Glasgow Math. J. **53** (2011) 379–389. © Glasgow Mathematical Journal Trust 2011.
doi:10.1017/S0017089511000012.

REMARKS ON THE DIVISIBILITY OF THE CLASS NUMBERS OF IMAGINARY QUADRATIC FIELDS $\mathbb{Q}(\sqrt{2^{2k} - q^n})$

AKIKO ITO

Graduate School of Mathematics, Nagoya University, Chikusa-ku, Nagoya 464-8602, Japan
e-mail: m07004a@math.nagoya-u.ac.jp

(Received 5 April 2009; revised 4 July 2010; accepted 30 November 2010)

Abstract. We consider the divisibility of the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - q^n})$, where q is an odd prime number, k and n are positive integers. Suppose that $k \equiv 1 \bmod 2$ or $n \not\equiv 3 \bmod 6$. We show that the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - q^n}) \neq \mathbb{Q}(\sqrt{-3})$ are divisible by n for $q \equiv 3 \bmod 8$. This is a generalization of the result of Kishi for imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ when $k \equiv 1 \bmod 2$ or $n \not\equiv 3 \bmod 6$. We also show that the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - q^n}) \neq \mathbb{Q}(\sqrt{-1})$ are divisible by n for $q \equiv 1 \bmod 4$ and the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - q^n}) \neq \mathbb{Q}(\sqrt{-3})$ are divisible by n for $q \equiv 7 \bmod 8$.

2010 *Mathematics Subject Classification.* 11R11, 11R29.

1. Introduction. In [**7**] and [**1**], it was proved that for any positive integer n, there exist infinitely many imaginary quadratic fields whose class numbers are divisible by n. Their proofs were given by constructing such quadratic fields explicitly. We begin with the result of Ankeny–Chowla.

THEOREM A (Ankeny–Chowla [**1**, Theorem 1]). *Let n be a positive even integer and $d := x^2 - 3^n < 0$ be a square-free integer with $2 \mid x$ and $0 < x < (2 \cdot 3^{n-1})^{\frac{1}{2}}$. Then the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{d})$ are divisible by n.*

Next, we state the following theorem related with Theorem A.

THEOREM B. *For any positive integers k and n with $2^{2k} < 3^n$and $(n, k) \neq (3, 2)$, the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ are divisible by n.*

This theorem was proved by Kishi. (See [**5**, Theorem 1.2] and [**6**, Theorem].) In his paper, it is written that the aim of [**5**, Theorem 1.2] is to remove the condition ‘square-free’ in Theorem A for the case when x is a power of two. Our aim is to prove the same type of his result for the divisibility of the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - q^n})$, where q is any odd prime number. We obtain the following theorem that is a generalization of Theorem B for imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ when $k \equiv 1 \bmod 2$ or $n \not\equiv 3 \bmod 6$.

THEOREM 1. *Let q be an odd prime number, n and k be positive integers with $2^{2k} < q^n$.*

(1) *For the case $q \equiv 3 \bmod 8$, if n and k satisfy either* (i) $k \equiv 1 \bmod 2$ *or* (ii) $n \not\equiv 3 \bmod 6$, *then the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k} - q^n})$ except $\mathbb{Q}(\sqrt{-3})$ are divisible by n.*

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

(2) *For the case* $q \equiv 1 \bmod 4$, *the class numbers of imaginary quadratic fields* $\mathbb{Q}(\sqrt{2^{2k} - q^n})$ *except* $\mathbb{Q}(\sqrt{-1})$ *are divisible by n.*

(3) *For the case* $q \equiv 7 \bmod 8$, *the class numbers of imaginary quadratic fields* $\mathbb{Q}(\sqrt{2^{2k} - q^n})$ *except* $\mathbb{Q}(\sqrt{-3})$ *are divisible by n.*

From this theorem, we obtain two corollaries. When $q \equiv 11, 23 \bmod 24$, we can show $\mathbb{Q}(\sqrt{2^{2k} - q^n}) \neq \mathbb{Q}(\sqrt{-3})$.

