An inequality between class numbers and Ono's numbers associated to imaginary quadratic fields

By Fumio SAIRAIJI*) and Kenichi SHIMIZU**)

(Communicated by Shigefumi MORI, M. J. A., Sept. 12, 2002)

Abstract: Ono's number p_D and the class number h_D, associated to an imaginary quadratic field with discriminant $-D$, are closely connected. For example, Frobenius-Rabinowitsch Theorem asserts that $p_D = 1$ if and only if $h_D = 1$. In 1986, T. Ono raised a problem whether the inequality $h_D \leq 2^{p_D}$ holds. However, in our previous paper [8], we saw that there are infinitely many D such that the inequality does not hold. In this paper we give a modification to the inequality $h_D \leq 2^{p_D}$. We also discuss lower and upper bounds for Ono's number p_D.

Key words: Ono's number; class number.

1. Introduction. Let k_D be an imaginary quadratic field with discriminant $-D$. We denote by h_D the class number of k_D. We put $\omega_D := \sqrt{-D/4}$ or $\omega_D := (1+\sqrt{-D})/2$ according as $D \equiv 0 \bmod 4$ or $D \equiv 3 \bmod 4$. We put $f_D(x) := \mathbf{N}(x+\omega_D)$, where $\mathbf{N}$ is the norm mapping. We define the natural number p_D by

$$p_D := \max\{\nu(f_D(x)) \mid x \in \mathbf{Z} \cap [0, D/4-1]\}$$

if $D \neq 3, 4$, and $p_D = 1$ if $D = 3, 4$, where $\nu(n)$ is the number of (not necessarily distinct) prime factors of n (cf. [3, 6]). We call the number p_D Ono's number.

Ono's number p_D is connected with the class number h_D. For example, the Frobenius-Rabinowitsch Theorem [2, 7] asserts that

$$p_D = 1 \quad \text{if and only if} \quad h_D = 1.$$

The theorems of R. Sasaki [9] assert that

$$p_D = 2 \quad \text{if and only if} \quad h_D = 2,$$

$$p_D \leq h_D \quad \text{for all} \quad D. \tag{1.1}$$

H. Möller [3] also obtains (1.1) essentially.

T. Ono [6] had a conjectural inequality

$$h_D \leq 2^{p_D} \quad \text{for all} \quad D. \tag{1.2}$$

H. Wada verified the inequality (1.2) for D whose square-free part is less than or equal to 8173, by using computer (cf. [6]; p. 57). However, in our previous paper [8], we showed that there exist infinitely many D such that the inequality (1.2) does not hold. Thus we want to modify the inequality (1.2). In fact, in our previous paper, we showed that for a given positive real number c the inequality $h_D > c^{p_D}$ holds for infinitely many D. Thus the problem is to find a suitable non-constant function on D instead of the constant c.

In this paper, we give a modification of (1.2) as follows. We denote by q_D the smallest prime number which splits completely in k_D.

Theorem 2.2. *The inequality $h_D < q_D^{p_D}$ holds for all D.*

Specially in the case of $D \equiv 7 \bmod 8$, that is, $q_D = 2$, we have the following corollary.

Corollary 2.3. *The inequality $h_D < 2^{p_D}$ holds if $D \equiv 7 \bmod 8$.*

We also have the following theorem.

Theorem 2.4. *For a given positive real number ε the inequality $h_D < q_D^{(0.5+\varepsilon)p_D}$ holds for sufficiently large D.*

In this paper we also discuss estimates for p_D.

Theorem 3.3. *The inequality*

$$p_D \geq \frac{\log\log 163}{\log 163} \frac{\log D}{\log\log D}$$

holds for all D under the Extended Riemann Hypothesis (E.R.H.).

Theorem 3.4. *The inequality $p_D < (2/\log 2) \log D$ holds.*

H. Möller [3] showed that there exists a positive constant c_1 such that $c_1 \log D/\log\log D < p_D$ for sufficiently large D under (E.R.H.). He also showed

2000 Mathematics Subject Classification. Primary 11R11; Secondary 11R29.

*) Hiroshima International University, 5-1-1, Hirokoshingai, Kure, Hiroshima 737-0112.

**) Kenmei Girls' Junior and Senior High School, 68, Honmachi, Himeji, Hyogo 670-0012.

that there exists a positive constant c_2 such that the inequality $p_D < c_2 \log D/\log\log D$ holds for infinitely many D, which means that the order of his lower bound can not be improved. We determine a constant c_1 effectively by showing Theorem 3.3.

In Section 2, we discuss estimates for $p_D \log q_D/\log h_D$, and show Theorems 2.2 and 2.4. In Section 3, we discuss lower and upper bounds for p_D, and show Theorems 3.3 and 3.4.

