A note on Ono's numbers associated to imaginary quadratic fields

By Fumio Sairaiji and Kenichi Shimizu

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

(Communicated by Shokichi Iyanaga, m. j. a., Feb. 13, 2001)

Abstract: T. Ono raised some problems on relations between Ono's numbers p_D and the class numbers h_D of imaginary quadratic fields. In this paper we give an upper bound for p_D. The upper bound contributes to one of the problems.

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

$$p_D := \max\left\{ \nu(f_D(x)) \;\middle|\; x \in \mathbf{Z} \cap \left[0, \frac{D}{4} - 1\right] \right\}$$

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. [2], [3]). We call the number p_D Ono's number. By using p_D, we can formulate the Frobenius-Rabinowitsch Theorem as follows:

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

T. Ono conjectured:

(i) $p_D = 2$ if and only if $h_D = 2$;

(ii) $p_D \leq h_D$,

both of which were proved by R. Sasaki [5]. Furthermore, T. Ono raised the problem to examine whether $h_D \leq 2^{p_D}$ holds. H. Wada verified the inequality for D whose square-free part is less than or equal to 8173, by computer (cf. [3]; p. 57).

In this paper, we give an upper bound for p_D. By using the upper bound, we show that there exist infinitely many D such that $h_D \leq 2^{p_D}$ does not hold. More generally, we prove:

Theorem 1. *Let c be a positive number which is greater than one. Then there exist infinitely many D such that $h_D > c^{p_D}$.*

2. An upper bound for p_D. We denote by t_D the number of distinct prime divisors of D. We denote by q_D the smallest prime number which splits completely in k_D.

Lemma 2. *The inequality $\nu(\gcd(D, f_D(x))) \leq t_D$ holds for each integer x such that $0 \leq x \leq D/4 - 1$. The equality holds if and only if $D \equiv 0 \bmod 4$, $D/4 \equiv 2 \bmod 4$ and $x = 0$.*

Proof. We first consider the case of $D \equiv 0 \bmod 4$. Since $D/4 \equiv 1, 2 \bmod 4$, 2^2 does not divide $x^2 + D/4$ for each x. Since $D/4$ is square-free, we have $\nu(\gcd(D, f_D(x))) \leq t_D$. Suppose that the equality $\nu(\gcd(D, f_D(x))) = t_D$ holds. Then $D/4$ divides $f_D(x)$. Since $D/4$ is square-free, we see that $D/4$ divides x. Together with the condition $0 \leq x \leq D/4 - 1$, we see $x = 0$. It follows from $t_D = \nu(\gcd(D, f_D(0))) = \nu(D/4)$ that $D/4 \equiv 2 \bmod 4$. Conversely it is clear that the equality holds for $D/4 \equiv 2 \bmod 4$ and $x = 0$.

Secondly we consider the case of $D \equiv 3 \bmod 4$. Since D is square-free, we have $\nu(\gcd(D, f_D(x))) \leq t_D$. Suppose that the equality $\nu(\gcd(D, f_D(x))) = t_D$ holds. Then D divides $f_D(x)$. Consequently we see that D divides $2x+1$, which contradicts the condition $0 \leq x \leq D/4 - 1$. Thus the equality does not hold in this case. □

Lemma 3. *The inequality $\max\{f_D(x) \mid x \in \boldsymbol{Z} \cap [0, D/4 - 1]\} < (D/4)^2$ holds for $D \geq 7$.*

Proof. If $D \equiv 0 \bmod 4$ and $D \geq 8$, then

$$f_D(x) \leq \left(\frac{D}{4} - 1\right)^2 + \frac{D}{4} < \left(\frac{D}{4}\right)^2$$

for each integer x in $[0, D/4 - 1]$. If $D \equiv 3 \bmod 4$ and $D \geq 7$, then

$$f_D(x) \leq \left(\frac{D-7}{4}\right)^2 + \left(\frac{D-7}{4}\right) + \frac{D+1}{4} < \left(\frac{D}{4}\right)^2$$

for each integer x in $[0, D/4 - 1]$. Thus Lemma 3 follows. □

1991 Mathematics Subject Classification. Primary 11R11; Secondary 11R29.

Now we have the following upper bound for p_D.

Proposition 4 (cf. [2]; p. 112)**.** *The inequality* $p_D < t_D - 1 + \log_{q_D}(D/4)^2$ *holds for* $D \geq 7$.

Proof. Since for each integer x the principal ideal $(x + \omega_D)$ is primitive, $f_D(x)$ is not divided by any prime number which remains prime in k_D. By the same reason, $f_D(x)$ is not divided by the second power of any prime number which ramifies in k_D. By definition, $p_D = \nu(f_D(x_0))$ for some x_0. We can put

$$f_D(x_0) = ap_1 \cdots p_r,$$

where $a := \gcd(D, f_D(x_0))$ and p_i is a prime number which splits completely in k_D.