Corollary 1. *Let q be an odd prime number such that* $q \equiv 11, 23 \bmod 24$, *n and k be positive integers with* $2^{2k} < q^n$. *For* $q \equiv 11 \bmod 24$, *if* $k \equiv 1 \bmod 2$ *or* $n \not\equiv 3 \bmod 6$, *then the class numbers of imaginary quadratic fields* $\mathbb{Q}(\sqrt{2^{2k} - q^n})$ *are divisible by n. For* $q \equiv 23 \bmod 24$, *the class numbers of imaginary quadratic fields* $\mathbb{Q}(\sqrt{2^{2k} - q^n})$ *are divisible by n.*

When n is even, we can also obtain $\mathbb{Q}(\sqrt{2^{2k} - q^n}) \neq \mathbb{Q}(\sqrt{-3})$ for any positive integers k, where $q \equiv 3 \bmod 4$ is a prime number.

Corollary 2. *Let q be an odd prime number such that* $q \equiv 3 \bmod 4$ *and n be a positive even integer. For any positive integers k with* $2^{2k} < q^n$, *the class numbers of imaginary quadratic fields* $\mathbb{Q}(\sqrt{2^{2k} - q^n})$ *are divisible by n.*

To show Theorem 1, it is essential to construct an ideal of $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$ such that the order of the ideal class is n and we approach this point as follows. Let

$$\alpha := 2^k + \sqrt{2^{2k} - q^n} \in \mathbb{Q}\left(\sqrt{2^{2k} - q^n}\right),$$

where q is an odd prime integer, $n \geq 1$, and $k \geq 1$ are integers with $2^{2k} < q^n$. Since $\alpha \in O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$, $N(\alpha) = q^n$, $(q, 2^{2k} - q^n) = 1$ and $q \nmid \alpha$, it follows that

$$(\alpha) = \wp^n$$

for some ideal $\wp$ of $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$, where N denotes the norm. Then, the order of the ideal class $[\wp]$ divides n and we will show the order of $[\wp]$ is n. To prove it, it is important to show that $\pm\alpha$ is not a pth power in $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$ for any prime p dividing n (see Lemma 4).

This paper is organized as follows. In Section 2, we state a result of Bugeaud–Shorey on positive integer solutions of some Diophantine equation. In Section 3, we prepare some lemmas for the proof of Theorem 1. By using the result of Bugeaud–Shorey, we show that the number of positive integer solutions (x, y) of the equation $D_1x^2 + 2^{2k} = q^y$ is at most one except for $(D_1, k, q) = (1, 1, 5)$, where D_1 is an odd positive integer (see Lemma 3). This is necessary to prove that $\pm\alpha$ is not a pth power in $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$. In Section 4, we prove Theorem 1 and Corollaries 1, 2. In Section 5, we state a remark on Theorem 1 (1) for the case when $n \equiv 3 \bmod 6$ and $k \equiv 0 \bmod 2$. We obtain an example that the class number of the field $\mathbb{Q}(\sqrt{2^{2k} - q^n})$ is not divisible by n when $q = 11$ (see Example in Section 5).

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

Remark. Imaginary quadratic fields (whose class numbers are divisible by a given positive integer) that are constructed in [**3**, **4**] also do not have the 'square-free' condition.

