Glasgow Math. J. **54** (2012) 149–154. © Glasgow Mathematical Journal Trust 2011.
doi:10.1017/S0017089511000486.

THE DIVISIBILITY OF THE CLASS NUMBER OF THE IMAGINARY QUADRATIC FIELD $\mathbf{Q}(\sqrt{2^{2m}-k^n})$

ZHU MINHUI
School of Science, Xi'an Polytechnic University, Xi'an, Shaanxi, P.R. China
e-mail: xiao-zhu123@sohu.com

and WANG TINGTING
Department of Mathematics, Northwest University, Xi'an, Shaanxi, P.R. China
e-mail: tingtingwang126@126.com

(Received 7 July 2010; revised 29 November 2010; accepted 16 August 2011)

Abstract. Let h_K denote the class number of the imaginary quadratic field $K = \mathbf{Q}(\sqrt{2^{2m}-k^n})$, where m and n are positive integers, k is an odd integer with $k > 1$ and $2^{2m} < k^n$. In this paper we prove that if either $3 \mid n$ and $2^{2m} - k^n \equiv 5 (\mathrm{mod}\ 8)$ or $n = 3$ and $k = (2^{2m+2} - 1)/3$, then $\frac{n}{3} \mid h_K$. Otherwise, we have $n \mid h_K$.

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

1. Introduction. Let $\mathbf{Z}, \mathbf{N}, \mathbf{Q}$ be the sets of all integers, positive integers and rational numbers, respectively. For any fixed positive integer D, there exists unique positive integers d and s such that

$$D = ds^2,\ d, s \in \mathbf{N},\ \ d \text{ is a square-free number.} \tag{1}$$

Let h_K denote the class number of the imaginary quadratic field $K = \mathbf{Q}(\sqrt{-D})$. There are many papers concerned with the divisibility of h_K, for

$$-D = a^2 - \delta k^n,\ \ a, k, n \in \mathbf{N},\ \ \gcd(a, k) = 1,\ \ k > 1,\ \ \delta \in \{1, 4\}, a^2 < 8k^n \tag{2}$$

(see [**1**, **3**, **4**, **7**, **8**, **9**]). Recently, Kishi [**7**] proved that if $a = 2^m, k = 3, \delta = 1$ and $(k, n) \neq (2, 3)$, where m is a positive integer, then $n \mid h_K$. In this paper, we prove a more general result than Kishi's result, as follows.

THEOREM. *If $a = 2^m$ and $\delta = 1$, where m is a positive integer, then*

$$h_K \equiv \begin{cases} 0 \left(mod\ \dfrac{n}{3}\right), & \text{if either } 3 \mid n \text{ and } 2^{2m} - k^n \equiv 5 (mod\ 8) \\ & \text{or } n = 3 \text{ and } k = (2^{2m+2} - 1)/3 \\ 0\ (mod\ n), & \text{otherwise} \end{cases}. \tag{3}$$

The proof of our theorem relies on a recent result concerning the existence of primitive divisors of Lehmer numbers given by Bilu et al. [**2**] and Voutier [**10**].

2. Preliminaries. For any positive integer D with $-D \equiv 0$ or $1 (\mathrm{mod}\ 4)$, let $H(-D)$ denote the class number of binary quadratic primitive forms with discriminant $-D$.

Let d be a square-free positive integer, and let $h(-d)$ denotes the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-d})$.

LEMMA 1. *(Section 16.13 in* [**6**]*)*

$$h(-d) = \begin{cases} H(-4d), & \text{if } d \equiv 1(\text{mod } 4) \\ H(-d), & \text{if } d \equiv 3(\text{mod } 4) \end{cases}.$$

LEMMA 2. *If $d > 3$ and $d \equiv 3(\text{mod } 4)$, then*

$$H(-d) = \begin{cases} \frac{1}{3}H(-4d), & \text{if } d \equiv 3(\text{mod } 8) \\ H(-4d), & \text{if } d \equiv 7(\text{mod } 8) \end{cases}. \tag{4}$$

Proof. Since $d \geq 7$, by Theorems 11.4.3 and 12.10.1 in [**6**], we have

$$H(-d) = \frac{\sqrt{d}}{\pi} K(-d), \tag{5}$$

and

$$H(-4d) = \frac{2\sqrt{d}}{\pi} K(-4d), \tag{6}$$

where $K(-d) = \sum_{n=1}^{\infty} (\frac{d}{n})(\frac{1}{n})$, (d/n) is the Kronecher symbol.

