Quadratic fields with noncyclic 5 or 7-class groups

*†‡

Dongho Byeon

Abstract. We shall show that the number of quadratic fields with absolute discriminant $\leq x$ and noncyclic 5 or 7-class group is $\gg x^{1/4}$ improving the existing known bound $\gg x^{\frac{1}{5}-\epsilon}$ for $g = 5$ and $\gg x^{\frac{1}{7}-\epsilon}$ for $g = 7$ in [1].

1 Introduction

Under the assumption that ideal class group of quadratic field is quite rarely noncyclic, Cohen and Lenstra [3] conjectured that the probability a given positive integer g divides the class numbers of quadratic fields is positive. After Murty [8] obtained the first quantitative result on the number of such quadratic fields, several authors improved his result. The best known quantitative result for imaginary quadratic fields is;

> (Soundararajan [10]) *If $g \geq 3$ is an odd positive integer, then the number of imaginary quadratic fields whose absolute discriminant is $\leq x$ and whose ideal class group has an element of order g is $\gg x^{\frac{1}{2}+\frac{1}{g}-\epsilon}$, for any $\epsilon > 0$.*

and for real quadratic fields is;

---

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

†This work was supported by KRF-2005-070-C00004.

‡The author also holds joint appointment in the Research Institute of Mathematics, Seoul National University.

(Yu [13]) *If $g \geq 3$ is an odd positive integer, then the number of real quadratic fields whose absolute discriminant is $\leq x$ and whose ideal class group has an element of order g is $\gg x^{\frac{1}{g}-\epsilon}$, for any $\epsilon > 0$.*

On the other hand, Yamamoto [12] proved that for any odd positive integer $g \geq 3$, there are infinitely many imaginary quadratic fields with ideal class group having a subgroup isomorphic to $\mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z}$. For real quadratic fields, less is known except the case $g = 3$, 5, 7 due to Craig [4] and Mestre [7]. The first quantitative result for imaginary quadratic fields with noncyclic ideal class group is

(Byeon [1]) *If $g \geq 3$ is an odd positive integer, then the number of imaginary quadratic fields whose absolute discriminant $\leq x$ and ideal class group having a subgroup isomorphic to $\mathbb{Z}/g\mathbb{Z}\times\mathbb{Z}/g\mathbb{Z}$ is $\gg x^{1/g-\epsilon}$, for any $\epsilon > 0$.*

In this paper, applying Stewart and Top's [11] result on square-free sieve to Mestre's [7] work on ideal class groups and elliptic curves, we shall improve this result for $g = 5$ or 7.

Theorem 1.1 *If $g = 5$ or 7, then the number of imaginary quadratic fields (or real quadratic fields) whose absolute discriminant $\leq x$ and ideal class group having a subgroup isomorphic to $\mathbb{Z}/g\mathbb{Z} \times \mathbb{Z}/g\mathbb{Z}$ is $\gg x^{\frac{1}{4}}$.*

Remark 1. Recently, using similar method we [2] improved the lower bound of the number of real quadratic fields whose absolute discriminant is $\leq x$ and whose class number is divisible by 5 or 7 to $\gg x^{1/2}$.
Remark 2. For $g = 3$, recently Luca and Pacelli [5] improved the lower bound of the number of quadratic fields with absolute discriminant $\leq x$ and noncyclic 3-class group to $\gg x^{\frac{1}{2}}$ by using a different method.

2 Ideal class groups and elliptic curves

First we recall Mestre's [7] construction of quadratic fields with class number divisible by 5 or 7 by using elliptic curves. Let A be an abelian variety defined over $\mathbb{Q}$ with a point P defined over $\mathbb{Q}$ of order p where p is an odd prime. Let A' denote the quotient of A divided by the subgroup generated by P and φ denote

the isogeny $A \to A'$. Let $A_{/\mathbb{Z}}$ be the Neron minimal model for A over $\mathbb{Z}$. Then there exists a group scheme $A'_{/\mathbb{Z}}$ with generic fiber A' and an exact sequence:

$$0 \to \mathbb{Z}/p\mathbb{Z} \to A_{/\mathbb{Z}} \to A'_{/\mathbb{Z}} \to 0.$$

If K is an algebraic number field with ring of integers O_K and ideal class group Cl_K, one obtains the exact sequence:

$$0 \to A'(O_K)/\varphi A(O_K) \to \mathrm{Hom}(\mathrm{Cl}_K, \mathbb{Z}/p\mathbb{Z}).$$

Thus the p-rank of Cl_K is bounded from below by the p-rank of $A'(O_K)/\varphi A(O_K)$.