2. A result of Bugeaud–Shorey. We state a result of Bugeaud–Shorey ([**2**, Theorem 1)] which is necessary in Section 3.

We define the sets $\mathcal{F}, \mathcal{G}, \mathcal{H}_\lambda \subset \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ by

$$\mathcal{F} := \{(F_{k-2\varepsilon}, L_{k+\varepsilon}, F_k) \mid k \geq 2, \varepsilon \in \{\pm 1\}\},$$

$$\mathcal{G} := \{(1, 4p^r - 1, p) \mid p \text{ is an odd prime}, r \geq 1\},$$

$$\mathcal{H}_\lambda := \left\{ (D_1, D_2, p) \;\middle|\; \begin{array}{c} \text{there exist positive integers } r, s, D_1, D_2 \\ \text{and an odd prime } p \text{ with } \gcd(D_1, D_2) = 1, \\ p \nmid D_1 D_2 \text{ such that } D_1 s^2 + D_2 = \lambda^2 p^r \\ \text{and } 3D_1 s^2 - D_2 = \pm\lambda^2 \end{array} \right\},$$

where F_n denotes the nth number in the Fibonacci sequence defined by $F_0 := 0, F_1 := 1, F_{n+2} := F_{n+1} + F_n\,(n \geq 0)$ and L_n denotes the nth number in the Lucas sequence defined by $L_0 := 2, L_1 := 1, L_{n+2} := L_{n+1} + L_n\,(n \geq 0)$.

Theorem C (Bugeaud–Shorey [**2**, Theorem 1]). *For any given $\lambda \in \{1, \sqrt{2}, 2\}$, a prime p and positive coprime integers D_1 and D_2, the number of positive integer solutions (x, y) of the equation*

$$D_1 x^2 + D_2 = \lambda^2 p^y$$

is at most one except for

$$(\lambda, D_1, D_2, p) \in \mathcal{E} := \left\{ \begin{array}{c} (2, 13, 3, 2), (\sqrt{2}, 7, 11, 3), (1, 2, 1, 3), (2, 7, 1, 2), \\ (\sqrt{2}, 1, 1, 5), (\sqrt{2}, 1, 1, 13), (2, 1, 3, 7) \end{array} \right\}$$

and

$$(D_1, D_2, p) \in \mathcal{F} \cup \mathcal{G} \cup \mathcal{H}_\lambda.$$

3. Some lemmas for the proof of Theorem 1. Our aim of this section is to show Lemma 4 which is essential for the proof of our theorem. We prepare some lemmas for the proof of Lemma 4.

Let q be an odd prime number.

Lemma 1. *The equation*

$$2^x - 3q^y = -1$$

has no positive integer solutions (x, y) with x even.

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

Proof. Suppose the equation has a positive integer solution (x, y). We obtain

$$2^x = 3q^y - 1 \equiv -1 \equiv 2 \bmod 3.$$

If $2^x \equiv 2 \bmod 3$, then the positive integer x is odd. □

Lemma 2. *The equation*

$$2^x - 3q^y = 1$$

has no positive integer solutions (x, y) *except for* $(q, x, y) = (5, 4, 1)$.

Proof. Suppose $x = 1, 2$. The equations $2^1 = 3q^y + 1$, $2^2 = 3q^y + 1$ have no solution because q is a prime number. Next, we consider the case when $x \geq 3$. If the equation has a positive integer solution (x, y), we have

$$3q^y = 2^x - 1 \equiv 0 \bmod 3.$$

Then, we obtain $x \equiv 0 \bmod 2$. We write $x = 2x'$ with some $x' \in \mathbb{Z}$. We have

$$3q^y = 2^{2x'} - 1 = (2^{x'} + 1)(2^{x'} - 1).$$

Since $2^{x'} + 1$ and $2^{x'} - 1$ are coprime integers and $y > 0$, we obtain two cases: (i) $2^{x'} + 1 = q^y$, $2^{x'} - 1 = 3$ or (ii) $2^{x'} + 1 = 3q^y$, $2^{x'} - 1 = 1$. Then, this equation has a positive integer solution (x, y) only in the case when $(q, x, y) = (5, 4, 1)$. □

Lemma D ([**2**, Lemma 3]). *For any integer* $k \geq 2$, *we have*

$$4F_k - F_{k-2\varepsilon} = L_{k+\varepsilon},$$

where $\varepsilon = \pm 1$.

We use Lemma 1, Lemma 2 and Lemma D to show the following lemma.

