Divisibility of class numbers of imaginary quadratic fields whose discriminant has only two prime factors

By Dongho BYEON*) and Shinae LEE**)

(Communicated by Shigefumi MORI, M.J.A., Dec. 12, 2007)

Abstract: Let $g \geq 2$ and $n \geq 1$ be integers. In this paper, we shall show that there are infinitely many imaginary quadratic fields whose class number is divisible by $2g$ and whose discriminant has only two prime divisors. As a corollary, we shall show that there are infinitely many imaginary quadratic fields whose 2-class group is a cyclic group of order divisible by 2^n.

Key words: Class number; imaginary quadratic fields.

1. Introduction and statement of results. Let $K = \mathbf{Q}(\sqrt{D})$ be the quadratic field with discriminant D, and $Cl(D)$ and $h(D)$ be the ideal class group of K and its class number respectively. The ideal class group of K in the narrow sense and its class number are denoted by $CL^+(D)$ and $h^+(D)$ respectively. We have $h^+(D) = 2h(D)$ if $D > 0$ and the fundamental unit ϵ_D has the norm 1, and $h^+(D) = h(D)$ otherwise. If we assume that $|D|$ has just two distinct prime divisors then by the genus theory of Gauss, the 2-class group of K (that is, the Sylow 2-subgroup of $CL^+(D)$) is cyclic. After Rédei and Reichardt [12–14], many authors [2,3,6–10,16] investigated the conditions for $h^+(D)$ to be divisible by 2^n when the 2-class group of K is cyclic. However the criterion for $h^+(D)$ to be divisible by 2^n is known for only $n \leq 4$ and the existence of quadratic fields with arbitrarily large cyclic 2-class groups is not known yet. In this direction, we shall show the following result.

Corollary 1.1. *Let $n \geq 1$ be an integer. There are infinitely many imaginary quadratic fields whose 2-class group is a cyclic group of order divisible by 2^n.*

On the other hand, Belabas and Fouvry [4] proved that there are infinitely many primes p such that the class number of the real quadratic field $\mathbf{Q}(\sqrt{p})$ is not divisible by 3. It seems interesting to consider similar question for the divisibility of class numbers of quadratic fields whose discriminant has a small number of prime divisors. In this direction, we shall show the following theorem.

Theorem 1.2. *Let $g \geq 2$ be an integer. Then there are infinitely many imaginary quadratic fields whose ideal class group has an element of order $2g$ and whose discriminant has only two prime divisors.*

We note that Corollary 1.1 is an immediate consequence of the case $g = 2^n$ in Theorem 1.2 and the genus theory of Gauss.

2. Proof of Theorem 1.2. To prove Theorem 1.2, we need some preliminaries. We recall a result of Brüdern, Kawada and Wooley [5], improving a previous result of Perelli [11], which implies almost all integer values of the polynomial $2\Phi(x)$ are the sum of two primes.

Lemma 2.1. *Let $\Phi(x) \in \mathbf{Z}[x]$ be a polynomial of degree k with positive leading coefficient and let $S_k(N, \Phi)$ be the number of positive integers n, with $1 \leq n \leq N$, for which the equation*

$$2\Phi(n) = p + q$$

has no solution in primes p, q. Then there is an absolute constant $c > 0$ such that

$$S_k(N, \Phi) \ll_{\Phi} N^{1-c/k}.$$

We note that $S_k(N, \Phi) \ll_{\Phi} N^{1-c/k}$ means that there is a constant C which depends on Φ and satisfies $S_k(N, \Phi) < C \cdot N^{1-c/k}$ for sufficiently large N. Now using well known results (for an example, see [15]) on the divisibility of class numbers of imaginary quadratic fields, we can prove Theorem 1.2.

Proof of Theorem 1.2. Let $g \geq 2$ be an integer and let

$$\Phi(x) = 2(8x + 1)^g \in \mathbf{Z}[X].$$

Then by Lemma 2.1, there are infinitely many

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

*) Department of Mathematics and Research Institute of Mathematics, Seoul National University, Seoul 151-747, Korea.
**) Kyungbock High School, Seoul 110-030, Korea.

positive integers m', for which the equation

$$2\Phi(m') = 4(8m'+1)^g = p + q \tag{1}$$

has a solution in odd primes p, q. Since $4(8m'+1)^g = p+q \equiv 4 \pmod 8$, the primes p, q should satisfy one of the following conditions:
(i) $p \equiv 1 \pmod 8$ and $q \equiv 3 \pmod 8$,
(ii) $p \equiv 3 \pmod 8$ and $q \equiv 1 \pmod 8$,
(iii) $p \equiv 5 \pmod 8$ and $q \equiv 7 \pmod 8$,
(iv) $p \equiv 7 \pmod 8$ and $q \equiv 5 \pmod 8$.

For m', p, q satisfying the equation (1), let $m = 8m'+1$ and $n = \frac{p-q}{2} > 0$ (we can assume $p > q$, without loss of generality). Then we have infinitely many distinct positive square-free integers

$$d = 4m^{2g} - n^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = pq. \tag{2}$$

We consider the ideal factorization in $\mathbf{Q}(\sqrt{-d})$

$$(4m^{2g}) = (n^2+d) = (n+\sqrt{-d})(n-\sqrt{-d}).$$

From the conditions (i)-(iv), we have that $-d \equiv 5 \pmod 8$ and n is odd. So $\frac{n\pm\sqrt{-d}}{2}$ is an algebraic integer and we can also consider the ideal factorization in $\mathbf{Q}(\sqrt{-d})$

$$(m)^{2g} = \left(\frac{n+\sqrt{-d}}{2}\right)\left(\frac{n-\sqrt{-d}}{2}\right).$$

We claim that the two ideals $(\frac{n+\sqrt{-d}}{2})$ and $(\frac{n-\sqrt{-d}}{2})$ are coprime. If $\mathbf{a}$ is a common factor, then $\mathbf{a}$ should divide (m^{2g}, n). But $(m^{2g}, n) = 1$, otherwise $d = 4m^{2g} - n^2$ is not square-free. So there are no common factors of the two ideals $(\frac{n+\sqrt{-d}}{2})$ and $(\frac{n-\sqrt{-d}}{2})$.