2. An inequality between p_D and h_D. In this section, we give a modification of Ono's conjectural inequality (1.2). We showed that for a given positive real number c the inequality $h_D > c^{p_D}$ holds for infinitely many D (cf. [8]; Theorem 1). Hence we want to find a non-constant function $f(D)$ instead of the constant c and obtain an inequality of the form: $h_D \le f(D)^{p_D}$ for all D.

In the following, we show that we can take q_D as $f(D)$ in Theorem 2.2. At first we estimate $p_D \log q_D/\log h_D$.

Theorem 2.1 (cf. [3]; p. 111)**.** *The inequality $p_D > \log_{q_D}(D/4-1)$ holds for $D > 4$.*

Proof. We denote by n the greatest integer not greater than $\log_{q_D}(D/4-1)$. If $n = 0$, our assertion is trivial. We consider the case of $n \ge 1$. Since q_D splits completely in k_D and $q_D^n \le D/4-1$, we can take an integer x_0 such that q_D^n divides $f_D(x_0)$ and $0 \le x_0 \le D/4-1$. Since there does not exist any principal primitive ideal with norm less than $D/4$ in k_D, $f_D(x_0) = \mathbf{N}(x_0 + w_D) \ne q_D^n$. Thus we have

$$p_D \ge \nu(f_D(x_0)) = n+1 > \log_{q_D}(D/4-1). \qquad \square$$

From Hilfssatz 4 of Siegel [10] (cf. also [5]; p. 254), we have

$$h_D < (3/\pi)\sqrt{D}\log D \tag{2.1}$$

for $D > 4$. Thus it follows from Theorem 2.1 and (2.1) that

$$\frac{p_D \log q_D}{\log h_D} > \frac{\log(D/4-1)}{\log((3/\pi)\sqrt{D}\log D)} \tag{2.2}$$

$$= \frac{\log(D/4-1)/\log D}{\log(3/\pi)/\log D + (1/2) + \log\log D/\log D} \tag{2.3}$$

for $D > 4$.

By using the inequality (2.2), we have the following theorem.

Theorem 2.2. *The inequality $h_D < q_D^{p_D}$ holds for all D.*

Proof. We first show that the right hand side of (2.2), that is, (2.3) is a monotone increasing function for $D > e^e$. Since $\log\log D/\log D$ is monotone decreasing for $D > e^e$, the denominator of (2.3) is monotone decreasing and positive for $D > e^e$. Since the numerator of (2.3) is monotone increasing and positive for $D > 8$, (2.3) is a monotone increasing function for $D > e^e$.

The smallest value of D for which the right hand side of (2.2) is greater than one is $D = 611$. When $D = 611$, we have

$$\frac{\log(D/4-1)}{\log((3/\pi)\sqrt{D}\log D)} = 1.00042\cdots.$$

Thus it follows from (2.2) that $p_D \log q_D/\log h_D > 1.00042\cdots > 1$ holds for $D \ge 611$. Namely the inequality $h_D < q_D^{p_D}$ holds for $D \ge 611$. The inequality $h_D < q_D^{p_D}$ can be directly verified for $D < 611$.

This completes the proof. $\square$

Specially in the case of $D \equiv 7 \bmod 8$, that is, $q_D = 2$, we have the following corollary. Hence the inequality $h_D < q_D^{p_D}$ is a modification of (1.2).

Corollary 2.3. *The inequality $h_D < 2^{p_D}$ holds if $D \equiv 7 \bmod 8$.*

Since (2.3) has the limit 2 as D tends to infinity, we have the inequality

$$\liminf_{D\to+\infty} \frac{p_D \log q_D}{\log h_D} \ge 2 \tag{2.4}$$

holds. The inequality (2.4) immediately implies the following theorem.

Theorem 2.4. *For a given positive real number ε the inequality $h_D < q_D^{(0.5+\varepsilon)p_D}$ holds for sufficiently large D.*

3. Lower and upper bounds for p_D. H. Möller showed the following theorem.

Theorem 3.1 ([3]; Satz 5)**.** *There exists a positive constant c_1 such that*

$$c_1 \frac{\log D}{\log\log D} < p_D \tag{3.1}$$

for sufficiently large D under the Extended Riemann Hypothesis (E.R.H.).

It follows from Theorem 3.1 that Ono's number p_D diverges as D tends to infinity under (E.R.H.). He also showed the following theorem.

Theorem 3.2 ([3]; Satz 6)**.** *There exists a positive constant c_2 such that the inequality*

$$p_D < c_2 \frac{\log D}{\log\log D}$$

holds for infinitely many D.

Theorem 3.2 means the order of the lower bound (3.1) can not be improved.

In this section, we determine a constant c_1 effectively. Next we discuss an upper bound for p_D.