Lemma 3. *For any given positive integer* k *and positive odd integer* D_1, *the number of positive integer solutions* (x, y) *of the equation*

$$D_1 x^2 + 2^{2k} = q^y$$

is at most one except for $(D_1, k, q) = (1, 1, 5)$.

Proof. We will show $(\lambda, D_1, D_2, p) = (1, D_1, 2^{2k}, q) \notin \mathcal{E}$ and $(D_1, D_2, p) = (D_1, 2^{2k}, q) \notin \mathcal{F} \cup \mathcal{G} \cup \mathcal{H}_1$ to use Theorem C with $\lambda = 1$. Since $k > 0$ and 2^{2k} is even, we have

$$(1, D_1, 2^{2k}, q) \notin \mathcal{E},\ (D_1, 2^{2k}, q) \notin \mathcal{G}.$$

Suppose $(D_1, 2^{2k}, q) \in \mathcal{F}$. There exists $h \geq 2$ such that

$$F_{h-2\varepsilon} = D_1,\ L_{h+\varepsilon} = 2^{2k},\ F_h = q,$$

where $\varepsilon = \pm 1$. Using Lemma D, we have

$$4q - D_1 = 2^{2k}.$$

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

Since D_1 is odd, $4q - D_1$ is also odd. This contradicts that $L_{h+\varepsilon} = 2^{2k}$ is even. Next suppose $(D_1, 2^{2k}, q) \in \mathcal{H}_1$. Then both $D_1 s^2 + 2^{2k} = q^r$ and $3D_1 s^2 - 2^{2k} = \pm 1$ hold for some positive integers r and s. Then, we have

$$2^{2(k+1)} - 3q^r = \pm 1.$$

This is a contradiction with Lemma 1, Lemma 2 except for $(q, 2(k+1), r) = (5, 4, 1)$, that is, $(q, k, r) = (5, 1, 1)$. From the equation $D_1 s^2 + 2^{2k} = q^r$, we have $D_1 = 1$ when $(q, k, r) = (5, 1, 1)$. □

We show the following Lemma 4 by using Lemma 3.

Lemma 4. *Let n be a positive integer, k be a positive integer with $2^{2k} < q^n$ and*

$$\alpha := 2^k + \sqrt{2^{2k} - q^n} \in \mathbb{Q}\left(\sqrt{2^{2k} - q^n}\right).$$

(1) *For the case $q \equiv 3 \bmod 8$, if $k \equiv 1 \bmod 2$ or $n \not\equiv 3 \bmod 6$, $\pm\alpha$ is not a pth power in $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$ for any prime p dividing n.*

(2) *For the case $q \equiv 1 \bmod 4$, $\pm\alpha$ is not a pth power in $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$ for any prime p dividing n except for the case when $\mathbb{Q}(\sqrt{2^{2k} - q^n}) = \mathbb{Q}(\sqrt{-1})$ with $(q, k) = (5, 1)$.*

(3) *For the case $q \equiv 7 \bmod 8$, $\pm\alpha$ is not a pth power in $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$ for any prime p dividing n.*

Proof. Let p be a prime number and D denotes the square-free part of $2^{2k} - q^n$. Then, $D < 0$ is an odd integer and we can write $2^{2k} - q^n = m^2 D$ for some odd positive integer m.

(I) We show that $\pm\alpha$ are not square numbers in $\mathbb{Q}(\sqrt{2^{2k} - q^n})$. The proof of this case is obtained in a way similar to that in [**5**, Lemma 2.3].

