Glasgow Math. J. **51** (2009) 187–191. © 2008 Glasgow Mathematical Journal Trust.
doi:10.1017/S001708950800462X. Printed in the United Kingdom

NOTE ON THE DIVISIBILITY OF THE CLASS NUMBER OF CERTAIN IMAGINARY QUADRATIC FIELDS

YASUHIRO KISHI
Department of Mathematics, Fukuoka University of Education,
Munakata, Fukuoka 811-4192, Japan
e-mail: ykishi@fukuoka-edu.ac.jp

(Received 8 April 2008; revised 3 June 2008; accepted 1 July 2008)

Abstract. We prove that the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ is divisible by n for any positive integers k and n with $2^{2k} < 3^n$, by using Y. Bugeaud and T. N. Shorey's result on Diophantine equations.

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

1. Introduction. In [**1**], N. C. Ankeny and S. Chowla proved

THEOREM 1.1. [**1**, Theorem 1] *Let n be an even positive integer and $d := x^2 - 3^n$ be a square-free integer with $2 \mid x$ and $0 < x < (2 \cdot 3^{n-1})^{1/2}$. Then the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ is divisible by n.*

The aim of the present paper is to remove the conditions 'even' and 'square-free' in the above theorem for the case where x is a power of two. Namely, we will prove

THEOREM 1.2. *For any positive integers k and n with $2^{2k} < 3^n$, the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ is divisible by n.*

B. H. Gross and D. E. Rohrlich [**3**] (resp. H. Ichimura [**5**]) proved that the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{1 - 4a^n})$ (resp. the real quadratic field $\mathbb{Q}(\sqrt{a^{2n} + 4})$) is divisible by n for any odd integer $n \geq 3$ and any integer $a \geq 2$ (resp. for any integer $n \geq 2$ and any odd integer $a \geq 3$). Our main theorem is a similar result of these ones.

REMARK 1.1. By putting $b = 2^k$ and $m = 3$ in Mollin's theorem [**6**, Theorem 3.1], we can show that if $2^{2k} - 3^n$ is *square-free*, then the class number of $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ is divisible by n.

To prove Theorem 1.2, we use the same method as [**5**] and need a result of Y. Bugeaud and T. N. Shorey which states the following:

Let F_n (resp. L_n) denote the nth number in the Fibonacci sequence (resp. Lucas sequence) defined by $F_0 = 0, F_1 = 1$ and $F_{n+2} = F_{n+1} + F_n$ $(n \geq 0)$ (resp. $L_0 = 2, L_1 = 1$ and $L_{n+2} = L_{n+1} + L_n$ $(n \geq 0)$). For $\lambda \in \{1, \sqrt{2}, 2\}$, we define the sets $\mathcal{F}, \mathcal{G}_\lambda, \mathcal{H}_\lambda \subset \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ by

$$\mathcal{F} := \{(F_{k-2\varepsilon}, L_{k+\varepsilon}, F_k) \mid k \geq 2, \varepsilon \in \{\pm 1\}\},$$
$$\mathcal{G}_\lambda := \{(1, 4p^r - 1, p) \mid p \text{ is an odd prime}, r \geq 1\},$$

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

except when $\lambda = 2$, in which case the condition 'odd' for p should be removed in the definitions of $\mathcal{G}_\lambda$ and $\mathcal{H}_\lambda$.

THEOREM 1.3 [**2**, Theorem 1]. *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 1 *except for*

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

and

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

2. Proofs.

First, we show two lemmas on Diophantine equations.

LEMMA 2.1. *The equation*

$$2^x - 3^y = \pm 1$$

has only three positive integer solutions $(x, y) = (1, 1), (2, 1), (3, 2)$.

Proof. This can be easily proved by taking modulo some power of two. See details in [**4**]. □

LEMMA 2.2. *Let k and* D_1 *be positive integers. Then the number of positive integer solutions* (x, y) *of the equation*

$$D_1 x^2 + 2^{2k} = 3^y$$

is at most 1.