The Extended Riemann Hypothesis asserts that all Hecke L-functions are zero-free in the half-plane $\mathrm{Re}(s) > 1/2$. Under (E.R.H.), E. Bach [1] showed that the inequality

$$q_D < 6\log^2 D \tag{3.2}$$

for all D. It follows from Theorem 2.1 and (3.2) that

$$p_D \geq \frac{\log(D/4-1)}{\log q_D} > \frac{\log(D/4-1)}{\log(6\log^2 D)}$$

for $D > 4$. Thus we have

(3.3)

$$\frac{p_D \log\log D}{\log D} > \frac{\log(D/4-1)}{\log D}\frac{\log\log D}{\log 6 + 2\log\log D}$$

for $D > 4$. The functions $\log(D/4-1)/\log D$ and $\log\log D/(\log 6 + 2\log\log D)$ are monotone increasing for $D > 4$, and they are positive for $D > 8$. Thus the right hand side of (3.3) is monotone increasing for $D > 8$.

By estimating the right hand side of (3.3), we have the following theorem.

Theorem 3.3. *The inequality*

$$p_D \geq \frac{\log\log 163}{\log 163}\frac{\log D}{\log\log D} \tag{3.4}$$

holds for all D *under* (*E.R.H.*).

Proof. The right hand side of (3.3) is monotone increasing for $D > 8$ and it is greater than $\log\log 163/\log 163$ for $D \geq 73279$. Thus we have the inequality (3.4) for $D \geq 73279$. It can be directly verified for $D < 73279$. □

Next we discuss an upper bound for p_D.

Theorem 3.4. *The inequality*

$$p_D < \frac{2}{\log 2}\log D \tag{3.5}$$

holds for all D.

Proof. When $D = 3, 4$, the inequality (3.5) directly follows. We assume $D \neq 3, 4$. By the definition of p_D, there exists an integer x_0 such that $0 \leq x_0 \leq D/4 - 1$ and $p_D = \nu(f_D(x_0))$. Since we have $2^{p_D} \leq f_D(x_0) < D^2$, the inequality (3.5) holds. □

When $q_D = 2$, that is, $D \equiv 7 \bmod 8$, it follows from Theorem 2.1 that

$$\frac{p_D}{\log D} \geq \frac{1}{\log 2}\frac{\log(D/4-1)}{\log D}. \tag{3.6}$$

The right hand side of (3.6) has the limit $1/\log 2$ as D tends to infinity. By virtue of Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many primes D such that $q_D = 2$. Thus we also have the inequality

$$\limsup_{D\to+\infty} \frac{p_D}{\log D} \geq \frac{1}{\log 2}.$$

Namely, for a given positive real number ε the inequality

$$p_D > (1/\log 2 - \varepsilon)\log D$$

holds for infinitely many D. This means that the order of our upper bound (3.5) can not be improved.

By using Theorem 3.4 and the theorem of Siegel [10], that is,

$$\lim_{D\to+\infty} \frac{\log h_D}{\log\sqrt{D}} = 1,$$

we see that

$$\sup \frac{p_D}{\log h_D} < +\infty. \tag{3.7}$$

The inequality (3.7) implies the inequality (1.1) for sufficiently large D, and it also implies the following theorem.

Theorem 3.5. *The equality* $p_D = h_D$ *in* (1.1) *holds only for finitely many* D.

References

[1] Bach, E.: Explicit bounds for primality testing and related problems. Math. Comp., **55**, 355–380 (1990).

[2] Frobenius, F. G.: Über quadratische Formen die viele Primzahlen darstellen. Sitzungsber. d. Kgl. Preuss. Acad. Wiss., Berlin, pp. 966–980 (1912).

[3] Möller, H.: Verallgemeinerung eines Satzes von Rabinowitsch über imaginär-quadratische Zahlkörper. J. Reine Angew. Math., **285**, 100–113 (1976).

[4] Mollin, R. A.: Quadratics. CRC Press, Boca Raton (1996).

[5] Narkiewicz, W.: Classical Problems in Number Theory. PWN-Polish Scientific Publishers, Warszawa (1986).

[6] Ono, T.: Arithmetic of algebraic groups and its applications. St. Paul's International Exchange Series Occasional Papers VI, St. Paul's University, Tokyo (1986).

[7] Rabinowitsch, G.: Eindeutigkeit der Zerlegung in Primzahlfaktoren in quadratischen Zahlkörpern. J. Reine Angew. Math., **142**, 153–164 (1913).

[8] Sairaiji, F., and Shimizu, K.: A note on Ono's numbers associated to imaginary quadratic field. Proc. Japan Acad., **77A**, 29–31 (2001).

[9] Sasaki, R.: On a lower bound for the class number of an imaginary quadratic field. Proc. Japan Acad., **62A**, 37–39 (1986).

[10] Siegel, C. L.: Über die Classenzahl quadratischer Zahlkörper. Acta Arith., **1**, 83–86 (1935).