(II) We consider the case $p \geq 3$. It is sufficient to prove that α is not a pth power in $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$. Suppose that α is a pth power in $O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$, that is, we can write

$$\alpha = \left(\frac{a + b\sqrt{D}}{2}\right)^p,$$

where $a, b \in \mathbb{Z}$, $a \equiv b \bmod 2$. We have

$$2^k + \sqrt{2^{2k} - q^n} = \frac{1}{2^p}\left(\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{p-2j} b^{2j} D^j + w\sqrt{D}\right)$$

for some $w \in \mathbb{Z}$. Comparing the real parts of this formula, we obtain

$$2^{k+p} = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{p-2j} b^{2j} D^j = a \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{p-2j-1} b^{2j} D^j.$$

Then, we get

$$a \mid 2^{k+p}.$$

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

(II-1) Assume that a is odd. Then, $a \mid 2^{k+p}$ is possible only if

$$a = \pm 1.$$

Since $a \equiv b \bmod 2$, b is also odd. We have

$$D \equiv 1 \bmod 4$$

in this case because $\alpha \in O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$.

(II-1-1) We can show a contradiction when $k = 1$ in a way similar to that in [**5**, Lemma 2.3].

(II-1-2) We consider the case when $k \geq 2$. Since $D \equiv 1 \bmod 4$ and m is odd, we have

$$-q^n \equiv 2^{2k} - q^n = m^2 D \equiv 1 \bmod 4.$$

This contradicts $-q^n \equiv -1 \bmod 4$ for $q \equiv 1 \bmod 4$. Next, we consider the case when $q \equiv 3 \bmod 8$. Only if n is odd, we can obtain $-q^n \equiv 1 \bmod 4$ because $q \equiv 3 \bmod 4$. If n is odd, we have

$$D \equiv m^2 D = 2^{2k} - q^n \equiv -q^n \equiv -3^n \equiv -3 \equiv 5 \bmod 8.$$

For any integer $s > 0$, we can obtain

$$\left(\frac{a + b\sqrt{D}}{2}\right)^s \in \mathbb{Z}[\sqrt{D}] \Leftrightarrow 3 \mid s$$

if $D \equiv 5 \bmod 8$. Then, p must be 3 and we get k is odd from the assumption of Lemma 4 and

$$2^{k+3} = a \sum_{j=0}^{\frac{3-1}{2}} \binom{3}{2j} a^{3-2j-1} b^{2j} D^j = a^3 + 3ab^2 D = \pm 1 \pm 3b^2 D.$$

Since $D < 0$, a must be -1. Then, we have

$$2^{k+3} = -1 - 3b^2 D \equiv -1 \equiv 2 \bmod 3.$$

This contradicts $2^{k+3} \equiv 1 \bmod 3$ because k is odd. Finally, we consider the case when $q \equiv 7 \bmod 8$. Since $-q^n \equiv 1 \bmod 4$, n is odd and we have

$$D \equiv m^2 D = 2^{2k} - q^n \equiv -q^n \equiv -7^n \equiv -7 \equiv 1 \bmod 8.$$

We show that, for any integer $s > 0$,

$$\left(\frac{a + b\sqrt{D}}{2}\right)^s \notin \mathbb{Z}[\sqrt{D}]$$

if $D \equiv 1 \bmod 8$. To show the above, it is enough to show that

$$\frac{1}{2}\left\{\left(\frac{a + b\sqrt{D}}{2}\right)^s + \left(\frac{a - b\sqrt{D}}{2}\right)^s\right\} \notin \mathbb{Z} \tag{1}$$

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

for any integer $s > 0$. Since $D \equiv 1 \bmod 8$, we can consider $\sqrt{D} \in \mathbb{Z}_2^\times$. Then, to show (1) is equivalent to show that

$$\frac{1}{2}\left\{\left(\frac{a+b\sqrt{D}}{2}\right)^s + \left(\frac{a-b\sqrt{D}}{2}\right)^s\right\} \notin \mathbb{Z}_2.$$

