqrt{-d}}{2}\right)^s\right\} \notin \mathbf{Z}_2.$$

□

Since $d \equiv 7 \bmod 8$, we have $-d \equiv 1 \bmod 4$. By Lemma 2.1 (2), we can write

$$a + b\sqrt{-d} = \pm\left(\frac{x_1 + y_1\sqrt{-d}}{2}\right)^r$$

for some $x_1, y_1 \in \mathbf{Z}$ with $x_1 \equiv y_1 \bmod 2$. From this and Lemma 3.1 (2), we obtain $x_1 \equiv y_1 \equiv 0 \bmod 2$. This case is reduced to considering the same power root of $a + b\sqrt{-d}$ in $\mathbf{Z}[\sqrt{-d}]$ as in Case 1 and we may check the case $r = 1, 3, 5$ in the same way to Case 1.

Case 3 ($d \equiv 3 \bmod 8$)**.** Since $d \equiv 3 \bmod 8$, we obtain $-d \equiv 1 \bmod 4$. By Lemma 2.1 (2), we have

$$a + b\sqrt{-d} = \pm\left(\frac{x_1 + y_1\sqrt{-d}}{2}\right)^r,$$
$$n = z_1 r\ (z_1 > 0),$$

where x_1, y_1, z_1 are integers such that $x_1^2 + dy_1^2 = 4k^{z_1}$, $x_1 \equiv y_1 \bmod 2$ and $h(-d) \equiv 0 \bmod z_1$. We consider two cases when $3 \nmid r$ or $3 \mid r$ respectively.

Case 3-1 ($d \equiv 3 \bmod 8$ and $3 \nmid r$)**.** Form $x_1 \equiv y_1 \bmod 2$ and Lemma 3.1 (1), we obtain $x_1 \equiv y_1 \equiv 0 \bmod 2$. This case is reduced to considering the same power root of $a + b\sqrt{-d}$ in $\mathbf{Z}[\sqrt{-d}]$ as in Case 1 and we may check the case $r = 1, 3, 5$ in the same way to Case 1.

Case 3-2 ($d \equiv 3 \bmod 8$ and $3 \mid r$)**.** From Lemma 3.1 (1) and $x_1 \equiv y_1 \bmod 2$, two cases when $x_1 \equiv y_1 \equiv 0 \bmod 2$ and $x_1 \equiv y_1 \equiv 1 \bmod 2$ are possible. We consider these cases respectively. If $x_1 \equiv y_1 \equiv 0 \bmod 2$, this case is reduced to considering the same power root of $a + b\sqrt{-d}$ in $\mathbf{Z}[\sqrt{-d}]$ as in Case 1. We may check the case $r = 1, 3, 5$ in the same way to Case 1. Next, we consider the case when $x_1 \equiv y_1 \equiv 1 \bmod 2$. By the assumption $3 \mid r$, we have $r = 3r'$ for some integer r'. Therefore, we obtain

$$a + b\sqrt{-d} = \pm\left(\frac{x_1 + y_1\sqrt{-d}}{2}\right)^{3r'}.$$

By Lemma 3.1 (1), we can write

$$\left(\frac{x_1 + y_1\sqrt{-d}}{2}\right)^3 = \gamma + \delta\sqrt{-d}$$

for some integers γ and δ. This implies that

$$a + b\sqrt{-d} = \pm(\gamma + \delta\sqrt{-d})^{r'},$$
$$n = 3r'z_1.$$

This case is reduced to considering the same power root of $a + b\sqrt{-d}$ in $\mathbf{Z}[\sqrt{-d}]$ as in Case 1 and we may check the case $r' = 1, 3, 5$. If $r' = 1$, $z_1 = n/3 \mid h(-d)$. If $r' = 5$, we have $k^{3z_1} = 55$. This is impossible. Next, we consider when $r' = 3$. In the cases (I), (II) of Case 1, we have $m^2 \pm 1 = k^{3z_1}$. By Lemma 2.2 and $2 \nmid k$, this is impossible. In the case (III) of Case 1, we have $m^2 \pm 3^l = k^{3z_1}$. By Lemma 2.3 (1), $l > 0$, $k > 1$ and $2 \nmid k$, $m^2 - 3^l = k^{3z_1}$ is impossible. By Lemma 2.3 (2) and $l > 0$, the equation $m^2 + 3^l = k^{3z_1}$ has two integer solutions $(l, k^{z_1}, m) = (4, 13, 46), (5, 7, 10)$. We obtain $b^2 d = 3^{2l} \cdot \left(\frac{3m^2 \pm 4\cdot 3^l}{4}\right)$ in a way similar to the case (I) of Case 1. If $(l, k^{z_1}, m) = (4, 13, 46), (5, 7, 10)$, $b^2 d$ is even. This is a contradiction with $2 \nmid b^2 d$. Then, these cases are impossible. The proof of Theorem 1.1 is completed.

Acknowledgments. The author would like to thank Prof. Kohji Matsumoto for his valuable advice and continuous encouragement. Further, she thanks the referee for careful reading and several useful comments. This research was supported by Grant-in-Aid for JSPS Fellows (22-222) from Japan Society for the Promotion of Science.

References

[BHV] Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, J. Reine Angew. Math. **539** (2001), 75–122.

[Ca1] Z. F. Cao, Divisibility of the class numbers of imaginary quadratic fields, Acta Math. Sinica **37** (1994), no. 1, 50–56.

[Ca2] Z. F. Cao, The divisibility of the class number of imaginary quadratic fields, Chinese Ann. Math. Ser. A **25** (2004), no. 3, 397–406.

[It] A. Ito, Remarks on the divisibility of the class numbers of imaginary quadratic fields $\mathbf{Q}(\sqrt{2^{2k} - q^n})$, Glasg. Math. J. **53** (2011), no. 2, 379–389.

[Ki] Y. Kishi, Note on the divisibility of the class number of certain imaginary quadratic fields, Glasg. Math. J. **51** (2009), no. 1, 187–191; Corrigendum, Glasg. Math. J. **52** (2010), no. 1, 207–208.

[Ko] C. Ko, On the Diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, Sci. Sinica **14** (1965), 457–460.

[Mo] R. A. Mollin, Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields, Glasg. Math. J. **38** (1996), no. 2, 195–197.

[Mou] M. Abouzaid, Les nombres de Lucas et Lehmer sans diviseur primitif (in French) [Lucas and Lehmer numbers with no primitive divisors], J. Théor. Nombres Bordeaux **18** (2006), no. 2, 299–313.

[Mu1] M. R. Murty, The *abc* conjecture and exponents of class groups of quadratic fields, in *Number theory* (*Tiruchirapalli,* 1996), 85–95, Contemp. Math., **210**, Amer. Math. Soc., Providence, RI, 1998.

[Mu2] M. R. Murty, Exponents of class groups of quadratic fields, in *Topics in number theory* (*University Park, PA,* 1997), 229–239, Math. Appl., **467**, Kluwer Acad. Publ., Dordrecht, 1999.

[So] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, J. London Math. Soc. (2) **61** (2000), no. 3, 681–690.

[St] R. Stanley, On Mordell's equation $y^2 + k = x^3$, with $k = \pm 2^n 3^m$, Doctoral dissertation, The City Univ. of New York, 1971.