Further, since $-d \equiv 1(\text{mod } 4)$, by the definition of fundamental discriminants (see Section 12.11 in [**6**]), $-d$ is a fundamental discriminant, while $-4d$ is not. Therefore, by Theorem 12.11.2 in [**6**], we have

$$K(-4d) = \left(1 - \left(\frac{-d}{2}\right)\frac{1}{2}\right) K(-d), \tag{7}$$

where $(-d/2)$ is the Kronecker symbol. Furthermore, by Theorems 3.6.3 and 12.3.1 in [**6**], we get

$$\left(\frac{-d}{2}\right) = \left(\frac{2}{d}\right) = (-1)^{(d^2-1)/8} = \begin{cases} 1, & \text{if } d \equiv 7(\text{mod } 8) \\ -1, & \text{if } d \equiv 3(\text{mod } 8) \end{cases}, \tag{8}$$

where $(2/d)$ is the Jacobi symbol. Substitute (8) into (7), we get

$$K(-4d) = \begin{cases} \frac{1}{2}K(-d), & \text{if } d \equiv 7(\text{mod } 8) \\ \\ \frac{3}{2}K(-d), & \text{if } d \equiv 3(\text{mod } 8) \end{cases}. \tag{9}$$

Thus, by (5), (6) and (9), we obtain (4). The lemma is proved. □

By Lemmas 1 and 2, we get the following lemma immediately.

LEMMA 3.

$$h(-d) = \begin{cases} \frac{1}{3}H(-4d), & \text{if } d > 3 \text{ and } d \equiv 3(\text{mod } 8) \\ H(-4d), & \text{otherwise} \end{cases}.$$

LEMMA 4. *Let D and k be positive integers such that* $D > 1$, $k > 1$ *and* $\gcd(k, 2D) = 1$. *If equation*

$$X^2 + DY^2 = k^Z,\ X, Y, Z \in \mathbf{N},\ \gcd(X, Y) = 1, Z > 0, \tag{10}$$

has solutions (X, Y, Z)*, then every solution* (X, Y, Z) *of (10) can be expressed as*

$$Z = Z_1 t,\ t \in \mathbf{N},$$

$$X + Y\sqrt{-D} = \lambda_1(X_1 + \lambda_2 Y_1\sqrt{-D})^t,\ \lambda_1, \lambda_2 \in \{\pm 1\},$$

where X_1, Y_1, *and* Z_1 *are positive integers satisfying*

$$X_1^2 + DY_1^2 = k^{Z_1},\ \gcd(X_1, Y_1) = 1, Z_1 \mid H(4D).$$

Proof. This is a special case of Theorem 6.2 in **[5]** for $(D_1, D_2) = (1, -D)$. We may assume that the solution (X, Y, Z) belongs to a certain solution class S_l of (10), and let (X_1, Y_1, Z_1) denote a solution of S_l such that $X_1 > 0$, $Y_1 > 0$ and $Z_1 \leq Z$ for all solutions $(X, Y, Z) \in S_l$. Then, by Theorem 6.2 in **[5]**, the lemma is proved. □

LEMMA 5. *Equation*

$$x^m - y^n = 1,\ x, y, m, n \in \mathbf{N},\ \min(x, y, m, n) > 1$$

has only one solution $(x, y, m, n) = (3, 2, 2, 3)$.

LEMMA 6. *Equation*

$$2^{2m+2} - 3y^n = 1,\ y, m, n \in \mathbf{N},\ n > 2 \tag{11}$$

has no solution (y, m, n).

Proof. Let (y, m, n) be a solution of (11). Since $(2^{m+1} + 1, 2^{m+1} - 1) = 1$, we get from (11) that either

$$2^{m+1} + 1 = a^n,\ 2^{m+1} - 1 = 3b^n,\ y = ab,\ a, b \in \mathbf{N}, \tag{12}$$

or

$$2^{m+1} + 1 = 3a^n,\ 2^{m+1} - 1 = b^n,\ y = ab,\ a, b \in \mathbf{N}. \tag{13}$$

But, since $n > 2$, by Lemma 5, (12) and (13) are both impossible. Thus, the lemma is proved.

Let α, β be algebraic integers. If $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero coprime integers and α/β is not a root of unity, then (α, β) is called a Lehmer pair. Further, let $a = (\alpha + \beta)^2$ and $c = \alpha\beta$. Then, we have

$$\alpha = \frac{1}{2}(\sqrt{a} + \lambda\sqrt{b}),\quad \beta = \frac{1}{2}(\sqrt{a} - \lambda\sqrt{b}),\quad \lambda \in \{\pm 1\},$$

where $b = a - 4c$. Such (a, b) is called the parameters of Lehmer pair (α, β). Two Lehmer pairs, (α_1, β_1) and (α_2, β_2), are called equivalent if $\alpha_1/\alpha_2 = \beta_1/\beta_2 \in \{\pm 1, \pm\sqrt{-1}\}$. Obviously, if (α_1, β_1) and (α_2, β_2) are equivalent Lehmer pairs with parameters (a_1, b_1) and (a_2, b_2) respectively, then $(a_2, b_2) = (\lambda a_1, b_1)$, where $\lambda \in \{\pm 1\}$.