Specially, to obtain quadratic fields with noncyclic p-class groups, we need two distinct points Q_1 and Q_2 on A' with coordinates in a quadratic field K such that the points in the fibers $\varphi^{-1}(Q_1)$ and $\varphi^{-1}(Q_2)$ generate two independent unramified cyclic extensions of degree p of K. Applying this to elliptic curves defined over $\mathbb{Q}$ with a point P defined over $\mathbb{Q}$ of order $p = 5$ or 7, Mestre obtained the following propositions.

Proposition 2.1 *(Mestre [7]) For integers u, v, let*

$B_2(u,v) = u^2 + 4uv - 4v^2$,
$B_4(u,v) = v(u-v)(10u^2 - 39uv + 20v^2)$,
$B_6(u,v) = v(u-v)(4u^4 - 56u^3v + 124u^2v^2 - 155uv^3 + 79v^4)$,
$D(x,u,v) = 4x^3 + B_2(u,v)x^2 + 2B_4(u,v)x + B_6(u,v)$.

Suppose that u is even and v is odd. If x_1, x_2 are two different rational numbers satisfying the following conditions:

(i) $D(x_1,u,v) = D(x_2,u,v)$
(ii) for any prime number l dividing $u^2 + 9uv - 11v^2$, x_1, x_2 are not congruent to $5u - 6v$ modulo l,
(iii) $x_1 \not\equiv x_2 \pmod 2$ and for a given prime number q such that q does not divide $v(u-v)(u^2+9uv-11v^2)$ and $(\frac{D(x,u,v)}{q}) \neq -1$, $x_1 \equiv x_2 \pmod q$,

then the ideal class group of quadratic field $K = \mathbb{Q}(\sqrt{D(x,u,v)})$ has a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Proposition 2.2 *(Mestre [7]) For integers u, v, let*

$B_2(u,v) = u^4 - 6u^3v + 3u^2v^2 + 2uv^3 + v^4$,

$B_4(u,v) = uv(u-v)(-10u^5 - 10u^4v + 61u^3v^2 - 81u^2v^3 + 59uv^4 - 10v^5)$,
$B_6(u,v) = uv(u-v)(-4u^9 - 36u^8v + 148u^7v^2 - 280u^6v^3 + 528u^5v^4 - 843u^4v^5 + 727u^3v^6 - 304u^2v^7 + 72uv^8 - 4v^9)$,
$D(x,u,v) = 4x^3 + B_2(u,v)x^2 + 2B_4(u,v)x + B_6(u,v)$.

Suppose that $u \equiv 2$ and $v \equiv 1 \pmod 3$. If x_1, x_2 are two different rational numbers satisfying the following conditions:

(i) $D(x_1,u,v) = D(x_2,u,v)$
(ii) for any prime number l dividing $u^3 - 8u^2v + 5uv^2 + v^3$, x_1, x_2 are not congruent to $-28u^2 + 20uv + 3v^2$ modulo l
(iii) $x_1 \not\equiv x_2 \pmod 3$ and for a given prime number q such that q does not divide $uv(u-v)(u^3 - 8u^2v + 5uv^2 + v^3)$ and $(\frac{D(x,u,v)}{q}) \neq -1$, $x_1 \equiv x_2 \pmod q$,

then the ideal class group of quadratic field $K = \mathbb{Q}(\sqrt{D(x,u,v)})$ has a subgroup isomorphic to $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

Remark. One cannot obtain similar propositions for $p \geq 11$, since rational p-torsion points on elliptic curves do not exist if $p \geq 11$ (See [6]).

3 Square-free sieve

Now we recall some results on counting square-free values of binary forms. Let A, B and M be integers with $M \geq 1$. Let

$$F(U,V) = a_rU^r + a_{r-1}U^{r-1}V + \cdots + a_0V^r$$

be a binary form with integer coefficients and positive degree r. For any positive real number X, let $S(X)$ denote the number of square-free integers t with $|t| \leq X$ for which there exist positive integers a, b and z with $a \equiv A \pmod M$, $b \equiv B \pmod M$ and $F(a,b) = tz^2$. Stewart and Top [11] obtained the following proposition.

Proposition 3.1 *(Stewart and Top [11]) Let A, B and M be integers with $M \geq 1$. Let F be a binary form with integer coefficients, non-zero discriminant and degree $r \geq 3$. Suppose that the largest degree of an irreducible factor of F over $\mathbb{Q}$ is ≤ 6. Then*

$$S(X) \gg X^{\frac{2}{r}}.$$

Remark. In [11], $S(X)$ is defined for integers a, b. But we easily see that nothing is changed if $S(X)$ is defined for positive integers a, b.