Thus each ideals $(\frac{n\pm\sqrt{-d}}{2})$ is a $2g$-th power, say $\mathbf{b}^{2g} = (\frac{n+\sqrt{-d}}{2})$. Suppose that $\mathbf{b}$ has order $r < 2g$. Then $r \le g$ and $\mathbf{b}^r = (\frac{u+v\sqrt{-d}}{2})$, where u, v are non-zero integers such that $u \equiv v \pmod 2$. Since $\mathbf{Q}(\sqrt{-d})$ has only the units ± 1, we have the relation

$$\left(\frac{n+\sqrt{-d}}{2}\right) = \pm\left(\frac{u+v\sqrt{-d}}{2}\right)^{\frac{2g}{r}}.$$

If we take norms on both sides of the equation $\mathbf{b}^{2g} = (\frac{n+\sqrt{-d}}{2})$, we have

$$\begin{aligned} m^{2g} &= \frac{n^2+d}{4} = N(\mathbf{b}^r)^{\frac{2g}{r}} \\ &= \left(\frac{u^2+v^2d}{4}\right)^{\frac{2g}{r}} \ge \left(\frac{1+d}{4}\right)^2, \end{aligned}$$

that is,

$$4m^g - 1 \ge d. \tag{3}$$

But from the equation (2), we have

$$(2m^g - n)(2m^g + n) = d.$$

If $2m^g - n > 1$ then $2m^g + n \le \frac{d}{2}$. It contradicts to (3). And $2m^g - n = 1$ is impossible because $2m^g - n = \frac{p+q}{2} - \frac{p-q}{2} = q$ can not be equal to 1. Thus we conclude that the order of $\mathbf{b}$ is exactly $2g$ and completes the proof. $\square$

Remark. The construction of imaginary quadratic fields with class number divisible by $2g$ in the proof of Theorem 1.2 is due to the idea of Balog and Ono in [1]. To get some results on the nontriviality of Shafarevich-Tate groups of certain elliptic curves, they construct infinitely many

$$d = ABp_1 \cdots p_{2l} = m^{2l} - n^2,$$

where A, B are integer constants and p_i, $1 \le i \le 2l$ are distinct primes satisfying some conditions.

Acknowledgements. The authors thank the referee for some helpful suggestions. This work was supported by KRF-2005-070-C00004.

References

[1] A. Balog and K. Ono, Elements of class groups and Shafarevich-Tate groups of elliptic curves, Duke Math. J. **120** (2003), no. 1, 35–63.
[2] P. Barrucand and H. Cohn, Notes on primes of type $x^2 + 32y^2$, class number, and residuacity, J. Reine Angew. Math. **238** (1969), 67–70.
[3] H. Bauer, Zur Berechnung der 2-Klassenzahl der quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, J. Reine Angew. Math. **248** (1971), 42–46.
[4] K. Belabas and E. Fouvry, Sur le 3-rang des corps quadratiques de discriminant premier ou presque premier, Duke Math. J. **98** (1999), no. 2, 217–268.
[5] J. Brüdern, K. Kawada and T. D. Wooley Additive reprensentation in thin sequences, II: The binary Goldbach problem, Mathematica **47** (2000), no. 1–2, 117–125.
[6] H. Hasse, Über die Teilbarkeit durch 2^3 der Klassenzahl imaginär-quadratischer Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, J. Reine Angew. Math. **241** (1970), 1–6.
[7] H. Hasse, Über die Teilbarkeit durch 2^3 der Klassenzahl quadratischen Zahlkörper mit genau zwei verschiedenen Diskriminantenprimteilern, Math. Nachr. **46** (1970), 61–70.
[8] P. Kaplan, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadra-

tique, J. Math. Soc. Japan **25** (1973), 596–608.

[9] P. Kaplan, Unités de norme -1 de $Q(\sqrt{p})$ et corps de classes de degre 8 de $Q(\sqrt{-p})$ où p est un nombre premier congru à 1 modulo 8, Acta Arith. **32** (1977), no. 3, 239–243.

[10] P. Kaplan, K. Williams and K. Hardy, Divisibilité par 16 du nombre des classes au sens strict des corps quadratiques réels dont le deux-groupe des classes est cyclique, Osaka J. Math. **23** (1986), no. 2, 479–489.

[11] A. Perelli, Goldbach numbers represented by polynomials, Rev. Mat. Iberoamericana, **12** (1996), no. 2, 477–490.

[12] L. Rédei, Über die Grundeinheit unt die durch 8 teilbaren Invarianten der absolten Klasseengruppe im quadratischen Zahlkörpers, J. Reine Angew. Math. **171** (1934), 131–148.

[13] L. Rédei and H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, J. Reine Angew. Math. **170** (1933), 69–74.

[14] H. Reichardt, Zur Struktur der absoluten Ideal-Klassengruppe im quadratichen Zahlkörper, J. Reine Angew. Math. **170** (1933), 75–82.

[15] K. Soundararajan, Divisibilty of class numbers of imaginary quadratic fields, J. London Math. Soc. (2) **61** (2000), no. 3, 681–690.

[16] Y. Yamamoto, Divisibility by 16 of class number of quadratic fields whose 2-class groups are cyclic, Osaka J. Math. **21** (1984), no. 1, 1–22.