For a fixed Lehmer pair (α, β), one defines the corresponding sequence of Lehmer numbers by

$$L_r(\alpha, \beta) = \begin{cases} \dfrac{\alpha^r - \beta^r}{\alpha - \beta}, & \text{if } r \text{ is old} \\ \dfrac{\alpha^r - \beta^r}{\alpha^2 - \beta^2}, & \text{if } r \text{ is even} \end{cases} \qquad r \in \mathbf{N}. \tag{14}$$

Then, Lehmer numbers $L_r(\alpha, \beta)$ $(r = 1, 2, \ldots)$ are non-zero integers. Further, for equivalent Lehmer pairs (α_1, β_1) and (α_2, β_2), we have $L_r(\alpha_1, \beta_1) = \pm L_r(\alpha_2, \beta_2)$ for any. A prime p is called a primitive divisor of the Lehmer number $L_r(\alpha, \beta)$ if $p \mid L_r(\alpha, \beta)$ and $p \nmid abL_1(\alpha, \beta) \ldots L_{r-1}(\alpha, \beta)$, where (a, b) is the parameters of Lehmer pair (α, β). A Lehmer pair (α, β) such that $L_r(\alpha, \beta)$ has no primitive divisor will be called r-defective Lehmer pair. □

LEMMA 7 **[10]**. *Let r satisfy $6 < r \leq 30$ and $r \neq 8, 10, 12$. Then, up to equivalence, all parameters (a, b) $(a > 0)$ of r-defective pairs are given as follows:*
$r = 7,\ (a, b) = (1, -7), (1, -19), (3, -5), (5, -7), (13, -3), (14, -22)$.
$r = 9,\ (a, b) = (5, -3), (7, -1), (7, -5)$.
$r = 13,\ (a, b) = (1, -7)$.
$r = 14,\ (a, b) = (3, -13), (5, -3), (7, -1), (7, -5), (19, -1), (22, -14)$.
$r = 15,\ (a, b) = (7, -1), (10, -2)$.
$r = 18,\ (a, b) = (1, -7), (3, -5), (5, -7)$.
$r = 24,\ (a, b) = (3, -5), (5, -3)$.
$r = 26,\ (a, b) = (7, -1)$.
$r = 30,\ (a, b) = (1, -7), (2, -10)$.

LEMMA 8 **[2]**. *If $r > 30$, then no Lehmer pair is r-defective.*

3. Proof of the theorem. Since $a = 2^m$ and $\delta = 1$, we see from (2) that k is an odd integer with $k > 1$. By (1) and (2), equation

$$X^2 - dY^2 = k^Z,\ X, Y, Z \in \mathbf{N},\ \gcd(X, Y) = 1, Z > 0$$

has a solution $(X, Y, Z) = (2^m, s, n)$. Therefore, by Lemma 4 we get

$$n = Z_1 t,\ t \in \mathbf{N}, \tag{15}$$
$$2^m + s\sqrt{-d} = \lambda_1(X_1 + \lambda_2 Y_1\sqrt{-d})^t,\ \lambda_1, \lambda_2 \in \{\pm 1\}, \tag{16}$$

where X_1, Y_1, and Z_1 are positive integers satisfying

$$X_1^2 - dY_1^2 = k^{Z_1},\ \gcd(X_1, Y_1) = 1, \tag{17}$$
$$Z_1 \mid H(-4d), \tag{18}$$

where $H(-4d)$ is the class number of binary quadratic primitive forms with discriminant $-4d$.

Since k is odd, we see from (1), (2) and (17) that D, d and s are odd, and $(X_1 Y_1)$ is even. Therefore, we find from (16) that t must be odd. Then, by (16), we get

$$2^m = \lambda_1 X_1 \sum_{i=0}^{(t-1)/2} \binom{t}{2i} X_1^{t-2i-1} \left(-d Y_1^2\right)^i, \tag{19}$$

$$s = \lambda_1 \lambda_2 Y_1 \sum_{i=0}^{(t-1)/2} \binom{t}{2i+1} X_1^{t-2i-1} \left(-d Y_1^2\right)^i. \tag{20}$$

Further, since s is odd, we see from (20) that Y_1 is odd and X_1 is even. Furthermore, since

$$\sum_{i=0}^{(t-1)/2} \binom{t}{2i} X_1^{t-2i-1} \left(-d Y_1^2\right)^i$$

is odd , we get from (19) that

$$X_1 = 2^m \tag{21}$$

and

$$\sum_{i=0}^{(t-1)/2} \binom{t}{2i} 2^{m(t-2i-1)} \left(-d Y_1^2\right)^i = \pm 1. \tag{22}$$