By Lemma 3, we have

$$q_D^r \leq p_1 \cdots p_r \leq f_D(x_0) < \left(\frac{D}{4}\right)^2,$$

and consequently, we have

$$r < \log_{q_D}\left(\frac{D}{4}\right)^2.$$

On the other hand, it follows from Lemma 2 that $\nu(a) \leq t_D - 1$ except for the case where $D \equiv 0 \bmod 4$, $D/4 \equiv 2 \bmod 4$ and $x_0 = 0$. Since $p_D = \nu(a) + r$, Proposition 4 follows except for this case. The exceptional case reduces to the case of $x_0 \neq 0$ as follows. In the exceptional case, the inequalities

$$\begin{aligned} p_D &\geq \nu\left(f_D\left(\frac{D}{4p}\right)\right) = \nu\left(\frac{D}{4p}\right) + \nu\left(\frac{D}{4p} + p\right) \\ &\geq \nu(f_D(0)) = p_D \end{aligned}$$

hold for a prime divisor p of $D/4$. Thus we can take $D/4p$ instead of 0 as x_0. □

As a corollary of Proposition 4, we give another upper bound for p_D in terms of the exponent e_D of the ideal class group of k_D.

Corollary 5. *The inequality* $p_D < 2e_D + t_D - 1$ *holds for* $D \geq 7$.

Proof. We note that the norm of each primitive principal ideal is greater than or equal to $D/4$. Since the n-th power of a prime ideal lying above q_D in k_D is primitive for each natural number n, it follows from Proposition 4 that

$$e_D \geq \log_{q_D}\frac{D}{4} > \frac{p_D - t_D + 1}{2}$$

for $D \geq 7$. Thus we obtain Corollary 5. □

3. Proof of Theorem 1. We first show that $h_D > c^{p_D}$ for D satisfying the conditions (i)-(iii) as below. Secondly we show that there exist infinitely many such D.

Let ε be a non-zero positive number less than one. Then, by the theorem of Siegel [6], there exists a constant $D_0(\varepsilon)$ such that

$$1 - \varepsilon < \frac{\log h_D}{\log\sqrt{D}} < 1 + \varepsilon$$

holds for $D \geq D_0(\varepsilon)$. Thus

$$D^{(1-\varepsilon)/2} < h_D \tag{1}$$

holds for $D \geq D_0(\varepsilon)$.

Let ℓ be an odd prime number such that

$$\ell > c^{4/(1-\varepsilon)}. \tag{2}$$

We suppose that we can take D_1, as D, satisfying the following conditions:

(i) $D_1 \geq \max\{D_0(\varepsilon), 7\}$;
(ii) $t_{D_1} = 1$;
(iii) $q_{D_1} = \ell$.

Then it follows from Proposition 4 that

$$p_{D_1} < \log_\ell\left(\frac{D_1}{4}\right)^2 < \frac{2}{\log_c \ell} \times \log_c D_1. \tag{3}$$

Since $2/\log_c \ell < (1-\varepsilon)/2$ from (2), it follows from (3) that

$$c^{p_{D_1}} < D_1^{(1-\varepsilon)/2}. \tag{4}$$

Thus, by (i) and (1), the inequality $c^{p_{D_1}} < h_{D_1}$ is verified.

Indeed, D_1 satisfies the condition (ii) if D_1 is an odd prime number such that $D_1 \equiv 3 \bmod 4$. Furthermore the condition (iii) is equivalent to the following simultaneous congruences:

(iiia) $(-D_1/p) = 0, -1$ for each prime number $p < \ell$;
(iiib) $(-D_1/\ell) = 1$,

where $(-D_1/p)$ is the Kronecker symbol. Hence, by virtue of Dirichlet's theorem on prime numbers in arithmetic progressions, there exist infinitely many D_1 satisfying the conditions (i)-(iii).

This completes the proof of Theorem 1. □

Remark 6. The smallest value of D for which $h_D > 2^{p_D}$ takes place is $D = 37123$. Then we have $h_{37123} = 17$ and $p_{37123} = 4$.

References

[1] Ishibashi, M.: A sufficient arithmetical condition for the ideal class group of an imaginary quadratic field to be cyclic. Proc. Amer. Math. Soc., **117**, 613–618 (1993).

[2] Möller, H.: Verallgemeinerung eines Satzes von Rabinowitsch über imaginär-quadratische Zahl-

körper. J. Reine Angew. Math., **285**, 100–113 (1976).

[3] Ono, T.: Arithmetic of Algebraic Groups and its Applications. St. Paul's International Exchange Series Occasional Papers VI, St. Paul's Univ., Tokyo (1986).

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

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

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

[7] Svirsky, J. B.: On the class numbers of imaginary quadratic fields. Ph. D. thesis, Johns Hopkins Univ. (1985).