Real quadratic fields with class number divisible by 5 or 7

Dongho Byeon *†

Department of Mathematics, Seoul National University, Seoul 151-747, Korea

E-mail: dhbyeon@math.snu.ac.kr

Abstract. We shall show that the number of real quadratic fields whose absolute discriminant is $\leq x$ and whose class number is divisible by 5 or 7 is $\gg x^{\frac{1}{2}}$ improving the existing best known bound $\gg x^{\frac{1}{5}-\epsilon}$ for $g = 5$ and $\gg x^{\frac{1}{7}-\epsilon}$ for $g = 7$ of Yu [11].

1 Introduction and statement of results

Cohen and Lenstra [2] conjectured that the probability a prime p divides the class numbers of imaginary quadratic fields is

$$1 - \prod_{i=1}^{\infty}(1 - \frac{1}{p^i})$$

and the probability a prime p divides the class numbers of real quadratic fields is

$$1 - \prod_{i=2}^{\infty}(1 - \frac{1}{p^i}).$$

However nothing is known. In [7] [8], Murty obtained the first quantitative result on the number of such quadratic fields. After him, several authors improved his result. The best known quantitative result for imaginary quadratic fields is;

Mathematics Subject Classification(2000): 11R11, 11R29

†This work was supported by KRF-R08-2003-000-10243-0 and partially by KRF-2005-070-C00004.

(Soundararajan [9]) *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 $\gg X^{\frac{1}{2}+\frac{3}{2(g+1)}-\epsilon}$, for any $\epsilon > 0$.*

and for real quadratic fields is;

(Yu [11]) *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 $\epsilon > 0$.*

Specially, when $g = 3$, the best known bound is $\gg X^{\frac{7}{8}}$ for imaginary and real quadratic fields (See [9] and [1]). In this note, applying Stewart and Top's [10] result on square free sieve to Mestre's [6] work on ideal class groups and elliptic curves, we shall improve Yu's result for $g = 5$ or 7.

Theorem 1.1 *If $g = 5$ or 7, then the number of real quadratic fields whose absolute discriminant $\leq X$ and ideal class group having an element of order g is $\gg X^{\frac{1}{2}}$.*

2 Ideal class groups and elliptic curves

First we recall Mestre's [6] 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 $A_{/Z}$ 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 rank of $A'(O_K)/\varphi A(O_K)$. 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 [6]) 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 is a rational number satisfying the following conditions:

(i) for any prime number l dividing $u^2 + 9uv - 11v^2$, x is not congruent to $5u - 6v$ modulo l,
(ii) x is 2-integral,

then the class number of quadratic field $K = \mathbb{Q}(\sqrt{D(x,u,v)})$ is divisible by 5.

Proposition 2.2 *(Mestre [6]) 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 $v \equiv 1$ (mod 3). If x is a rational number satisfying the following conditions:

(i) for any prime number l dividing $u^3 - 8u^2v + 5uv^2 + v^3$, x is not congruent to $-28u^2 + 20uv + 3v^2$ modulo l,
(ii) x is 3-integral,

then the class number of quadratic field $K = \mathbb{Q}(\sqrt{D(x,u,v)})$ is divisible by 7.

Remark. One can not obtain similar propositions for $p \geq 11$, since rational p-torsion points on elliptic curves do not exist if $p \geq 11$ (See [5]).

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

$$F(U,V) = a_r U^r + a_{r-1} U^{r-1} V + \cdots + a_0 V^r$$

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 [10] modified the result of Greaves [4], Gouvea and Mazur [3] and obtained the following proposition.

Proposition 3.1 *(Stewart and Top [10]) 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. Proposition 3.1 follows from the same proof as Stewart and Top [10] gave for a more general $S(X)$.

4 Proof of Theorem 1.1

To prove Theorem 1.1, we need the following lemmas.

Lemma 4.1 *Let $D(x) = 4x^3 + 188x^2 + 21824x + 24761$. If x is a rational number satisfying the following conditions:*

(i) $x \not\equiv 54$ modulo 241
(ii) x is 2-integral,

then the class number of quadratic field $K = \mathbb{Q}(\sqrt{D(x)})$ is divisible by 5.

Proof: If we take $u = 12$ and $v = 1$, the lemma follows from Proposition 2.1 (1). We note that $u = 12$ is the smallest positive even integer for which all of B_2, B_4, B_6 are positive when $v = 1$. □

Example. If we take $x = 1$ in Lemma 4.1, then $D(1) = 46777$ and the class number of $\mathbb{Q}(\sqrt{46777})$ is 10.

Lemma 4.2 *Let* $D(x) = 4x^3 + 42225x^2 + 1193496668x + 398877631516$. *If* x *is a rational number satisfying the following conditions:*

(i) $x \not\equiv 2237$ *modulo* 3613
(ii) x *is* 3*-integral,*

then the class number of quadratic field $K = \mathbb{Q}(\sqrt{D(x)})$ *is divisible by* 7.

Proof: If we take $u = -13$ and $v = 1$, the lemma follows from Proposition 2.2 (1). □

Example. If we take $x = -338$ in Lemma 4.2, then $D(-338) = 145252744$ and the class number of $\mathbb{Q}(\sqrt{145252744})$ is 28.

Proof of Theorem 1.1: First we prove the theorem for the case of $g = 5$. Let $A = 1$, $B = 1$ and $M = 2 \cdot 241$. Let a, b be positive integers for which $a \equiv 1 \pmod{2 \cdot 241}$, $b \equiv 1 \pmod{2 \cdot 241}$. Then by Lemma 4.1, the class number of real quadratic field

$$\begin{aligned} K &= \mathbb{Q}(\sqrt{4(a/b)^3 + 188(a/b)^2 + 21824(a/b) + 24761}) \\ &= \mathbb{Q}(\sqrt{b(4a^3 + 188a^2b + 21824ab^2 + 24761b^3)}) \end{aligned}$$

is divisible by 5. Let $F(U, V)$ be the following binary form of degree 4

$$F(U, V) = V(4U^3 + 188U^2V + 21824UV^2 + 24761V^3).$$

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 $a \equiv 1 \pmod{2 \cdot 241}$, $b \equiv 1 \pmod{2 \cdot 241}$ and $F(a, b) = tz^2$ is $\gg X^{\frac{1}{2}}$ and the theorem follows. For the case $g = 7$, we can similarly prove it from Lemma 4.2. □

Acknowledgement. The author thanks Ken Ono for suggesting him to count the number of quadratic fields with class number divisible by p by using elliptic curves. And the author thanks the referee for informing him that with the constructions given by Proposition 2.1 and 2.2, one can obtain a lower bound for Theorem 1.1 with $g = 5, 7$ as strong as $\gg X^{\frac{2}{3}-\epsilon}$.

References

[1] D. Byeon and E. Koh, Real quadratic fields with class number divisible by 3, Manuscripta Mathematica 111, (2003) 261-263.

[2] 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.

[3] F. Gouvea and B. Mazur, The square-free seive and the rank of elliptic curves, J. Amer. Math. Soc. **4** (1991), 1–23.

[4] G. .H Greaves, Power-free values of binary forms, Quart. J. Math. Oxford Ser. (2) **43** (1992), 45–65.

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

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

[7] M. R. Murty, The ABC conjecture and exponents of quadratic fields, in "Number Theory", Contemp. Math. **210** (1997) 85–95, AMS.

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

[10] 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.

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