Proof. It is easily seen that $(1, D_1, 2^{2k}, 3) \notin \mathcal{E}$ and $(D_1, 2^{2k}, 3) \notin \mathcal{G}_1$ for any positive integers k and D_1. Suppose that $(D_1, 2^{2k}, 3) \in \mathcal{F}$. Then we have $k = 1$ and $D_1 = 8$. In this case, the equation $8x^2 + 4 = 3^y$ has no integer solutions. Next suppose that $(D_1, 2^{2k}, 3) \in \mathcal{H}_1$. Then both $D_1 s^2 + 2^{2k} = 3^r$ and $3D_1 s^2 - 2^{2k} = \pm 1$ hold for some positive integers r and s. Hence, we have

$$2^{2(k+1)} = 3^{r+1} \mp 1,$$

which is impossible by Lemma 2.1. Thus, we have $(D_1, 2^{2k}, 3) \notin \mathcal{H}_1$. The proof is completed. □

The following is the key lemma for the proof of our main theorem.

LEMMA 2.3. *Let k and n be positive integers with $2^{2k} < 3^n$ and $n \geq 3$, and put $\alpha := 2^k + \sqrt{2^{2k} - 3^n} \in \mathbb{Q}(\sqrt{2^{2k} - 3^n})$. Then $\pm\alpha$ is not a pth power in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ for any prime p.*

Proof. Let p be a prime number and let D denote the square-free part of $2^{2k} - 3^n$. Then D is a negative odd integer.

First, we consider the case $p = 2$. Assume that α is a square in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$;

$$\alpha = \left(\frac{a + b\sqrt{D}}{2}\right)^2 \quad (a, b \in \mathbb{Z},\ a \equiv b \ (\mathrm{mod}\ 2)).$$

Then we have

$$2^k + \sqrt{2^{2k} - 3^n} = \frac{a^2 + b^2 D}{4} + \frac{ab}{2}\sqrt{D}. \tag{2.1}$$

Let us express $2^{2k} - 3^n = Dm^2$ for some non-zero integer m. We see that m must be congruent to 1 or -1 modulo 4. Then equation (2.1) implies $ab = 2m$, which is congruent to 2 modulo 4, a contradiction. Therefore, α is not a square in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$. By the same argument, we can show that $-\alpha$ is not a square in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$.

From now on we assume $p \geq 3$. If $-\alpha$ is a pth power in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$, then so α. It is therefore sufficient to prove that α is not a pth power in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$. Assume, for a contradiction, that α is a pth power in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$;

$$\alpha = \left(\frac{a + b\sqrt{D}}{2}\right)^p \quad (a, b \in \mathbb{Z},\ a \equiv b \ (\mathrm{mod}\ 2)).$$

Then we have

$$2^k + \sqrt{2^{2k} - 3^n} = \frac{1}{2^p}\left\{\sum_{j=0}^{(p-1)/2} \binom{p}{2j} a^{p-2j} b^{2j} D^j + w\sqrt{D}\right\}$$

for some $w \in \mathbb{Z}$, where $\binom{p}{j}$ denotes the binomial coefficient. Hence we obtain the relation

$$2^{k+p} = a \sum_{j=0}^{(p-1)/2} \binom{p}{2j} a^{p-2j-1} b^{2j} D^j. \tag{2.2}$$

It is easily seen that a divides 2^{k+p}.

First, we suppose that a is odd. Then b is also odd and a is equal to ± 1. Since α is an integer in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$, we have $D \equiv 1 \ (\mathrm{mod}\ 4)$ in this case. Assume that $k = 1$. Considering (2.2) modulo p, we have

$$4 \equiv a = \pm 1 \ (\mathrm{mod}\ p),$$

and hence $(a, p) = (1, 3)$ or $(a, p) = (-1, 5)$. If $(a, p) = (1, 3)$, then we have

$$5 = b^2 D$$

https://doi.org/10.1017/S001708950800462X Published online by Cambridge University Press

by (2.2). This contradicts $D < 0$. If $(a, p) = (-1, 5)$, then we have

$$-13 = 2b^2D + b^4D^2$$

by (2.2). This is also a contradiction because the equation $-13 = 2X + X^2$ has no solutions in $\mathbb{R}$, and so in particular none in $\mathbb{Z}$. Hence, k must be greater than or equal to 2. Recalling that $D \equiv 1 \pmod 4$, we have

$$2^{2k} - 3^n \equiv D \equiv 1 \pmod 4.$$

Therefore, n must be odd. Since the square of any odd integer is congruent to 1 modulo 8, we have

$$D \equiv 2^{2k} - 3^n \equiv -3 \equiv 5 \pmod 8.$$

In this case, we can easily see that for a positive integer m,

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

Then p must be equal to 3, and hence we have

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

b y (2.2). This contradicts $D < 0$.