Since $\sqrt{D} \equiv 1 \bmod 2\mathbb{Z}_2$ and b is odd, we have

$$b\sqrt{D} \equiv 1, 3 \bmod 4\mathbb{Z}_2.$$

By checking four cases (i) $(a, b\sqrt{D}) = (\bar{1}, \bar{1})$, (ii) $(a, b\sqrt{D}) = (\bar{1}, \bar{3})$, (iii) $(a, b\sqrt{D}) = (\bar{3}, \bar{1})$, (iv) $(a, b\sqrt{D}) = (\bar{3}, \bar{3})$, where $a = \bar{j}$ denotes $a \equiv j \bmod 4\mathbb{Z}_2$, we obtain

$$\frac{a+b\sqrt{D}}{2} \not\equiv \frac{a-b\sqrt{D}}{2} \bmod 2\mathbb{Z}_2.$$

Then, we have

$$\left(\frac{a+b\sqrt{D}}{2}\right)^s + \left(\frac{a-b\sqrt{D}}{2}\right)^s \equiv 1 \bmod 2\mathbb{Z}_2,$$

that is,

$$\frac{1}{2}\left\{\left(\frac{a+b\sqrt{D}}{2}\right)^s + \left(\frac{a-b\sqrt{D}}{2}\right)^s\right\} \notin \mathbb{Z}_2.$$

(II-2) We consider the case when a is even. In this case, b is also even and we can write $a = 2u$, $b = 2v$ $(u, v \in \mathbb{Z})$. Since

$$\alpha = 2^k + \sqrt{2^{2k} - q^n} = (u + v\sqrt{D})^p,$$

we have

$$2^k = u\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} u^{p-2j-1} v^{2j} D^j = u^p + u\sum_{j=1}^{\frac{p-1}{2}} \binom{p}{2j} u^{p-2j-1} v^{2j} D^j \equiv u^p \equiv u \bmod p.$$

By taking the norm of α, we have

$$(u^2 - v^2 D)^p = N((u + v\sqrt{D})^p) = N(\alpha) = q^n.$$

Then, $u^2 - v^2 D$ is odd. Hence, we get

$$u \not\equiv v \bmod 2.$$

(II-2-1) Suppose u is odd and v is even. We can show a contradiction in a way similar to that in [**5**, Lemma 2.3].

(II-2-2) Suppose u is even and v is odd. We can obtain

$$q^{\frac{n}{p}} = 2^{2k} - v^2 D$$

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

in a way similar to that in [5, Lemma 2.3]. This implies that both

$$(x, y) = (m, n) \text{ and } (x, y) = \left(|v|, \frac{n}{p}\right)$$

are positive integer solutions of the equation

$$-Dx^2 + 2^{2k} = q^y.$$

Since D is odd and

$$n \neq \frac{n}{p},$$

this contradicts Lemma 3 except for $(D, k, q) = (-1, 1, 5)$. The case $(D, k, q) = (-1, 1, 5)$ is not contained in the assumption of this lemma. □

4. Proof of Theorem 1.

In this section, we show Theorem 1 and Corollaries 1, 2 by using Lemma 4.

Proof of Theorem 1. Since $N(\alpha) = q^n$, $(q, D) = 1$ and $q \nmid \alpha$, we can write

$$(\alpha) = \wp^n,$$

where $\wp$ is a prime factor of (q) which splits completely in $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$. Let s be the order of the ideal class $[\wp]$. We can write

$$n = sn'$$

for some $n' \in \mathbb{Z}$. Since $\wp^s \sim (1)$, there exists some element $\beta \in O_{\mathbb{Q}(\sqrt{2^{2k}-q^n})}$ such that

$$(\alpha) = \wp^n = (\wp^s)^{n'} = (\beta)^{n'} = (\beta^{n'}).$$

We show that $\mathbb{Q}(\sqrt{2^{2k} - q^n})$ is different from $\mathbb{Q}(\sqrt{-1})$ (resp. $\mathbb{Q}(\sqrt{-3})$) when $q \equiv 3 \bmod 4$ (resp. $q \equiv 1 \bmod 4$). First, we consider the case when $q \equiv 3 \bmod 4$. Suppose that $\mathbb{Q}(\sqrt{2^{2k} - q^n}) = \mathbb{Q}(\sqrt{-1})$, that is, there exists $t > 0 \in \mathbb{Z}$ such that $2^{2k} - q^n = -t^2$. Then, we have