4 Proof of Theorem 1.1

To prove Theorem 1.1, we need the following lemmas.

Lemma 4.1 *Let $m(t)$ be the polynomial of degree* 8

$$\begin{aligned} m(t) &= (t^2+t+1) \\ &\times (2267524411729t^6 + 6809864269707t^5 \\ &+ 13573373036210t^4 + 15772668841175t^3 \\ &+ 13536917863610t^2 + 6795282200667t \\ &+ 2267524411729). \end{aligned}$$

Suppose that t is a positive rational number satisfying

(i) $t \equiv 0$ (mod 139*) and $t \equiv 0$ (mod* 409*),*
(ii) $t \equiv 0$ (mod 2*) and $t \equiv 2$ (mod* 3*).*

Then the ideal class group of real quadratic field $K = \mathbb{Q}(\sqrt{m(t)})$ has a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Proof: If we take $u = 234$, $v = 1$ and $q = 3$ in Proposition 2.1, then we have

$$D(x,u,v) = 4x^3 + 55688x^2 + 250919564x + 2628731414009.$$

For a positive rational number t satisfying the conditions (i) (ii), let

$$\begin{aligned} x_1(t) &= -(5591t^2 + 3400t + 3070)/(t^2+t+1), \\ x_2(t) &= -(3070t^2 + 2740t + 5261)/(t^2+t+1). \end{aligned}$$

Then we see that $x_1(t)$ and $x_2(t)$ satisfy the conditions in Proposition 2.1 and $D(x_1(t), 234, 1) = D(x_2(t), 234, 1)$ is equal to $m(t)$ up to a square factor. Since the coefficients of $m(t)$ are positive, the quadratic field $K = \mathbb{Q}(\sqrt{m(t)})$ is real. Thus the lemma follows from Proposition 2.1. □

Lemma 4.2 *(Mestre [7] and Schoof [9]) Let $m(t)$ be the polynomial of degree* 8

$$m(t) = -(t^2+t+1)(47t^6 + 21t^5 + 598t^4 + 1561t^3 + 1198t^2 + 261t + 47).$$

Suppose that t is a positive rational number satisfying

(i) $t \equiv 0$ (mod 11*),*
(ii) $t \equiv 0$ (mod 2*) and $t \equiv 3$ (mod* 5*).*

Then the ideal class group of imaginary quadratic field $K = \mathbb{Q}(\sqrt{m(t)})$ has a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Proof: If we take $u = 0$, $v = 1$, $q = 5$ and let

$$\begin{aligned} x_1(t) &= -(2t^2 - 3t - 4)/(t^2 + t + 1), \\ x_2(t) &= (4t^2 + 5t - 1)/(t^2 + t + 1), \end{aligned}$$

then the lemma follows from Proposition 2.1. □

Lemma 4.3 *Let $m(t)$ be the polynomial of degree* 8

$$\begin{aligned} m(t) &= (t^2 + t + 1) \\ &\times (4784122454229365644086428380t^6 \\ &+ 1435511886274120607167109630 0t^5 \\ &+ 2871532698806629998543754549 1t^4 \\ &+ 3349628420472022605338389328 2t^3 \\ &+ 2870156948780075428837848969 1t^2 \\ &+ 1434961586263498779284747398 0t \\ &+ 478412245422936564408642838 0). \end{aligned}$$

Suppose that t is a positive rational number satisfying

(i) $t \equiv 0$ (mod 29*), $t \equiv 0$ (mod* 113*), $t \equiv 0$ (mod* 3793*),*
(ii) $t \equiv 0$ (mod 3*) and $t \equiv 0$ (mod* 11*).*

Then the ideal class group of real quadratic field $K = \mathbb{Q}(\sqrt{m(t)})$ has a subgroup isomorphic to $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

Proof: If we take $u = -229$, $v = 1$, $q = 11$ and let

$$\begin{aligned} x_1(t) &= -1/4 \cdot (1065646690t^2 + 983260749t + 837118325)/(t^2 + t + 1), \\ x_2(t) &= -1/4 \cdot (837118325t^2 + 690975901t + 919504266)/(t^2 + t + 1), \end{aligned}$$

then the lemma follows from Proposition 2.2. □

Lemma 4.4 *Let $m(t)$ be the polynomial of degree* 8

$$\begin{aligned} m(t) &= -(t^2 + t + 1) \\ &\times (156793522148t^6 + 287439299684t^5 \\ &+ 451040463269t^4 + 1032819649598t^3 \\ &+ 1365746797069t^2 + 653321833204t \\ &+ 156793522148). \end{aligned}$$