Next, we suppose that a is even. Then b is also even. By putting $a = 2u$ and $b = 2v$ with $u, v \in \mathbb{Z}$, we have

$$2^k + \sqrt{2^{2k} - 3^n} = (u + v\sqrt{D})^p. \tag{2.3}$$

Then we have

$$2^k = u \sum_{j=0}^{(p-1)/2} \binom{p}{2j} u^{p-2j-1} v^{2j} D^j. \tag{2.4}$$

Considering (2.4) modulo p, we obtain

$$2^k \equiv u \pmod p. \tag{2.5}$$

Here, we note that the parities of u and v are different because the norm of $u + v\sqrt{D}$ is odd (especially a power of 3). When u is odd and v is even, the right-hand side of (2.4) is odd, which leads a contradiction. Hence, u is even and v is odd. Since

$$\sum_{j=0}^{(p-1)/2} \binom{p}{2j} u^{p-2j-1} v^{2j} D^j = u^2 \sum_{j=0}^{(p-1)/2} \binom{p}{2j} u^{p-2j-3} v^{2j} D^j + pv^{p-1} D^{(p-1)/2}$$

is odd, we have

$$2^k = \pm u. \tag{2.6}$$

https://doi.org/10.1017/S001708950800462X Published online by Cambridge University Press

From (2.5), (2.6) and $p \geq 3$, we have $u = 2^k$. Then we can rewrite the relation (2.3) into the following:

$$2^k + \sqrt{2^{2k} - 3^n} = (2^k + v\sqrt{D})^p. \tag{2.7}$$

Let us express $2^{2k} - 3^n = v_0^2 D$ ($v_0 \in \mathbb{Z},\ v_0 > 0$). Considering the norm of both sides of (2.7), we have

$$-v^2 D + 2^{2k} = 3^{n/p}.$$

Then we obtain two positive integer solutions $(x, y) = (v_0, n), (v, n/p)$ of the equation

$$-Dx^2 + 2^{2k} = 3^y.$$

This contradicts Lemma 2.2. The proof of Lemma 2.3 is completed. □

Proof of Theorem 1.2. Put $\alpha := 2^k + \sqrt{2^{2k} - 3^n}$. Then we have $3 \nmid \alpha$ and $N(\alpha) = 3^n$, where N is the norm map of $\mathbb{Q}(\sqrt{2^{2k} - 3^n})/\mathbb{Q}$, and hence $(\alpha) = \mathfrak{a}^n$ for some ideal $\mathfrak{a}$ of $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$. Denote the order of the ideal class $[\mathfrak{a}]$ by s. It is clear that $s \mid n$. Now let us express $\mathfrak{a}^s = (\beta)$, where β is an integer in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$. Then by putting $n = sm$ for some positive integer m, we have

$$(\alpha) = \mathfrak{a}^n = (\mathfrak{a}^s)^m = (\beta)^m = (\beta^m).$$

We see that $3^n - 2^{2k}$ is not square because it is congruent to -1 modulo 3. Hence we have $\mathbb{Q}(\sqrt{2^{2k} - 3^n}) \neq \mathbb{Q}(\sqrt{-1})$. Moreover, we immediately have $\mathbb{Q}(\sqrt{2^{2k} - 3^n}) \neq \mathbb{Q}(\sqrt{-3})$. Thus, the only units in $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ are ± 1, and hence we get

$$\pm\alpha = \beta^m.$$

When $n = 2$, it must hold that $k = 1$. Since $\pm\alpha = \pm(2 + \sqrt{-5})$ is not a square in $\mathbb{Q}(\sqrt{2^2 - 3^2}) = \mathbb{Q}(\sqrt{-5})$, we have $m = 1$. When $n \geq 3$, we obtain $m = 1$ by Lemma 2.3. Therefore, we obtain $s = n$ in any case. This implies that the class number of $\mathbb{Q}(\sqrt{2^{2k} - 3^n})$ is divisible by n. The proof is completed. □

ACKNOWLEDGEMENT. The author thanks the referee for his/her careful reading and for several helpful 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. 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.

4. A. Herschfeld, The equation $2^x - 3^y = d$, *Bull. Amer. Math. Soc.* **42** (1936), 231–234.

5. H. Ichimura, Note on the class numbers of certain real quadratic fields, *Abh. Math. Sem. Univ. Hamburg* **73** (2003), 281–288.

6. R. A. Mollin, Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields, *Glasgow Math. J.* **38** (1996), 195–197.