$$2^{2k} \equiv -t^2 \bmod q$$

by $n \neq 0$. Since $q \nmid t$, the existence of x such that $-t^2 \equiv x^2 \bmod q$ is equivalent to the condition that $-t^2 \in \left(\mathbb{F}_q^\times\right)^2$. We know that $-t^2 \in \left(\mathbb{F}_q^\times\right)^2$ is equivalent to $\left(\frac{-t^2}{q}\right) = 1$. By $q \equiv 3 \bmod 4$, we have

$$\left(\frac{-t^2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{t}{q}\right)^2 = \left(\frac{-1}{q}\right) = -1.$$

This contradicts $\left(\frac{-t^2}{q}\right) = 1$. Secondly, we consider the case when $q \equiv 1 \bmod 4$. Suppose that $\mathbb{Q}(\sqrt{2^{2k} - q^n}) = \mathbb{Q}(\sqrt{-3})$, that is, there exists $t > 0 \in \mathbb{Z}$ such that $2^{2k} - q^n = -3t^2$. Since t is odd, we have

$$-q^n \equiv 2^{2k} - q^n = -3t^2 \equiv -3 \bmod 4.$$

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

This contradicts $-q^n \equiv -1 \bmod 4$. Since $\mathbb{Q}(\sqrt{2^{2k} - q^n}) \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, we obtain

$$O^{\times}_{\mathbb{Q}(\sqrt{2^{2k}-q^n})} = \{\pm 1\},$$

that is,

$$\pm\alpha = \beta^{n'}.$$

From Lemma 4, we get $n' = 1$ and then we have

$$n = s.$$

The proof of Theorem 1 is completed. □

Proof of Corollary 1. We can prove $\mathbb{Q}(\sqrt{2^{2k} - q^n}) \neq \mathbb{Q}(\sqrt{-3})$ for $q \equiv 11, 23 \bmod 24$ in a way similar to the proof of $\mathbb{Q}(\sqrt{2^{2k} - q^n}) \neq \mathbb{Q}(\sqrt{-1})$ for $q \equiv 3 \bmod 8$ (see the proof of Theorem 1). Suppose that there exists $t > 0 \in \mathbb{Z}$ such that $2^{2k} - q^n = -3t^2$. Then, we have

$$2^{2k} \equiv -3t^2 \bmod q$$

by $n \neq 0$. Since

$$\left(\frac{-3t^2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{3}{q}\right)\left(\frac{t}{q}\right)^2 = \left(\frac{-1}{q}\right)\left(\frac{3}{q}\right) = -\left(\frac{3}{q}\right)$$

and

$$\left(\frac{3}{p}\right) = 1 \Leftrightarrow p \equiv 1 \quad \text{or} \quad 11 \bmod 12$$

and

$$q \equiv 11 \bmod 12,$$

we have

$$\left(\frac{-3t^2}{q}\right) = -1.$$

Then, we get a contradiction. Using this and Theorem 1 (1), (3), the proof of Corollary 1 is completed. □

Proof of Corollary 2. Suppose $\mathbb{Q}(\sqrt{2^{2k} - q^n}) = \mathbb{Q}(\sqrt{-3})$. Then, we have $q^n \equiv 3 \bmod 4$. This contradicts $q^n \equiv 1 \bmod 4$ since n is even. Using this and Theorem 1 (1), (3), the proof of Corollary 2 is completed. □

5. Additional Remarks. We conclude this paper with remarks on Theorem 1 (1).

EXAMPLE. We give an example for Theorem 1 (1) that the class number is not divisible by n when $n \equiv 3 \bmod 6$ and $k \equiv 0 \bmod 2$. For $(q, n, k) = (11, 3, 4)$, we have $2^{2k} - q^n = 2^8 - 11^3 = -1075 = 5^2 \times (-43)$. The class number of the field $\mathbb{Q}(\sqrt{-43})$ is 1 and is not divisible by 3.