Let

$$\alpha = Y_1 \sqrt{-d} + 2^m, \ \beta = Y_1 \sqrt{-d} - 2^m. \tag{23}$$

Then we have

$$\alpha + \beta = 2 Y_1 \sqrt{-d}, \ \alpha - \beta = 2^{m+1}, \ \alpha\beta = -k^{Z_1}, \tag{24}$$

by (17). We see from (24) that $(\alpha + \beta)^2 = -4d Y_1^2$ and $\alpha\beta = -k^{Z_1}$ are coprime non-zero integers. Further, by (23), (α/β) satisfies

$$k^{Z_1} \left(\frac{\alpha}{\beta}\right)^2 - 2(2^{2m} - d Y_1^2)\frac{\alpha}{\beta} + k^{Z_1} = 0. \tag{25}$$

Since $k > 1$ and $\gcd(k^{Z_1}, 2(2^{2m} - d Y_1^2)) = \gcd(2^{2m} + d Y_1^2, 2(2^{2m} - d Y_1^2)) = 1$, we find from (25) that α/β is not a root of unity. Therefore, by (23), (α, β) is a Lehmer pair with parameters $(-4d Y_1^2, 2^{2m+2})$.

Let $L_r(\alpha, \beta)$ $(r = 1, 2, \ldots)$ denote the Lehmer numbers defined by (14). We get from (14), (22) and (23) that

$$L_t(\alpha, \beta) = \pm 1. \tag{26}$$

It implies that the Lehmer number $L_t(\alpha, \beta)$ has no primitive divisor. Therefore, by Lemma 8, we get $t \leq 30$. Further, since t is odd, by Lemma 7, we get $t \in \{1, 3, 5\}$.

If $t = 5$, then from (22) we have

$$2^{4m} - 10 \cdot 2^{2m} d Y_1^2 + 5 \left(d Y_1^2\right)^2 = \pm 1. \tag{27}$$

But, since dY_1^2 is odd, we see from (27) that $2^{4m} - 10 \cdot 2^{2m} dY_1^2 + 5(dY_1^2)^2 \equiv 5 \not\equiv \pm 1 \pmod 8$, a contradiction.

If $t = 3$, then we have

$$2^{2m} - 3dY_1^2 = 1, \tag{28}$$

since $2^{2m} \equiv 1 \pmod 3$. The combination of (17), (21) and (28) yields

$$2^{2m+2} - 3k^{Z_1} = 1. \tag{29}$$

Since $k > 1$, by Lemma 6 we see from (29) that $Z_1 = 1$. Therefore, by (15) we get

$$n = 3,\ Z_1 = 1,\ k = \frac{1}{3}(2^{2m+2} - 1). \tag{30}$$

By the above analysis we get from (15) that $t = 1$ and

$$n = Z_1 \tag{31}$$

except the case (30). Therefore, by (18) and (31), we have

$$n \mid H(-4d) \tag{32}$$

except when (30). Further, by Lemma 3 we deduce from (30) and (32) that (3) is true. Thus, the theorem is proved.

ACKNOWLEDGEMENTS. The authors would like to thank the referee for his very helpful and detailed comments.

REFERENCES

1. N. C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, *Pacific J. Math.* **5**(4) (1955), 321–324.

2. Y. Bilu, G. Hanrot and P. M. Voutier (with an appendix by M. Mignotte), Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539** (2001), 75–122.

3. M. J. Cowles, On the divisibility of the class number of imaginary quadratic fields, *J. Number Theory* **12**(2) (1980), 113–115.

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**(2) (1978), 201–224.

5. C. Heuberger and M. H. Le, On the generalized Ramanujan–Nagell equation $x^2 + D = p^Z$, *J. Number Theory* **78**(4) (1999), 312–331.

6. L. K. Hua, *Introduction to number theory* (Springer-Verlag, Berlin, 1982).

7. Y. Kishi, Note on the divisibility of the class number of certain imaginary quadratic fields, *Glasgow Math. J.* **51**(1) (2009), 187–191 (Corrigendum: *Glasgow Math. J.* **52**(2) (2010), 207–208).

8. R. A. Mollin, Diophantine equations and class numbers, *J. Number Theory* **24**(1) (1986), 7–19.

9. R. A. Mollin, Solutions, of diophantine equations and divisibility of class numbers of complex quadratic fields, *Glasgow Math. J.* **38**(2) (1996), 195–197.

10. P. M. Voutier, Primitive divisors of Lucas and Lehmer sequences, *Math. Comp.* **64**(5) (1995), 869–888.