Suppose that t is a positive rational number satisfying

(i) $t \equiv 0$ *(mod* 617*),*
(ii) $t \equiv 0$ *(mod* 3*) and* $t \equiv 11$ *(mod* 17*).*

Then the ideal class group of imaginary quadratic field $K = \mathbb{Q}(\sqrt{m(t)})$ *has a subgroup isomorphic to* $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$*.*

Proof: If we take $u = 5$, $v = -2$, $q = 17$ and let

$$\begin{aligned} x_1(t) &= -1/4 \cdot (669t^2 + 9685t + 5354)/(t^2 + t + 1) \\ x_2(t) &= -1/4 \cdot (5354t^2 + 1023t - 3662)/(t^2 + t + 1). \end{aligned}$$

then the lemma follows from Proposition 2.2. □

Proof of Theorem 1.1: First we prove the theorem for the case of $g = 5$ and real quadratic fields. Let $A = 2 \cdot 2 \cdot 139 \cdot 233 \cdot 409$, $B = 1$ and $M = 2 \cdot 3 \cdot 139 \cdot 233 \cdot 409$. Let a, b be positive integers for which $a \equiv A \pmod{M}$, $b \equiv B \pmod{M}$. Then by Lemma 4.1, the ideal class group of real quadratic field

$$\begin{aligned} K &= \mathbb{Q}(\sqrt{m(a/b)}) \\ &= \mathbb{Q}(\sqrt{b^8 m(a/b)}), \end{aligned}$$

where

$$\begin{aligned} b^8 m(a/b) &= 2267524411729a^8 + 9077388681436a^7 b \\ &+ 22650761717646a^6 b^2 + 36155906147092a^5 b^3 \\ &+ 42882959740995a^4 b^4 + 36104868905452a^3 b^5 \\ &+ 22599724476006a^2 b^6 + 9062806612396ab^7 \\ &+ 2267524411729b^8, \end{aligned}$$

has a subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Let $F(U, V) := V^8 m(U/V)$ be the binary form of degree 8. Then Proposition 3.1 implies that the number of square-free integers t with $0 < t \leq x$ for which there exist positive integers a, b and z with $a \equiv A \pmod{M}$, $b \equiv B \pmod{M}$ and $F(a, b) = tz^2$ is $\gg x^{\frac{1}{4}}$ and the theorem follows. For the remaining cases, we can similarly prove them from Lemma 4.2, 4.3 and 4.4. □

Acknowledgement The author would like to thank the referee for correcting an error in Lemma 4.1, finding a mistake in Lemma 4.4 and making many valuable suggestions.

References

[1] D. Byeon, Imaginary quadratic fields with noncyclic ideal class groups, Ramnujan J., **11** (2006), 159–163.

[2] D. Byeon, Real quadratic fields with class number divisible by 5 or 7, Manuscripta Math., **120** (2006), 211–215.

[3] H. Cohen and H. W. Lenstra, Heuristics on class groups of number fields in : Number Theory (Noordwijkerhout 1983), Lecture Notes in Math. 1068, Springer-Verlag, New York, 33–62.

[4] M. Craig, A construction for irregular discriminants, Osaka J. Math, **14** (1977), 365–402.

[5] F. Luca and A. Pacelli, Class groups of quadratic fields of 3-rank at least 2: Effective bounds, preprint.

[6] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math., No. 47 (1978), 33–186.

[7] J. -F. Mestre, Courbes elliptiques et groupes de classes d'idéaux de certains corps quadratiques, J. Reine Angew. Math. **343** (1983), 23–35.

[8] M. R. Murty, Exponents of class groups of quadratic fields, in "Topics in Number Theory", 229–239, Mathematical Applications, vol. 467, Kluwer, 1999.

[9] R. J. Schoof, Class groups of complex quadratic fields, Math. of Computation, **4** (1983), 295–302.

[10] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, J. London Math. Soc., **61** (2000), 681–690.

[11] C. L. Stewart and J. Top, On ranks of twists of elliptic curves and power-free values of binary forms, J. of Amer. Math. Soc., **8** (1995), 943–973.

[12] Y. Yamamoto, On ramified Galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57–76

[13] G. Yu, A note on the divisibility of class numbers of real quadratic fields, J. Number Theory, **97** (2002), 35–44.

Department of Mathematics
Seoul National University
Seoul 151-747, Korea
E-mail: dhbyeon@snu.ac.kr