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

For Theorem B, the class number of the field $\mathbb{Q}(\sqrt{2^{2k}-3^n})$ is not divisible by n only in the case when $(n, k) = (3, 2)$, that is, the class number of the field $\mathbb{Q}(\sqrt{2^{2\times 2}-3^3}) = \mathbb{Q}(\sqrt{-11})$ is 1 and not divisible by 3. But we do not know how many quadratic fields $\mathbb{Q}(\sqrt{2^{2k}-q^n})$ exist, whose class numbers are not divisible by n when $q \equiv 3 \bmod 8$, $n \equiv 3 \bmod 6$ and $k \equiv 0 \bmod 2$. As for this point, we give the following remark (cf. Lemma 4). We can prove that Lemma 4 also holds except for Case (II-1-2) when $q \equiv 3 \bmod 8$, k is even and $p = 3$. For the proof of Case (II-1-2) of Lemma 4, we have to consider whether we can show a contradiction with

$$2^{k+3} = -1 - 3b^2 D \tag{2}$$

when k is even. By taking the norm of both sides of the equation

$$(\alpha =)\, 2^k + \sqrt{2^{2k} - q^n} = \left(\frac{a + b\sqrt{D}}{2}\right)^3,$$

we have

$$q^n = \left(\frac{a^2 - b^2 D}{4}\right)^3.$$

Then, we obtain

$$4q^{\frac{n}{3}} = a^2 - b^2 D.$$

From the above equation and (2), we have

$$2^{k+1} + 1 = 3q^{\frac{n}{3}}.$$

Then, this consideration is related to the determination of positive integer solutions (q, x, y) of the equation $2^x - 3q^y = -1$, where x, y are odd and $q \equiv 3 \bmod 8$ are prime numbers (see Lemma 1). We can obtain that, if (n, k) does not satisfy $2^{k+1} - 3q^{\frac{n}{3}} = -1$, the class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{2^{2k}-q^n})$ except $\mathbb{Q}(\sqrt{-3})$ are also divisible by n when $q \equiv 3 \bmod 8$, $n \equiv 3 \bmod 6$ and $k \equiv 0 \bmod 2$. For the case when $q = 3$, the result on positive integer solutions of the equation $2^x - 3^y = -1$ is written in [**5**, Lemma 2.1].

Acknowledgements. The author thanks Professor Yasuhiro Kishi, Professor Shin Nakano and Professor Nobuhiro Terai for helpful comments in Section 5 of this paper. She would also like to thank Professor Hiroshi Suzuki and Professor Kohji Matsumoto for valuable comments and encouragement. Further, she thanks the referee for careful reading and several useful comments.

REFERENCES

1. N. C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, *Pacific J. Math.* **5** (1955), 321–324.

2. Y. Bugeaud and T. N. Shorey, On the number of solutions of the generalized Ramanujan–Nagell equation, *J. Reine Angew. Math.* **539** (2001), 55–74.

3. J. H. E. Cohn, On the class number of certain imaginary quadratic fields, *Proc. Amer Math. Soc.* **130** (2001), 1275–1277.

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press

4. B. H. Gross and D. E. Rohrlich, Some results on the Mordell-Weil group of the Jacobian of the Fermat curve, *Invent. Math.* **44** (1978), 201–224.

5. Y. Kishi, Note on the divisibility of the class number of certain imaginary quadratic fields, *Glasgow Math. J.* **51** (2009), 187–191.

6. Y. Kishi, Note on the divisibility of the class number of certain imaginary quadratic fields—Corrigendum, *Glasgow Math. J.* **52** (2010), 207–208.

7. T. Nagell, Über die Klassenzahl imaginär-quadratischer Zahlkörper, *Abh. Math. Sem. Univ. Hamburg* **1** (1922), 140–150.

https://doi.org/10.1017/S0017089511000012 Published online by Cambridge University Press